ACL Configuration Mode Commands

deny/permit (by source IP address masking) ........................................... 240
deny/permit (any) .................................................................................. 243
deny/permit (by host IP address) .............................................................. 245
deny/permit (by source ICMP packets) ...................................................... 247
deny/permit (by IP packets) .................................................................... 251
deny/permit (by TCP/UDP packets) ........................................................ 255
end .......................................................................................................... 260
exit .......................................................................................................... 261
redirect context (by IP address masking) ................................................. 262
redirect context (any) .............................................................................. 270
redirect context (by host IP address) ........................................................ 272
redirect context (by source ICMP packets) ............................................. 274
redirect context (by IP packets) ............................................................... 278
redirect context (by TCP/UDP packets) .................................................. 282
redirect css delivery-sequence ............................................................... 286
redirect css service (any) ..................................................................... 287
redirect css service (by host IP address) ................................................. 289
redirect css service (by ICMP packets) .................................................. 291
redirect css service (by IP packets) ....................................................... 295
redirect css service (by source IP address masking) .............................. 299
redirect css service (by TCP/UDP packets) .......................................... 301
redirect css service (for downlink, any) ................................................ 306
redirect css service (for downlink, by host IP address) .......................... 308
redirect css service (for downlink, by ICMP packets) ......................... 310
redirect css service (for downlink, by IP packets) .................................. 314
redirect css service (for downlink, by source IP address masking) ........... 318
redirect css service (for downlink, by TCP/UDP packets) ...................... 321
redirect css service (for uplink, any) .................................................... 326
redirect css service (for uplink, by host IP address) .............................. 328
redirect css service (for uplink, by ICMP packets) ................................ 331
redirect css service (for uplink, by IP packets) ...................................... 335
redirect css service (for uplink, by source IP address masking) .............. 339
redirect css service (for uplink, by TCP/UDP packets) ......................... 341
redirect nexthop (by IP address masking) ............................................. 345
redirect nexthop (any) ......................................................................... 348
redirect nexthop (by host IP address) .................................................... 351
redirect nexthop (by source ICMP packets) .......................................... 354
redirect nexthop (by IP packets) ............................................................. 358
redirect nexthop (by TCP/UDP packets) .............................................. 362
ACS Bandwidth Policy Configuration Mode Commands .................. 367
end .......................................................................................... 368
exit ....................................................................................... 369
flow limit-for-bandwidth ....................................................... 370
group-id .............................................................................. 371

ACS Charging Action Configuration Mode Commands ............... 373
allocation-retention-priority .................................................. 374
billing-action ........................................................................ 376
cca charging credit ............................................................... 379
charge-units .......................................................................... 381
charge-volume ...................................................................... 382
content-filtering processing server-group ................................ 385
content-id .............................................................................. 386
end ....................................................................................... 387
exit ....................................................................................... 388
flow action ............................................................................ 389
flow idle-timeout .................................................................. 395
flow limit-for-bandwidth ....................................................... 396
flow limit-for-flow-type ......................................................... 399
ip tos ................................................................................... 401
ip vlan .................................................................................. 403
nexthop-forwarding-address ............................................... 405
pco-custom1 ........................................................................ 406
product-offer-id-avp .............................................................. 407
qos-class-identifier ............................................................... 408
qos-renegotiate .................................................................. 409
service-detection ................................................................. 411
tft packet-filter ................................................................. 413
tft-notify-ue ........................................................................ 414
tos ...................................................................................... 415
tpo profile ............................................................................ 417
video bitrate ........................................................................ 418
video cae-readdressing ......................................................... 419
video detailed-statistics ......................................................... 420
video optimization-preprocessing all .................................... 421
video optimization-preprocessing cae-readdressing .................. 422
video pacing by-policing ....................................................... 423
xheader-insert ...................................................................... 425

ACS Configuration Mode Commands ........................................ 427
access-ruledef ....................................................................... 428
bandwidth-policy .................................................................. 430
buffering-limit ..................................................................... 432
charging-action .................................................................... 433
content-filtering category match-method ............................... 435
content-filtering category policy-id ....................................... 436
credit-control ....................................................................... 438
diameter credit-control .......................................................... 440
edr-format ............................................................................. 441
edr-ipproto-port-map ............................................................ 443
edr-udr-flow-control ............................................................. 444
end ....................................................................................... 445
exit ....................................................................................... 446
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>fair-usage deact-margin</td>
<td>447</td>
</tr>
<tr>
<td>fair-usage tcp-proxy</td>
<td>448</td>
</tr>
<tr>
<td>fair-usage threshold-percent</td>
<td>449</td>
</tr>
<tr>
<td>firewall dos-protection flooding</td>
<td>450</td>
</tr>
<tr>
<td>firewall flow-recovery</td>
<td>452</td>
</tr>
<tr>
<td>firewall max-ip-packet-size</td>
<td>454</td>
</tr>
<tr>
<td>firewall mime-flood</td>
<td>455</td>
</tr>
<tr>
<td>firewall nat-alg</td>
<td>456</td>
</tr>
<tr>
<td>firewall no-rulledef-matches</td>
<td>458</td>
</tr>
<tr>
<td>firewall port-scan</td>
<td>459</td>
</tr>
<tr>
<td>firewall ruledef</td>
<td>461</td>
</tr>
<tr>
<td>firewall tcp-syn-flood-intercept</td>
<td>463</td>
</tr>
<tr>
<td>firewall track-list</td>
<td>464</td>
</tr>
<tr>
<td>fw-and-nat action</td>
<td>465</td>
</tr>
<tr>
<td>fw-and-nat policy</td>
<td>467</td>
</tr>
<tr>
<td>group-of-objects</td>
<td>469</td>
</tr>
<tr>
<td>group-of-prefixed-urls</td>
<td>471</td>
</tr>
<tr>
<td>group-of-rulledefs</td>
<td>473</td>
</tr>
<tr>
<td>h323 time-to-live</td>
<td>475</td>
</tr>
<tr>
<td>h323 timeout</td>
<td>476</td>
</tr>
<tr>
<td>h323 tpkt</td>
<td>478</td>
</tr>
<tr>
<td>h323 version</td>
<td>479</td>
</tr>
<tr>
<td>host-pool</td>
<td>480</td>
</tr>
<tr>
<td>idle-timeout</td>
<td>482</td>
</tr>
<tr>
<td>imsi-pool</td>
<td>484</td>
</tr>
<tr>
<td>ip dns-learnt-entries</td>
<td>486</td>
</tr>
<tr>
<td>ip max-fragments</td>
<td>488</td>
</tr>
<tr>
<td>label content-id</td>
<td>489</td>
</tr>
<tr>
<td>nat allocation-failure</td>
<td>490</td>
</tr>
<tr>
<td>nat allocation-in-progress</td>
<td>491</td>
</tr>
<tr>
<td>nat ip downlink reassembly-timeout</td>
<td>492</td>
</tr>
<tr>
<td>nat tcp-2msl-timeout</td>
<td>493</td>
</tr>
<tr>
<td>nat unsolicited-pkts</td>
<td>494</td>
</tr>
<tr>
<td>p2p-detection attribute</td>
<td>495</td>
</tr>
<tr>
<td>p2p-detection behavioral</td>
<td>497</td>
</tr>
<tr>
<td>p2p-detection ecs-analysis</td>
<td>498</td>
</tr>
<tr>
<td>p2p-detection protocol</td>
<td>499</td>
</tr>
<tr>
<td>packet-filter</td>
<td>518</td>
</tr>
<tr>
<td>passive-mode</td>
<td>519</td>
</tr>
<tr>
<td>pcp-service</td>
<td>520</td>
</tr>
<tr>
<td>policy-control bearer-bw-limit</td>
<td>522</td>
</tr>
<tr>
<td>policy-control bind-default-bearer</td>
<td>523</td>
</tr>
<tr>
<td>policy-control burst-size</td>
<td>525</td>
</tr>
<tr>
<td>policy-control charging-action-override</td>
<td>526</td>
</tr>
<tr>
<td>policy-control charging-rule-base-name</td>
<td>527</td>
</tr>
<tr>
<td>policy-control dynamic-rule-limit</td>
<td>529</td>
</tr>
<tr>
<td>policy-control update-default-bearer</td>
<td>530</td>
</tr>
<tr>
<td>port-map</td>
<td>532</td>
</tr>
<tr>
<td>qos-group-of-rulledefs</td>
<td>534</td>
</tr>
<tr>
<td>readdress-server-list</td>
<td>536</td>
</tr>
<tr>
<td>redirect user-agent</td>
<td>538</td>
</tr>
<tr>
<td>rulebase</td>
<td>539</td>
</tr>
<tr>
<td>rulebase-list</td>
<td>541</td>
</tr>
<tr>
<td>ruledef</td>
<td>543</td>
</tr>
</tbody>
</table>
ACS Readdress Server List Configuration Mode .............................. 607
  consecutive-failures .................................................................. 608
  end ......................................................................................... 609
  exit ......................................................................................... 610
  reactivation-time .................................................................. 611
  response-timeout .................................................................. 612
  server ......................................................................................... 613
ACS Rulebase Configuration Mode Commands ............................ 615
  action priority ..................................................................... 616
  active-charging rf ................................................................. 619
  bandwidth default-policy ..................................................... 621
  billing-records ..................................................................... 622
  cca diameter requested-service-unit ..................................... 624
  cca quota .............................................................................. 626
  cca quota time-duration algorithm ........................................ 628
  cca radius accounting interval ............................................. 630
  cca radius charging context .................................................. 631
  cca radius user-password ....................................................... 632
  charging-action-override ....................................................... 633
  charging-rule-optimization .................................................... 635
  constituent-policies ............................................................... 637
  content-filtering category policy-id ........................................ 639
  content-filtering flow-any-error ............................................ 641
  content-filtering mode ........................................................... 642
  dynamic-rule order ................................................................. 644
  edr p2p .................................................................................. 645
  edr sn-charge-volume ............................................................ 647
  edr suppress-zero-byte-records ............................................ 648
  edr transaction-complete ........................................................ 649
  edr voip-call-end .................................................................. 651
  egcdr inactivity-meter ............................................................ 653
  egcdr cdr-encoding ................................................................. 654
  egcdr tariff ............................................................................. 656
  egcdr threshold ..................................................................... 657
  egcdr time-duration algorithm ................................................. 659
  end ......................................................................................... 661
  exit ......................................................................................... 662
  extract-host-from-uri ............................................................ 663
  firewall dos-protection .......................................................... 665
  firewall flooding ................................................................. 668
  firewall icmp-destination-unreachable-message-threshold ........ 670
  firewall max-ip-packet-size ................................................... 672
  firewall mime-flood ............................................................... 674
  firewall no-ruledef-matches ................................................... 676
  firewall policy ..................................................................... 678
  firewall priority ................................................................. 679
  firewall tcp-first-packet-non-syn ............................................ 682
  firewall tcp-idle-timeout-action ............................................ 683
  firewall tcp-reset-message-threshold ..................................... 684
  firewall tcp-syn-flood-intercept ............................................. 686
  flow any-error ..................................................................... 688
  flow control-handshaking ..................................................... 690
  flow end-condition ............................................................... 692
flow limit-across-applications ................................................................. 695
flow rtsp-all-pkts .............................................................................. 697
fw-and-nat default-policy ................................................................. 699
http header-parse-limit ................................................................. 700
ip reassembly-timeout .................................................................. 701
ip reset-tos ..................................................................................... 702
nat binding-record ....................................................................... 703
nat policy ......................................................................................... 705
nat suppress-aaa-update call-termination ..................................... 707
p2p dynamic-flow-detection .............................................................. 708
pcp service ....................................................................................... 709
post-processing dynamic ............................................................... 710
post-processing policy .................................................................. 712
post-processing priority ................................................................. 714
qos-renegotiate timeout ................................................................. 716
radius threshold ............................................................................. 717
ran bandwidth optimize ................................................................. 719
route priority ................................................................................... 721
rtsp dynamic-flow-detection .............................................................. 724
rtsp initial-bytes-limit .................................................................. 726
ruledef-parsing ............................................................................... 727
tcp 2msi-timeout ........................................................................... 728
tcp check-window-size ................................................................. 729
tcp mss ........................................................................................... 730
tcp out-of-order-timeout ................................................................. 732
tcp packets-out-of-order ................................................................. 733
tcp proxy-mode ............................................................................... 735
tethering-detection ........................................................................ 737
tft-notify-ue-def-bearing ................................................................. 739
timestamp rounding ....................................................................... 740
tpo default-policy ........................................................................... 742
transactional-rule-matching .......................................................... 743
transport-layer-checksum ............................................................... 744
udr threshold .................................................................................. 745
udr trigger ....................................................................................... 747
url-blacklisting action ................................................................... 749
url-preprocessing .......................................................................... 751
video optimization-preprocessing cae-readdressing ..................... 752
wtp out-of-order-timeout ................................................................. 753
wtp packets-out-of-order ............................................................... 754
xheader-encryption ........................................................................ 756

ACS Ruledef Configuration Mode Commands ...................................... 759
bearer 3gpp apr ................................................................. 760
bearer 3gpp imsi ............................................................................. 762
bearer 3gpp rat-type ................................................................. 764
bearer 3gpp sgsn-address .............................................................. 765
bearer 3gpp2 bsid .......................................................................... 766
bearer 3gpp2 service-option ............................................................ 768
bearer apr ......................................................................................... 769
bearer imsi ....................................................................................... 771
bearer rat-type ................................................................................ 773
bearer sgsn-address ..................................................................... 774
bearer traffic-group ....................................................................... 775
cca quota-state ............................................................................... 777
<table>
<thead>
<tr>
<th>Keyword</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>cca redirect-indicator</td>
<td>779</td>
</tr>
<tr>
<td>copy-packet-to-log</td>
<td>781</td>
</tr>
<tr>
<td>dns answer-name</td>
<td>782</td>
</tr>
<tr>
<td>dns any-match</td>
<td>784</td>
</tr>
<tr>
<td>dns previous-state</td>
<td>785</td>
</tr>
<tr>
<td>dns query-name</td>
<td>786</td>
</tr>
<tr>
<td>dns return-code</td>
<td>788</td>
</tr>
<tr>
<td>dns state</td>
<td>789</td>
</tr>
<tr>
<td>dns tid</td>
<td>790</td>
</tr>
<tr>
<td>email</td>
<td>791</td>
</tr>
<tr>
<td>end</td>
<td>793</td>
</tr>
<tr>
<td>exit</td>
<td>794</td>
</tr>
<tr>
<td>file-transfer any-match</td>
<td>795</td>
</tr>
<tr>
<td>file-transfer chunk-number</td>
<td>796</td>
</tr>
<tr>
<td>file-transfer current-chunk-length</td>
<td>797</td>
</tr>
<tr>
<td>file-transfer declared-chunk-length</td>
<td>798</td>
</tr>
<tr>
<td>file-transfer declared-file-size</td>
<td>799</td>
</tr>
<tr>
<td>file-transfer filename</td>
<td>800</td>
</tr>
<tr>
<td>file-transfer previous-state</td>
<td>802</td>
</tr>
<tr>
<td>file-transfer state</td>
<td>803</td>
</tr>
<tr>
<td>file-transfer transferred-file-size</td>
<td>805</td>
</tr>
<tr>
<td>ftp any-match</td>
<td>806</td>
</tr>
<tr>
<td>ftp client-ip-address</td>
<td>807</td>
</tr>
<tr>
<td>ftp client-port</td>
<td>808</td>
</tr>
<tr>
<td>ftp command args</td>
<td>809</td>
</tr>
<tr>
<td>ftp command id</td>
<td>811</td>
</tr>
<tr>
<td>ftp command name</td>
<td>812</td>
</tr>
<tr>
<td>ftp connection-type</td>
<td>814</td>
</tr>
<tr>
<td>ftp data-any-match</td>
<td>815</td>
</tr>
<tr>
<td>ftp filename</td>
<td>816</td>
</tr>
<tr>
<td>ftp pdu-length</td>
<td>818</td>
</tr>
<tr>
<td>ftp pdu-type</td>
<td>819</td>
</tr>
<tr>
<td>ftp previous-state</td>
<td>820</td>
</tr>
<tr>
<td>ftp reply code</td>
<td>821</td>
</tr>
<tr>
<td>ftp server-ip-address</td>
<td>822</td>
</tr>
<tr>
<td>ftp server-port</td>
<td>823</td>
</tr>
<tr>
<td>ftp session-length</td>
<td>824</td>
</tr>
<tr>
<td>ftp state</td>
<td>825</td>
</tr>
<tr>
<td>ftp url</td>
<td>826</td>
</tr>
<tr>
<td>ftp user</td>
<td>828</td>
</tr>
<tr>
<td>http any-match</td>
<td>830</td>
</tr>
<tr>
<td>http attribute-in-data</td>
<td>831</td>
</tr>
<tr>
<td>http attribute-in-url</td>
<td>833</td>
</tr>
<tr>
<td>http content-disposition</td>
<td>835</td>
</tr>
<tr>
<td>http content-length</td>
<td>837</td>
</tr>
<tr>
<td>http content-type</td>
<td>838</td>
</tr>
<tr>
<td>http cookie</td>
<td>840</td>
</tr>
<tr>
<td>http domain</td>
<td>842</td>
</tr>
<tr>
<td>http error</td>
<td>844</td>
</tr>
<tr>
<td>http first-request-packet</td>
<td>846</td>
</tr>
<tr>
<td>http header-length</td>
<td>847</td>
</tr>
<tr>
<td>http host</td>
<td>848</td>
</tr>
<tr>
<td>http payload-length</td>
<td>851</td>
</tr>
<tr>
<td>http pdu-length</td>
<td>852</td>
</tr>
<tr>
<td>Feature</td>
<td>Page</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>http previous-state</td>
<td>853</td>
</tr>
<tr>
<td>http referer</td>
<td>854</td>
</tr>
<tr>
<td>http reply code</td>
<td>857</td>
</tr>
<tr>
<td>http request method</td>
<td>858</td>
</tr>
<tr>
<td>http session-length</td>
<td>860</td>
</tr>
<tr>
<td>http state</td>
<td>861</td>
</tr>
<tr>
<td>http transaction-length</td>
<td>862</td>
</tr>
<tr>
<td>http transfer-encoding</td>
<td>864</td>
</tr>
<tr>
<td>http url</td>
<td>866</td>
</tr>
<tr>
<td>http user-agent</td>
<td>869</td>
</tr>
<tr>
<td>http version</td>
<td>872</td>
</tr>
<tr>
<td>http x-header</td>
<td>874</td>
</tr>
<tr>
<td>icmp any-match</td>
<td>876</td>
</tr>
<tr>
<td>icmp code</td>
<td>878</td>
</tr>
<tr>
<td>icmp type</td>
<td>879</td>
</tr>
<tr>
<td>icmpv6 any-match</td>
<td>880</td>
</tr>
<tr>
<td>icmpv6 code</td>
<td>881</td>
</tr>
<tr>
<td>icmpv6 type</td>
<td>882</td>
</tr>
<tr>
<td>if-protocol</td>
<td>883</td>
</tr>
<tr>
<td>imap any-match</td>
<td>884</td>
</tr>
<tr>
<td>imap cc</td>
<td>886</td>
</tr>
<tr>
<td>imap command</td>
<td>887</td>
</tr>
<tr>
<td>imap content class</td>
<td>889</td>
</tr>
<tr>
<td>imap content type</td>
<td>891</td>
</tr>
<tr>
<td>imap date</td>
<td>893</td>
</tr>
<tr>
<td>imap final-reply</td>
<td>895</td>
</tr>
<tr>
<td>imap from</td>
<td>897</td>
</tr>
<tr>
<td>imap mail-size</td>
<td>898</td>
</tr>
<tr>
<td>imap mailbox-size</td>
<td>900</td>
</tr>
<tr>
<td>imap message-type</td>
<td>901</td>
</tr>
<tr>
<td>imap previous-state</td>
<td>902</td>
</tr>
<tr>
<td>imap session-length</td>
<td>903</td>
</tr>
<tr>
<td>imap session-previous-state</td>
<td>904</td>
</tr>
<tr>
<td>imap session-state</td>
<td>905</td>
</tr>
<tr>
<td>imap state</td>
<td>906</td>
</tr>
<tr>
<td>imap subject</td>
<td>907</td>
</tr>
<tr>
<td>imap to</td>
<td>908</td>
</tr>
<tr>
<td>ip any-match</td>
<td>910</td>
</tr>
<tr>
<td>ip dscp</td>
<td>912</td>
</tr>
<tr>
<td>ip downlink</td>
<td>913</td>
</tr>
<tr>
<td>ip dst-address</td>
<td>914</td>
</tr>
<tr>
<td>ip dst-address</td>
<td>915</td>
</tr>
<tr>
<td>ip error</td>
<td>917</td>
</tr>
<tr>
<td>ip protocol</td>
<td>918</td>
</tr>
<tr>
<td>ip server-domain-name</td>
<td>920</td>
</tr>
<tr>
<td>ip server-ip-address</td>
<td>921</td>
</tr>
<tr>
<td>ip src-address</td>
<td>923</td>
</tr>
<tr>
<td>ip subscriber-ip-address</td>
<td>925</td>
</tr>
<tr>
<td>ip total-length</td>
<td>927</td>
</tr>
<tr>
<td>ip uplink</td>
<td>928</td>
</tr>
<tr>
<td>ip version</td>
<td>929</td>
</tr>
<tr>
<td>mms any-match</td>
<td>930</td>
</tr>
<tr>
<td>mms bcc</td>
<td>931</td>
</tr>
<tr>
<td>mms cc</td>
<td>933</td>
</tr>
</tbody>
</table>
mms content location .................................................. 935
mms content type .................................................. 937
mms downlink .......................................................... 939
mms from ................................................................. 940
mms message-id ...................................................... 942
mms pdu-type .......................................................... 944
mms previous-state .................................................. 946
mms response status ................................................. 948
mms state ............................................................... 949
mms status ............................................................. 951
mms subject ............................................................ 952
mms tid ................................................................. 954
mms to ................................................................. 956
mms uplink ............................................................ 958
mms version ........................................................... 959
multi-line-or all-lines .............................................. 960
p2p any-match ....................................................... 961
p2p behavioral ....................................................... 962
p2p protocol .......................................................... 964
p2p protocol-group ................................................ 972
p2p traffic-type ...................................................... 974
pop3 any-match ....................................................... 976
pop3 command args ................................................. 977
pop3 command id .................................................... 979
pop3 command name ............................................... 980
pop3 mail-size ......................................................... 982
pop3 pdu-length ...................................................... 984
pop3 pdu-type ........................................................ 986
pop3 previous-state ............................................... 987
pop3 reply args ...................................................... 988
pop3 reply id ........................................................ 990
pop3 reply status ................................................... 991
pop3 session-length ............................................... 992
pop3 state ............................................................ 994
pop3 user-name ...................................................... 995
pptp any-match ....................................................... 997
pptp ctrl-msg-type ................................................ 998
pptp gre any-match ................................................ 1000
radius state .......................................................... 1001
rtcp any-match ....................................................... 1002
rtcp jitter ............................................................. 1003
rtcp parent/proto ................................................... 1004
rtcp pdu-length ...................................................... 1005
rtcp rtsp-id .......................................................... 1006
rtcp session-length ................................................ 1008
rtcp uri ............................................................... 1009
rtp any-match ......................................................... 1011
rtp parent/proto ..................................................... 1012
rtp pdu-length ....................................................... 1013
rtp rtsp-id ........................................................... 1014
rtp session-length .................................................. 1016
rtp uri ................................................................. 1017
rtsp any-match ....................................................... 1019
rtsp content length ................................................ 1020
<table>
<thead>
<tr>
<th>Protocol</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>rtsp content type</td>
<td>1021</td>
</tr>
<tr>
<td>rtsp date</td>
<td>1023</td>
</tr>
<tr>
<td>rtsp previous-state</td>
<td>1025</td>
</tr>
<tr>
<td>rtsp reply code</td>
<td>1026</td>
</tr>
<tr>
<td>rtsp request method</td>
<td>1027</td>
</tr>
<tr>
<td>rtsp request packet</td>
<td>1029</td>
</tr>
<tr>
<td>rtsp rtp-seq</td>
<td>1030</td>
</tr>
<tr>
<td>rtsp rtp-time</td>
<td>1031</td>
</tr>
<tr>
<td>rtsp rtp-uri</td>
<td>1032</td>
</tr>
<tr>
<td>rtsp session-id</td>
<td>1034</td>
</tr>
<tr>
<td>rtsp session-length</td>
<td>1036</td>
</tr>
<tr>
<td>rtsp state</td>
<td>1037</td>
</tr>
<tr>
<td>rtsp uri</td>
<td>1038</td>
</tr>
<tr>
<td>rtsp uri sub-part</td>
<td>1041</td>
</tr>
<tr>
<td>rtsp user-agent</td>
<td>1043</td>
</tr>
<tr>
<td>rtsp-stream any-match</td>
<td>1045</td>
</tr>
<tr>
<td>rtsp-stream first-setup-url</td>
<td>1046</td>
</tr>
<tr>
<td>rule-application</td>
<td>1049</td>
</tr>
<tr>
<td>sdp any-match</td>
<td>1051</td>
</tr>
<tr>
<td>sdp connection-ip-address</td>
<td>1052</td>
</tr>
<tr>
<td>sdp media-audio-port</td>
<td>1053</td>
</tr>
<tr>
<td>sdp media-video-port</td>
<td>1054</td>
</tr>
<tr>
<td>sdp uplink</td>
<td>1055</td>
</tr>
<tr>
<td>secure-http any-match</td>
<td>1056</td>
</tr>
<tr>
<td>secure-http uplink</td>
<td>1057</td>
</tr>
<tr>
<td>sip any-match</td>
<td>1058</td>
</tr>
<tr>
<td>sip call-id</td>
<td>1059</td>
</tr>
<tr>
<td>sip content-length</td>
<td>1061</td>
</tr>
<tr>
<td>sip content type</td>
<td>1062</td>
</tr>
<tr>
<td>sip from</td>
<td>1064</td>
</tr>
<tr>
<td>sip previous-state</td>
<td>1066</td>
</tr>
<tr>
<td>sip reply code</td>
<td>1067</td>
</tr>
<tr>
<td>sip request method</td>
<td>1068</td>
</tr>
<tr>
<td>sip request packet</td>
<td>1069</td>
</tr>
<tr>
<td>sip state</td>
<td>1070</td>
</tr>
<tr>
<td>sip to</td>
<td>1071</td>
</tr>
<tr>
<td>sip uri</td>
<td>1073</td>
</tr>
<tr>
<td>smtp any-match</td>
<td>1075</td>
</tr>
<tr>
<td>smtp command arguments</td>
<td>1076</td>
</tr>
<tr>
<td>smtp command id</td>
<td>1078</td>
</tr>
<tr>
<td>smtp command name</td>
<td>1079</td>
</tr>
<tr>
<td>smtp mail-size</td>
<td>1081</td>
</tr>
<tr>
<td>smtp pdu-length</td>
<td>1083</td>
</tr>
<tr>
<td>smtp previous-state</td>
<td>1085</td>
</tr>
<tr>
<td>smtp recipient</td>
<td>1086</td>
</tr>
<tr>
<td>smtp reply arguments</td>
<td>1088</td>
</tr>
<tr>
<td>smtp reply id</td>
<td>1090</td>
</tr>
<tr>
<td>smtp reply status</td>
<td>1091</td>
</tr>
<tr>
<td>smtp sender</td>
<td>1092</td>
</tr>
<tr>
<td>smtp session-length</td>
<td>1094</td>
</tr>
<tr>
<td>smtp state</td>
<td>1096</td>
</tr>
<tr>
<td>tcp analyzed out-of-order</td>
<td>1097</td>
</tr>
<tr>
<td>tcp any-match</td>
<td>1099</td>
</tr>
<tr>
<td>tcp connection-initiator</td>
<td>1100</td>
</tr>
</tbody>
</table>
tcp downlink.................................................................1101
tcp dst-port.................................................................1102
tcp duplicate ...............................................................1104
tcp either-port ............................................................1105
tcp error ........................................................................1107
tcp flag .........................................................................1108
tcp initial-handshake-lost ..............................................1110
tcp payload .....................................................................1111
tcp payload-length ........................................................1112
tcp previous-state ..........................................................1113
tcp proxy-prev-state ........................................................1115
tcp proxy-state .................................................................1117
tcp session-length ..........................................................1119
tcp src-port ....................................................................1120
tcp state ........................................................................1122
tcp uplink ......................................................................1124
tethering-detection ........................................................1125
tftp any-match .................................................................1127
tftp data-any-match ........................................................1128
udp any-match .................................................................1129
udp downlink .................................................................1130
udp dst-port ..................................................................1131
udp either-port ..............................................................1133
udp payload starts-with ................................................1135
udp src-port ..................................................................1136
udp uplink ....................................................................1138
wsp any-match ...............................................................1139
wsp content type ..........................................................1140
wsp domain ....................................................................1142
wsp downlink .................................................................1144
wsp first-request-packet .................................................1145
wsp host .......................................................................1146
wsp pdu-length ..............................................................1148
wsp pdu-type ..................................................................1149
wsp previous-state ........................................................1151
wsp reply code ...............................................................1152
wsp session-length ........................................................1153
wsp session-management ..............................................1154
wsp state .....................................................................1156
wsp status .....................................................................1157
wsp tid .........................................................................1158
wsp total-length ............................................................1159
wsp transfer-encoding ....................................................1160
wsp uplink ....................................................................1162
wsp url .........................................................................1163
wsp user-agent ...............................................................1166
wsp x-header .................................................................1168
wtp any-match ...............................................................1170
wtp downlink .................................................................1171
wtp gtr .........................................................................1172
wtp pdu-length ..............................................................1173
wtp pdu-type ..................................................................1174
wtp previous-state ........................................................1176
wtp rid .........................................................................1177
<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>wtp state</td>
<td>1178</td>
</tr>
<tr>
<td>wtp tid</td>
<td>1179</td>
</tr>
<tr>
<td>wtp transaction class</td>
<td>1180</td>
</tr>
<tr>
<td>wtp ttr</td>
<td>1181</td>
</tr>
<tr>
<td>wtp uplink</td>
<td>1182</td>
</tr>
<tr>
<td>www any-match</td>
<td>1183</td>
</tr>
<tr>
<td>www content type</td>
<td>1184</td>
</tr>
<tr>
<td>www domain</td>
<td>1186</td>
</tr>
<tr>
<td>www downlink</td>
<td>1188</td>
</tr>
<tr>
<td>www first-request-packet</td>
<td>1189</td>
</tr>
<tr>
<td>www header-length</td>
<td>1190</td>
</tr>
<tr>
<td>www host</td>
<td>1191</td>
</tr>
<tr>
<td>www payload-length</td>
<td>1193</td>
</tr>
<tr>
<td>www pdu-length</td>
<td>1194</td>
</tr>
<tr>
<td>www previous-state</td>
<td>1195</td>
</tr>
<tr>
<td>www reply code</td>
<td>1196</td>
</tr>
<tr>
<td>www state</td>
<td>1197</td>
</tr>
<tr>
<td>www transfer-encoding</td>
<td>1198</td>
</tr>
<tr>
<td>www url</td>
<td>1200</td>
</tr>
</tbody>
</table>

ACS Timedef Configuration Mode Commands ....................................... 1203

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>end</td>
<td>1204</td>
</tr>
<tr>
<td>exit</td>
<td>1205</td>
</tr>
<tr>
<td>start</td>
<td>1206</td>
</tr>
</tbody>
</table>

ACS x-Header Format Configuration Mode Commands ............................ 1209

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>end</td>
<td>1210</td>
</tr>
<tr>
<td>exit</td>
<td>1211</td>
</tr>
<tr>
<td>insert</td>
<td>1212</td>
</tr>
</tbody>
</table>

ALCAP Configuration Mode Commands ............................................ 1215

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>aal2-node</td>
<td>1216</td>
</tr>
<tr>
<td>aal2-route</td>
<td>1218</td>
</tr>
<tr>
<td>associate</td>
<td>1220</td>
</tr>
<tr>
<td>end</td>
<td>1221</td>
</tr>
<tr>
<td>exit</td>
<td>1222</td>
</tr>
<tr>
<td>maximum reset-retransmission</td>
<td>1223</td>
</tr>
<tr>
<td>self-point-code</td>
<td>1224</td>
</tr>
<tr>
<td>timeout alicap</td>
<td>1225</td>
</tr>
<tr>
<td>timeout stc</td>
<td>1228</td>
</tr>
</tbody>
</table>

APN Configuration Mode Commands .............................................. 1231

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>aaa</td>
<td>1232</td>
</tr>
<tr>
<td>access-link</td>
<td>1234</td>
</tr>
<tr>
<td>accounting-mode</td>
<td>1236</td>
</tr>
<tr>
<td>active-charging bandwidth-policy</td>
<td>1239</td>
</tr>
<tr>
<td>active-charging link-monitor tcp</td>
<td>1240</td>
</tr>
<tr>
<td>active-charging rulebase</td>
<td>1242</td>
</tr>
<tr>
<td>active-charging rulebase-list</td>
<td>1243</td>
</tr>
<tr>
<td>apn-ambr</td>
<td>1244</td>
</tr>
<tr>
<td>associate accounting-policy</td>
<td>1246</td>
</tr>
<tr>
<td>associate qci-qos-mapping</td>
<td>1247</td>
</tr>
<tr>
<td>authentication</td>
<td>1248</td>
</tr>
<tr>
<td>authorize-with-hss</td>
<td>1252</td>
</tr>
<tr>
<td>bearer-control-mode</td>
<td>1254</td>
</tr>
<tr>
<td>cc-home</td>
<td>1256</td>
</tr>
</tbody>
</table>
mediation-device ........................................................................................................... 1338
mobile-ip home-agent ................................................................................................. 1340
mobile-ip min-reg-lifetime-override ........................................................................... 1341
mobile-ip mn-aaa-removal-indication ........................................................................ 1342
mobile-ip mn-ha-hash-algorithm ............................................................................... 1343
mobile-ip mn-ha-shared-key ...................................................................................... 1344
mobile-ip mn-ha-spi ................................................................................................. 1345
mobile-ip required ..................................................................................................... 1346
mobile-ip reverse-tunnel ............................................................................................ 1347
nai-construction ......................................................................................................... 1348
nbns .......................................................................................................................... 1350
network-behind-mobile .............................................................................................. 1351
next-hop-forwarding-address .................................................................................... 1353
npu qos ....................................................................................................................... 1354
outbound .................................................................................................................... 1355
p-cscf ........................................................................................................................ 1357
pco-options ............................................................................................................... 1359
pdn-behavior ............................................................................................................. 1361
pdp-type .................................................................................................................... 1362
permission .................................................................................................................. 1364
policy ........................................................................................................................... 1365
ppp ............................................................................................................................... 1367
proxy-mip .................................................................................................................... 1369
qos negotiate-limit .................................................................................................... 1371
qos rate-limit ............................................................................................................. 1374
qos-renegotiate ......................................................................................................... 1377
qos traffic-police ........................................................................................................ 1378
radius ........................................................................................................................ 1379
radius group ............................................................................................................... 1380
radius returned-framed-ip-address .......................................................................... 1381
radius returned-username ......................................................................................... 1382
restriction-value ........................................................................................................ 1384
secondary ip pool ....................................................................................................... 1386
selection-mode .......................................................................................................... 1387
timeout ........................................................................................................................ 1388
timeout bearer-inactivity ............................................................................................ 1391
timeout emergency-inactivity .................................................................................... 1393
timeout idle .................................................................................................................. 1394
timeout idle micro-checkpoint-periodicity ................................................................ 1395
timeout long-duration ................................................................................................ 1397
tpo policy .................................................................................................................... 1399
tunnel address-policy ................................................................................................. 1400
tunnel gre .................................................................................................................... 1402
tunnel ipip .................................................................................................................... 1404
tunnel ipsec ................................................................................................................ 1406
tunnel l2tp .................................................................................................................. 1407
virtual-apn gdcr .......................................................................................................... 1410
virtual-apn preference ............................................................................................... 1411

APN Profile Configuration Mode .................................................................................. 1417

address-resolution-mode ........................................................................................... 1418
apn-resolve-dns-query ............................................................................................... 1419
associate sgw-paging-profile .................................................................................... 1420
cc ................................................................................................................................. 1421
dedicated-bearers ........................................................................................................ 1423
<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>description</td>
<td>1424</td>
</tr>
<tr>
<td>direct-tunnel</td>
<td>1425</td>
</tr>
<tr>
<td>dns-extn</td>
<td>1426</td>
</tr>
<tr>
<td>end</td>
<td>1428</td>
</tr>
<tr>
<td>exit</td>
<td>1429</td>
</tr>
<tr>
<td>gateway-address</td>
<td>1430</td>
</tr>
<tr>
<td>gtp</td>
<td>1432</td>
</tr>
<tr>
<td>idle-mode-acl</td>
<td>1434</td>
</tr>
<tr>
<td>ip</td>
<td>1435</td>
</tr>
<tr>
<td>isr-sequential-paging</td>
<td>1438</td>
</tr>
<tr>
<td>ntsf</td>
<td>1439</td>
</tr>
<tr>
<td>overcharge-protection</td>
<td>1441</td>
</tr>
<tr>
<td>pdp-data-inactivity</td>
<td>1443</td>
</tr>
<tr>
<td>pdp-type-ipv4v6-override</td>
<td>1445</td>
</tr>
<tr>
<td>pgw-address</td>
<td>1446</td>
</tr>
<tr>
<td>qos apn-ambr</td>
<td>1448</td>
</tr>
<tr>
<td>qos class</td>
<td>1449</td>
</tr>
<tr>
<td>qos dedicated-bearer</td>
<td>1456</td>
</tr>
<tr>
<td>qos default-bearer</td>
<td>1457</td>
</tr>
<tr>
<td>qos pgw-upgrade</td>
<td>1459</td>
</tr>
<tr>
<td>qos prefer-as-cap</td>
<td>1461</td>
</tr>
<tr>
<td>qos rate-limit direction</td>
<td>1463</td>
</tr>
<tr>
<td>ranap allocation-retention-priority-ie</td>
<td>1467</td>
</tr>
<tr>
<td>restrict access-type</td>
<td>1469</td>
</tr>
</tbody>
</table>

**APN Remap Table Configuration Mode**

- apn-remap
- apn-selection-default
- blank-apn
- cc
- description
- end
- exit
- wildcard-apn

**ATM Port Configuration Mode Commands**

- clock-source
- description
- end
- exit
- line-timing
- loopback
- preferred slot
- pvc
- shutdown
- smtp trap link-status
- threshold high-activity
- threshold monitoring
- threshold rx-utilization
- threshold tx-utilization
- toh-sdfs

**BFD Configuration Mode Commands**

- bfd multihop-peer
- bfd nbr-group-name
echo ........................................................................................................... 1514
end ............................................................................................................. 1515
exit .............................................................................................................. 1516
slow-timers ................................................................................................. 1517

BGP Address-Family (IPv4/IPv6) Configuration Mode Commands ........................................................................... 1519
end ............................................................................................................. 1520
exit .............................................................................................................. 1521
maximum-paths ......................................................................................... 1522
neighbor .................................................................................................... 1523
network ...................................................................................................... 1527
redistribute ............................................................................................... 1528

BGP Address-Family (VPNv4/VPNv6) Configuration Mode Commands ................................................................. 1531
end ............................................................................................................. 1532
exit .............................................................................................................. 1533
neighbor .................................................................................................... 1534

BGP Address-Family (VRF) Configuration Mode Commands ...................................................................................... 1537
end ............................................................................................................. 1538
exit .............................................................................................................. 1539
neighbor .................................................................................................... 1540
redistribute ............................................................................................... 1544

BGP Configuration Mode Commands ......................................................................................................................... 1547
accept-zero-as-rd ....................................................................................... 1548
address-family ipv4 .................................................................................... 1549
address-family ipv6 .................................................................................... 1551
address-family vpnv4 ................................................................................ 1552
address-family vpnv6 ................................................................................ 1553
bgp ................................................................................................................ 1554
distance ..................................................................................................... 1555
end ............................................................................................................. 1557
enforce-first-as .......................................................................................... 1558
exit .............................................................................................................. 1559
ip vrf .......................................................................................................... 1560
maximum-paths ......................................................................................... 1561
neighbor .................................................................................................... 1562
network ...................................................................................................... 1566
redistribute ............................................................................................... 1567
router-id .................................................................................................... 1569
scan-time ................................................................................................... 1570
timers ......................................................................................................... 1571

BGP IP VRF Configuration Mode Commands ........................................................................................................... 1573
end ............................................................................................................. 1574
exit .............................................................................................................. 1575
route-distinguisher ..................................................................................... 1576
route-target ............................................................................................... 1577

BITS Port Configuration Mode Commands ............................................................................................................. 1579
default ........................................................................................................... 1580
description ................................................................................................. 1581
end ............................................................................................................. 1582
exit .............................................................................................................. 1583
mode ............................................................................................................ 1584
preferred slot ............................................................................................ 1585
<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>recover</td>
<td>1586</td>
</tr>
<tr>
<td>shutdown</td>
<td>1588</td>
</tr>
<tr>
<td>snmp trap link-status</td>
<td>1589</td>
</tr>
<tr>
<td><strong>BMSC Profile Configuration Mode Commands</strong></td>
<td><strong>1591</strong></td>
</tr>
<tr>
<td>end</td>
<td>1592</td>
</tr>
<tr>
<td>exit</td>
<td>1593</td>
</tr>
<tr>
<td>gmb diameter dictionary</td>
<td>1594</td>
</tr>
<tr>
<td>gmb diameter endpoint</td>
<td>1595</td>
</tr>
<tr>
<td>gmb diameter peer-select</td>
<td>1596</td>
</tr>
<tr>
<td>gmb user-data</td>
<td>1598</td>
</tr>
<tr>
<td><strong>Bulk Statistics Configuration Mode Commands</strong></td>
<td><strong>1601</strong></td>
</tr>
<tr>
<td>Overview</td>
<td>1602</td>
</tr>
<tr>
<td>Schema Format String Syntax</td>
<td>1602</td>
</tr>
<tr>
<td>Schema Format String Length</td>
<td>1602</td>
</tr>
<tr>
<td>Common Statistics</td>
<td>1602</td>
</tr>
<tr>
<td>aal2 schema</td>
<td>1603</td>
</tr>
<tr>
<td>alcap schema</td>
<td>1605</td>
</tr>
<tr>
<td>apn schema</td>
<td>1607</td>
</tr>
<tr>
<td>asngw schema</td>
<td>1609</td>
</tr>
<tr>
<td>bcmcs schema</td>
<td>1611</td>
</tr>
<tr>
<td>card schema</td>
<td>1613</td>
</tr>
<tr>
<td>context schema</td>
<td>1615</td>
</tr>
<tr>
<td>cscf schema</td>
<td>1617</td>
</tr>
<tr>
<td>cs-network-ranap schema</td>
<td>1619</td>
</tr>
<tr>
<td>cs-network-rtp schema</td>
<td>1621</td>
</tr>
<tr>
<td>cs-network-scpc schema</td>
<td>1623</td>
</tr>
<tr>
<td>dcca schema</td>
<td>1625</td>
</tr>
<tr>
<td>dcca-group schema</td>
<td>1626</td>
</tr>
<tr>
<td>default</td>
<td>1627</td>
</tr>
<tr>
<td>diameter-acct schema</td>
<td>1629</td>
</tr>
<tr>
<td>diameter-auth schema</td>
<td>1630</td>
</tr>
<tr>
<td>dlci-util schema</td>
<td>1631</td>
</tr>
<tr>
<td>d pca schema</td>
<td>1633</td>
</tr>
<tr>
<td>ecs schema</td>
<td>1634</td>
</tr>
<tr>
<td>egtpc schema</td>
<td>1635</td>
</tr>
<tr>
<td>end</td>
<td>1637</td>
</tr>
<tr>
<td>exit</td>
<td>1638</td>
</tr>
<tr>
<td>fa schema</td>
<td>1639</td>
</tr>
<tr>
<td>file</td>
<td>1641</td>
</tr>
<tr>
<td>fing schema</td>
<td>1643</td>
</tr>
<tr>
<td>footer</td>
<td>1644</td>
</tr>
<tr>
<td>gather-on-standby</td>
<td>1646</td>
</tr>
<tr>
<td>gprs schema</td>
<td>1647</td>
</tr>
<tr>
<td>gtpc schema</td>
<td>1649</td>
</tr>
<tr>
<td>gtpp schema</td>
<td>1651</td>
</tr>
<tr>
<td>gtpu schema</td>
<td>1653</td>
</tr>
<tr>
<td>ha schema</td>
<td>1655</td>
</tr>
<tr>
<td>header</td>
<td>1657</td>
</tr>
<tr>
<td>hnbw-hnbap schema</td>
<td>1659</td>
</tr>
<tr>
<td>hnbw-hnbap-access-closed schema</td>
<td>1661</td>
</tr>
<tr>
<td>hnbw-hnbap-access-hybrid schema</td>
<td>1663</td>
</tr>
<tr>
<td>hnbw-hnbap-access-open schema</td>
<td>1665</td>
</tr>
<tr>
<td>hnbw-ranap schema</td>
<td>1667</td>
</tr>
</tbody>
</table>
**Contents**

- hnbgw-ranap-access-closed schema ................................................................. 1669
- hnbgw-ranap-access-hybrid schema ................................................................. 1671
- hnbgw-ranap-access-open schema ....................................................................... 1673
- hnbgw-rtp schema ............................................................................................ 1675
- hnbgw-rtp-access-closed schema ........................................................................ 1677
- hnbgw-rtp-access-hybrid schema ........................................................................ 1679
- hnbgw-rtp-access-open schema .......................................................................... 1681
- hnbgw-rua schema ............................................................................................ 1683
- hnbgw-rua-access-closed schema ....................................................................... 1685
- hnbgw-rua-access-hybrid schema ....................................................................... 1687
- hnbgw-rua-access-open schema .......................................................................... 1689
- hnbgw-sctp schema ............................................................................................ 1691
- hsgw schema ...................................................................................................... 1693
- hss schema ........................................................................................................ 1694
- imsa schema ...................................................................................................... 1696
- ippool schema ................................................................................................. 1698
- ipsg schema ....................................................................................................... 1700
- lac schema ........................................................................................................ 1702
- limit .................................................................................................................... 1704
- lma schema ....................................................................................................... 1705
- lns schema ......................................................................................................... 1707
- local-directory .................................................................................................. 1708
- mag schema ...................................................................................................... 1709
- mipv6ha schema ............................................................................................... 1711
- mme schema ..................................................................................................... 1713
- mvs schema ...................................................................................................... 1715
- nat-realm schema .............................................................................................. 1716
- p2p schema ........................................................................................................ 1717
- pcc-af schema ................................................................................................... 1718
- pcc-policy schema ............................................................................................ 1720
- pcc-profile schema .......................................................................................... 1722
- pcc-sp-endpt schema ....................................................................................... 1724
- pcc-service schema .......................................................................................... 1726
- pdf schema ....................................................................................................... 1728
- pgw schema ...................................................................................................... 1730
- port schema ...................................................................................................... 1731
- ppp schema ....................................................................................................... 1733
- ps-network-gtpu schema ................................................................................... 1735
- ps-network-ranap schema ................................................................................ 1737
- ps-network-sccp schema ................................................................................... 1739
- radius schema ................................................................................................... 1741
- radius-group schema ........................................................................................ 1743
- receiver ............................................................................................................. 1745
- remotefile ......................................................................................................... 1747
- rlf schema ........................................................................................................ 1749
- rlf-detailed schema .......................................................................................... 1751
- rp schema ........................................................................................................ 1753
- saegw schema ................................................................................................... 1755
- sample-interval ............................................................................................... 1756
- sccp schema ...................................................................................................... 1757
- schema ............................................................................................................. 1759
- sgs schema ....................................................................................................... 1761
- sgs-vlr schema ................................................................................................. 1763
- sgsw schema ...................................................................................................... 1765

---

Cisco ASR 5x00 Command Line Interface Reference
srsn-core-nw-interface ........................................... 1951
srsn-number ......................................................... 1952
sgtp-service ............................................................ 1953
sms-mo ................................................................. 1954
sms-mt ................................................................. 1956
srns-inter ............................................................... 1958
srns-intra ............................................................... 1960
srvcc exclude-stnsr-nanpi ........................................... 1962
subscriber-control-inactivity ....................................... 1963
super-charger ........................................................... 1965
tau ................................................................. 1966
treat-as-hplmn ........................................................ 1968
vplmn-address .......................................................... 1969
zone-code ............................................................ 1971

Call-Home Configuration Mode ..................................... 1973
activate ............................................................... 1974
alert-group .............................................................. 1975
contact-email-addr ...................................................... 1977
contract-id .............................................................. 1978
customer-id ............................................................. 1979
d ............................................................... 1980
exit ............................................................... 1981
mail-server ............................................................. 1982
phone-number .......................................................... 1983
profile .............................................................. 1984
rate-limit ............................................................... 1985
sender ............................................................. 1986
site-id ............................................................. 1987
street-address ........................................................... 1988

Call-Home Profile Configuration Mode ................................. 1989
active ............................................................... 1990
destination ............................................................. 1991
d ............................................................... 1993
exit ............................................................... 1994
subscribe-to-alert-group .............................................. 1995

CAMEL Service Configuration Mode Commands ...................... 1999
associate-sccp-network ................................................. 2000
d ............................................................... 2001
exit ............................................................... 2002
tcap destination-address .................................................. 2003
timeout .............................................................. 2004

Card Configuration Mode Commands ..................................... 2007
aps .............................................................. 2008
d ............................................................... 2010
exit ............................................................... 2011
framing .............................................................. 2012
header-type ............................................................ 2014
initial-e1-framing ......................................................... 2015
link-aggregation .......................................................... 2016
mode .............................................................. 2018
redundancy ............................................................. 2020
redundant with .......................................................... 2022
CBS Service Configuration Mode Commands ........................................ 2027
bind .................................................................................................. 2028
cbc-address-validation ................................................................. 2029
cbc-server .................................................................................... 2030
end ................................................................................................ 2031
exit ............................................................................................... 2032
sabp timer .................................................................................... 2033
sabp-class2-aggregation .............................................................. 2034
tcp-keepalive ............................................................................... 2035
tcp-mode ..................................................................................... 2036
Channelized Port Configuration Mode Commands ....................... 2037
alarm-disable ............................................................................... 2038
alarm-soak-timer ........................................................................ 2039
clock-source ............................................................................... 2040
description .................................................................................. 2041
dlci ............................................................................................... 2042
end ................................................................................................ 2044
exit ............................................................................................... 2045
frame-relay .................................................................................. 2046
hopath-sdsf ............................................................................... 2048
line-timing .................................................................................. 2049
loopback ..................................................................................... 2050
lopath-sdsf ............................................................................... 2051
path ............................................................................................. 2052
preferred slot ............................................................................. 2056
pwe3-cesopsn ............................................................................. 2057
shutdown ..................................................................................... 2058
snmp trap link-status .................................................................. 2059
threshold high-activity ................................................................. 2060
threshold monitoring ................................................................... 2061
threshold rx-utilization ............................................................... 2063
threshold tx-utilization ............................................................... 2065
toh-sdsf ...................................................................................... 2067
vc-mapping ................................................................................ 2068
Cipher Suite Configuration Mode Commands ............................. 2069
encryption ................................................................................... 2070
end ................................................................................................ 2071
exit ............................................................................................... 2072
hmac ......................................................................................... 2073
key-exchange ............................................................................ 2074
Class-Map Configuration Mode Commands .................................. 2075
end ................................................................................................ 2076
exit ............................................................................................... 2077
match any ................................................................................... 2078
match dst-ip-address ................................................................. 2079
match dst-port-range ............................................................... 2080
match ip-tos ............................................................................... 2081
match ipsec-spi ......................................................................... 2082
match packet-size ...................................................................... 2083
match protocol ......................................................................... 2084
<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>match src-ip-address</td>
<td>2086</td>
</tr>
<tr>
<td>match src-port-range</td>
<td>2087</td>
</tr>
<tr>
<td><strong>CGW Service Configuration Mode Commands</strong></td>
<td><strong>2089</strong></td>
</tr>
<tr>
<td>associate</td>
<td>2090</td>
</tr>
<tr>
<td>bind</td>
<td>2092</td>
</tr>
<tr>
<td>enable-bra-failure-handling</td>
<td>2093</td>
</tr>
<tr>
<td>end</td>
<td>2094</td>
</tr>
<tr>
<td>exit</td>
<td>2095</td>
</tr>
<tr>
<td>reg-lifetime</td>
<td>2096</td>
</tr>
<tr>
<td>revocation</td>
<td>2097</td>
</tr>
<tr>
<td>session-delete-delay</td>
<td>2098</td>
</tr>
<tr>
<td>timestamp-option-validation</td>
<td>2099</td>
</tr>
<tr>
<td>timestamp-replay-protection</td>
<td>2100</td>
</tr>
<tr>
<td><strong>Congestion Action Profile Configuration Mode Commands</strong></td>
<td><strong>2101</strong></td>
</tr>
<tr>
<td>drop</td>
<td>2102</td>
</tr>
<tr>
<td>end</td>
<td>2104</td>
</tr>
<tr>
<td>exclude-emergency-events</td>
<td>2105</td>
</tr>
<tr>
<td>exclude-voice-events</td>
<td>2106</td>
</tr>
<tr>
<td>exit</td>
<td>2107</td>
</tr>
<tr>
<td>none</td>
<td>2108</td>
</tr>
<tr>
<td>reject</td>
<td>2110</td>
</tr>
<tr>
<td>report-overload</td>
<td>2112</td>
</tr>
<tr>
<td><strong>Connected Apps Configuration Mode Commands</strong></td>
<td><strong>2115</strong></td>
</tr>
<tr>
<td>activate</td>
<td>2116</td>
</tr>
<tr>
<td>end</td>
<td>2117</td>
</tr>
<tr>
<td>exit</td>
<td>2118</td>
</tr>
<tr>
<td>ha-chassis-mode</td>
<td>2119</td>
</tr>
<tr>
<td>ha-network-mode</td>
<td>2120</td>
</tr>
<tr>
<td>sess-ip-address</td>
<td>2121</td>
</tr>
<tr>
<td>sess-name</td>
<td>2122</td>
</tr>
<tr>
<td>sess-passwd</td>
<td>2123</td>
</tr>
<tr>
<td>sess-userid</td>
<td>2124</td>
</tr>
<tr>
<td><strong>Content Filtering Policy Configuration Mode Commands</strong></td>
<td><strong>2125</strong></td>
</tr>
<tr>
<td>analyze</td>
<td>2126</td>
</tr>
<tr>
<td>discarded-flow-content-id</td>
<td>2130</td>
</tr>
<tr>
<td>end</td>
<td>2131</td>
</tr>
<tr>
<td>exit</td>
<td>2132</td>
</tr>
<tr>
<td>failure-action</td>
<td>2133</td>
</tr>
<tr>
<td>timeout action</td>
<td>2135</td>
</tr>
<tr>
<td><strong>Content Filtering Server Group Configuration Mode Commands</strong></td>
<td><strong>2137</strong></td>
</tr>
<tr>
<td>connection retry-timeout</td>
<td>2138</td>
</tr>
<tr>
<td>deny-message</td>
<td>2139</td>
</tr>
<tr>
<td>deny-response code</td>
<td>2140</td>
</tr>
<tr>
<td>dictionary</td>
<td>2141</td>
</tr>
<tr>
<td>end</td>
<td>2143</td>
</tr>
<tr>
<td>exit</td>
<td>2144</td>
</tr>
<tr>
<td>failure-action</td>
<td>2145</td>
</tr>
<tr>
<td>icap server</td>
<td>2148</td>
</tr>
<tr>
<td>origin address</td>
<td>2150</td>
</tr>
<tr>
<td>response-timeout</td>
<td>2151</td>
</tr>
<tr>
<td>timeout action</td>
<td>2152</td>
</tr>
</tbody>
</table>
Context Configuration Mode Commands A-D ........................................ 2155

- aaa accounting ................................................................. 2156
- aaa authentication ......................................................... 2158
- aaa constructed-nai ........................................................ 2160
- aaa filter-id rulebase mapping ......................................... 2163
- aaa group ........................................................................ 2164
- aaa nai-policy .................................................................. 2165
- access-list undefined ....................................................... 2167
- administrator ................................................................... 2168
- apn .................................................................................. 2171
- asn-qos-descriptor .......................................................... 2173
- asn-service-profile ......................................................... 2175
- asngw-service ................................................................ 2177
- asnpc-service .................................................................. 2179
- atcf .................................................................................. 2181
- bfd-protocol .................................................................... 2182
- bgp extended-asn-cap ...................................................... 2183
- bmisc-profile .................................................................... 2184
- busyout ip .......................................................................... 2185
- busyout ipv6 ....................................................................... 2187
- cae-group ......................................................................... 2189
- camel-service .................................................................... 2190
- cbs-service ........................................................................ 2191
- cipher-suite ....................................................................... 2192
- class-map .......................................................................... 2193
- closedrp-rp handoff .......................................................... 2195
- config-administrator .......................................................... 2196
- content-filtering ............................................................... 2199
- credit-control-service ......................................................... 2200
- crypto dns-nameresolver .................................................... 2202
- crypto group ...................................................................... 2203
- crypto ipsec transform-set .................................................. 2204
- crypto map .......................................................................... 2206
- crypto template .................................................................. 2208
- cscf access-profile ........................................................... 2210
- cscf acl ............................................................................ 2211
- cscf diameter-selection ...................................................... 2212
- cscf ifc-filter-criteria ......................................................... 2214
- cscf ifc-spt-condition ........................................................ 2216
- cscf ifc-spt-group .............................................................. 2218
- cscf ifc-trigger-point .......................................................... 2220
- cscf isc-template .............................................................. 2222
- cscf last-route-profile ........................................................ 2223
- cscf peer-servers .............................................................. 2225
- cscf peer-servers-group ..................................................... 2227
- cscf policy ......................................................................... 2229
- cscf prefix-table ............................................................... 2231
- cscf routes ......................................................................... 2232
- cscf service ....................................................................... 2233
- cscf session-template ........................................................ 2235
- cscf subdomain-routes ....................................................... 2237
- cscf translation ................................................................. 2238
- cscf urn-service-list .......................................................... 2240
css server ................................................................. 2242
dhcp-client-profile .................................................. 2243
dhcp-server-profile .................................................. 2245
dhcp-service ........................................................... 2247
dhcpv6-service ......................................................... 2249
diameter accounting .................................................. 2251
diameter authentication .............................................. 2254
diameter authentication failure-handling ....................... 2257
diameter dictionary .................................................... 2259
diameter endpoint ...................................................... 2260
diameter sctp ............................................................. 2261
diameter origin ........................................................ 2263
dns-client ............................................................... 2264
domain ................................................................. 2265

Context Configuration Mode Commands E-H .................. 2267
eap-profile .................................................................. 2268
edr-module active-charging-service ............................... 2269
egrp-service ............................................................. 2271
deal ........................................................................... 2273
epg-service .............................................................. 2274
event-notif-endpoint .................................................... 2276
exit ............................................................................ 2278
external-inline-server .................................................. 2279
fa-service .................................................................... 2280
firewall max-associations .......................................... 2282
fng-service ............................................................... 2283
ggsp-service ............................................................ 2284
gprs-service .............................................................. 2286
gs-service ................................................................. 2288
gtpc overload-protection egress .................................... 2290
gtpc overload-protection ingress ................................... 2291
gtp algorithm ............................................................ 2293
gtp attribute ............................................................. 2294
gtpc charging-agent ................................................... 2302
gtp data-request sequence-numbers ............................. 2304
gtpc dead-server suppress-cdr ..................................... 2305
gtpc deadtime .......................................................... 2306
gtpc detect-dead-server .............................................. 2307
gtpc dictionary ......................................................... 2309
gtpc duplicate-hold-time ............................................. 2312
gtpc echo-interval ...................................................... 2313
gtpc egcdn .............................................................. 2315
gtpc error-response .................................................... 2318
gtpc group ............................................................... 2319
gtpc max-cdrs .......................................................... 2321
gtpc max-pdu-size ...................................................... 2323
gtpc max-retries ......................................................... 2325
gtpc node-id ............................................................. 2327
gtpc redirection-allowed ............................................. 2328
gtpc redirection-disallowed ........................................ 2329
gtpc server .............................................................. 2330
gtpc source-port-validation ......................................... 2332
gtpc storage-server .................................................... 2333
gtpc storage-server local file ....................................... 2334
gtpp storage-server max-retries .................................................. 2338
gtpp storage-server mode .......................................................... 2339
gtpp storage-server timeout ....................................................... 2341
gtpp suppress-cdrs zero-volume ................................................. 2342
gtpp suppress-cdrs zero-volume-and-duration ............................... 2344
gtpp timeout ........................................................................... 2345
gtpp trigger .............................................................................. 2346
gtpp transport-layer .................................................................. 2347
gtpu-service ............................................................................. 2348
ha-service ............................................................................... 2350
hnbgw-service ......................................................................... 2352
hsgw-service ............................................................................ 2354
hss-peer-service ........................................................................ 2356

**Context Configuration Mode Commands I-M** ............................ 2359
ikev1 disable-initial-contact ....................................................... 2360
ikev1 disable-phase1-rekey .......................................................... 2361
ikev1 keepalive dpd ................................................................. 2362
ikev1 policy .............................................................................. 2364
ikev2-ikesa .............................................................................. 2365
ims-auth-service ....................................................................... 2367
ims-sh-service ......................................................................... 2369
inspector .................................................................................. 2370
interface .................................................................................. 2373
ip access-group ........................................................................ 2375
ip access-list ............................................................................ 2377
ip arp .......................................................................................... 2379
ip as-path access-list ................................................................ 2381
ip dns-proxy source-address ....................................................... 2382
ip domain-lookup ..................................................................... 2383
ip domain-name ....................................................................... 2384
ip forward .................................................................................. 2385
ip guarantee .............................................................................. 2386
ip identification packet-size-threshold ...................................... 2387
ip igmp profile ......................................................................... 2388
ip localhost .............................................................................. 2389
ip name-servers ....................................................................... 2390
ip pool ....................................................................................... 2392
ip prefix-list ............................................................................ 2404
ip prefix-list sequence-number .................................................. 2406
ip route ...................................................................................... 2407
ip routing maximum-paths ......................................................... 2410
ip routing overlap-pool .............................................................. 2411
ip vrf ......................................................................................... 2412
ip vrf-list .................................................................................. 2414
ipms ......................................................................................... 2415
ipsec replay .............................................................................. 2416
ipsec transform-set ................................................................... 2417
ipsg-service .............................................................................. 2418
ipv6 access-group ..................................................................... 2419
ipv6 access-list ....................................................................... 2420
ipv6 dns-proxy ......................................................................... 2421
ipv6 neighbor ........................................................................... 2422
ipv6 pool .................................................................................. 2423
ipv6 prefix-list ........................................................................ 2424
ipv6 prefix-list ........................................................................ 2428
Context Configuration Mode Commands N-R

nw-reachability server ............................................. 2474
network-requested-pdp-context activate ......................... 2476
network-requested-pdp-context gsn-map .......................... 2478
network-requested-pdp-context hold-down-time ................ 2480
network-requested-pdp-context interval ......................... 2481
network-requested-pdp-context sgsn-cache-time ............... 2482
operator ......................................................... 2483
optimize pdn inter-service-handoff ............................. 2486
pcc-af-service ............................................... 2487
pcc-policy-service ............................................ 2489
pcc-service .................................................. 2491
pcc-sp-endpoint ............................................. 2493
pdg-service .................................................. 2495
pdf-service .................................................. 2496
pdsn-service .................................................. 2497
pgw-service .................................................. 2499
pilot-packet .................................................. 2501
policy ......................................................... 2503
policy-group .................................................. 2504
policy-map .................................................... 2505
ppp .......................................................... 2506
ppp magic-number ............................................... 2511
ppp statistics .................................................. 2512
proxy-dns intercept-list ....................................... 2514
radius accounting .......................................................... 2516
radius accounting algorithm ........................................... 2519
radius accounting apn-to-be-included ................................. 2521
radius accounting billing-version ..................................... 2522
radius accounting gtp trigger-policy ................................. 2523
radius accounting ha policy ............................................ 2524
radius accounting interim volume .................................... 2525
radius accounting ip remote-address ................................ 2527
radius accounting keepalive ............................................ 2528
radius accounting rp .................................................... 2530
radius accounting server .............................................. 2533
radius algorithm ................................................................ 2536
radius allow .................................................................. 2537
radius attribute .............................................................. 2538
radius authenticate null-username ..................................... 2540
radius authenticate apn-to-be-included ............................... 2541
radius authenticator-validation .......................................... 2542
radius change-authorize-nas-ip .......................................... 2543
radius charging .............................................................. 2546
radius charging accounting algorithm ............................... 2548
radius charging accounting server .................................... 2549
radius charging algorithm ............................................... 2551
radius charging server .................................................... 2552
radius deadtime ................................................................ 2554
radius detect-dead-server ................................................ 2555
radius dictionary ........................................................... 2557
radius group .................................................................. 2559
radius ip vrf ................................................................. 2560
radius keepalive ................................................................ 2562
radius max-outstanding .................................................... 2564
radius max-retries .......................................................... 2565
radius max-transmissions ................................................ 2566
radius mediation-device .................................................... 2567
radius probe-interval ....................................................... 2568
radius probe-max-retries .................................................. 2569
radius probe-message ...................................................... 2570
radius probe-timeout ....................................................... 2571
radius server .................................................................. 2572
radius strip-domain .......................................................... 2575
radius timeout ............................................................... 2576
radius trigger ................................................................. 2577
remote-server-list ........................................................... 2579
route-access-list extended ............................................... 2580
route-access-list named .................................................. 2582
route-access-list standard ............................................... 2584
route-map ..................................................................... 2586
router ........................................................................... 2588

**Context Configuration Mode Commands S-Z** .......................... 2591

saegw-service ............................................................... 2592
server ........................................................................... 2594
service-redundancy-protocol ............................................ 2596
session-event-module ....................................................... 2597
gsnn-service ................................................................. 2598
sgs-service ..................................................................... 2600
Credit Control Configuration Mode Commands ........................................... 2629

apn-name-to-be-included ................................................................. 2630
app-level-retransmission ............................................................... 2631
associate .................................................................................. 2632
diameter dictionary .................................................................. 2634
diameter disable-final-reporting-in-ccru ................................ 2636
diameter dynamic-rules request-quota .......................................... 2637
diameter enable-quota-retry ......................................................... 2638
diameter exclude-msc-in-ccr-terminate ....................................... 2639
diameter fui-redirected-flow ......................................................... 2640
diameter gsu-with-only-infinite-quota .......................................... 2641
diameter ignore-returned-rulebase-id ........................................... 2642
diameter ignore-service-id ............................................................ 2643
diameter mscc-final-unit-action terminate ................................. 2644
diameter mscc-per-ccr-update ....................................................... 2646
diameter origin host .................................................................. 2647
diameter origin endpoint ............................................................... 2648
diameter peer-select ................................................................. 2649
diameter pending-timeout .......................................................... 2652
diameter reauth-blacklisted-content ........................................... 2654
diameter redirect-url-token ........................................................ 2656
diameter result-code ................................................................ 2658
diameter send-ccr ..................................................................... 2660
diameter service-context-id ........................................................... 2661
diameter session failover ............................................................. 2662
diameter update-dictionary-avps ............................................... 2663
end ............................................................................................. 2664
event-based-session ................................................................. 2665
exit ............................................................................................. 2667
failure-handling ........................................................................ 2668
imsi-imeisv-encode-format ....................................................... 2672
mode ......................................................................................... 2673
pending-traffic-treatment ............................................................ 2674
quota ......................................................................................... 2676
quota request-trigger ............................................................... 2677
quota time-threshold ................................................................. 2678
quota units-threshold ................................................................. 2679
quota volume-threshold ............................................................. 2680
radius usage-reporting-algorithm ............................................... 2681
redirect-indicator-received ................................................................. 2682
redirect-require-user-agent .............................................................. 2683
servers-unreachable ......................................................................... 2684
subscription-id service-type ............................................................... 2689
timestamp-rounding .......................................................................... 2691
trigger type ......................................................................................... 2692
usage-reporting .................................................................................. 2694

Crypto Group Configuration Mode Commands ..................................... 2695
end ....................................................................................................... 2696
exit ....................................................................................................... 2697
match address ...................................................................................... 2698
match ip pool ....................................................................................... 2700
switchover ............................................................................................ 2702

Crypto IPSec Transform Set Configuration Mode Commands .............. 2705
end ....................................................................................................... 2706
exit ....................................................................................................... 2707
mode ..................................................................................................... 2708

Crypto Map IKEv2-IPv4 Configuration Mode Commands ..................... 2709
allow-cert-enc cert-hash-url ................................................................. 2710
authentication ...................................................................................... 2711
blacklist ................................................................................................. 2713
certificate list ....................................................................................... 2714
cryptocurrency list ............................................................................... 2715
certificate ............................................................................................. 2717
control-dont-fragment ........................................................................ 2718
end ....................................................................................................... 2719
exit ....................................................................................................... 2720
ikev2-ikesa .......................................................................................... 2721
keepalive .............................................................................................. 2724
match ..................................................................................................... 2725
natt ......................................................................................................... 2727
ocsp ....................................................................................................... 2728
payload ................................................................................................. 2730
peer ......................................................................................................... 2732
remot-secret-list .................................................................................. 2734
whitelist ............................................................................................... 2735

Crypto Map IKEv2-IPv4 Payload Configuration Mode Commands .......... 2737
end ....................................................................................................... 2738
exit ....................................................................................................... 2739
ipse ........................................................................................................ 2740
lifetime ................................................................................................ 2741
rekey ..................................................................................................... 2743

Crypto Map IKEv2-IPv6 Configuration Mode Commands ...................... 2745
allow-cert-enc cert-hash-url ................................................................. 2746
authentication ...................................................................................... 2747
blacklist ................................................................................................. 2749
certificate list ....................................................................................... 2750
cryptocurrency list ............................................................................... 2751
certificate ............................................................................................. 2753
control-dont-fragment ........................................................................ 2754
end ....................................................................................................... 2755
<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>exit</td>
<td>2756</td>
</tr>
<tr>
<td>ikev2-ikesa</td>
<td>2757</td>
</tr>
<tr>
<td>keepalive</td>
<td>2759</td>
</tr>
<tr>
<td>match</td>
<td>2760</td>
</tr>
<tr>
<td>ocsx</td>
<td>2762</td>
</tr>
<tr>
<td>payload</td>
<td>2764</td>
</tr>
<tr>
<td>peer</td>
<td>2766</td>
</tr>
<tr>
<td>remote-secret-list</td>
<td>2768</td>
</tr>
<tr>
<td>whitelist</td>
<td>2769</td>
</tr>
<tr>
<td><strong>Crypto Map IKEv2-IPv6 Payload Configuration Mode Commands</strong></td>
<td>2771</td>
</tr>
<tr>
<td>end</td>
<td>2772</td>
</tr>
<tr>
<td>exit</td>
<td>2773</td>
</tr>
<tr>
<td>ipsec</td>
<td>2774</td>
</tr>
<tr>
<td>lifetime</td>
<td>2776</td>
</tr>
<tr>
<td>rekey</td>
<td>2778</td>
</tr>
<tr>
<td><strong>Crypto Map IPSec Dynamic Configuration Mode Commands</strong></td>
<td>2781</td>
</tr>
<tr>
<td>end</td>
<td>2782</td>
</tr>
<tr>
<td>exit</td>
<td>2783</td>
</tr>
<tr>
<td>set</td>
<td>2784</td>
</tr>
<tr>
<td><strong>Crypto Map IPSec IKEv1 Configuration Mode Commands</strong></td>
<td>2787</td>
</tr>
<tr>
<td>end</td>
<td>2788</td>
</tr>
<tr>
<td>exit</td>
<td>2789</td>
</tr>
<tr>
<td>match address</td>
<td>2790</td>
</tr>
<tr>
<td>match crypto group</td>
<td>2792</td>
</tr>
<tr>
<td>match ip pool</td>
<td>2794</td>
</tr>
<tr>
<td>set</td>
<td>2796</td>
</tr>
<tr>
<td><strong>Crypto Map IPSec Manual Configuration Mode Commands</strong></td>
<td>2799</td>
</tr>
<tr>
<td>end</td>
<td>2800</td>
</tr>
<tr>
<td>exit</td>
<td>2801</td>
</tr>
<tr>
<td>match address</td>
<td>2802</td>
</tr>
<tr>
<td>set control-dont-fragment</td>
<td>2804</td>
</tr>
<tr>
<td>set peer</td>
<td>2806</td>
</tr>
<tr>
<td>set session-key</td>
<td>2808</td>
</tr>
<tr>
<td>set transform-set</td>
<td>2811</td>
</tr>
<tr>
<td><strong>Crypto Template Configuration Mode Commands</strong></td>
<td>2813</td>
</tr>
<tr>
<td>allow-cert-enc cert-hash-url</td>
<td>2814</td>
</tr>
<tr>
<td>allow-custom-fqdn-idr</td>
<td>2815</td>
</tr>
<tr>
<td>authentication</td>
<td>2816</td>
</tr>
<tr>
<td>blacklist</td>
<td>2818</td>
</tr>
<tr>
<td>ca-certificate list</td>
<td>2819</td>
</tr>
<tr>
<td>ca-crl list</td>
<td>2820</td>
</tr>
<tr>
<td>certificate</td>
<td>2821</td>
</tr>
<tr>
<td>control-dont-fragment</td>
<td>2822</td>
</tr>
<tr>
<td>default</td>
<td>2823</td>
</tr>
<tr>
<td>dns-handling</td>
<td>2824</td>
</tr>
<tr>
<td>dos cookie-challenge notify-payload</td>
<td>2826</td>
</tr>
<tr>
<td>end</td>
<td>2827</td>
</tr>
<tr>
<td>exit</td>
<td>2828</td>
</tr>
<tr>
<td>identity local</td>
<td>2829</td>
</tr>
<tr>
<td>ikev2-ikesa</td>
<td>2830</td>
</tr>
<tr>
<td>keepalive</td>
<td>2833</td>
</tr>
</tbody>
</table>
CSCF Access Profile Configuration Mode Commands

1. access-security-type
2. authentication
3. diameter-selection
4. end
5. exit
6. pcrr-policy-control
7. sigcomp
8. timeout

CSCF ACL Configuration Mode Commands

1. after
2. before
3. deny
4. end
5. exit
6. permit
7. redirect

CSCF AoR Policy Rules Configuration Mode Commands

1. after
2. aor
3. before
4. end
5. exit

CSCF ATCF-ATGW Configuration Mode Commands

1. call-linger-timer
2. end
3. exit
4. mgmt-uri
5. policy name
6. stn-sr

Crypto Template IKEv2-Dynamic Payload Configuration Mode Commands

1. default
2. end
3. exit
4. ignore-rekeying-requests
5. ip-address-allocation
6. ipsec
7. lifetime
8. maximum-child-sa
9. rekey
10. tsi
11. tsr

Contents
<table>
<thead>
<tr>
<th>Command Group</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCF ATCF-ATGW Policy Configuration Mode Commands</td>
<td>2899</td>
</tr>
<tr>
<td>criteria</td>
<td>2900</td>
</tr>
<tr>
<td>end</td>
<td>2902</td>
</tr>
<tr>
<td>exit</td>
<td>2903</td>
</tr>
<tr>
<td>ps-cs-alerting</td>
<td>2904</td>
</tr>
<tr>
<td>CSCF Charging Configuration Mode Commands</td>
<td>2905</td>
</tr>
<tr>
<td>end</td>
<td>2906</td>
</tr>
<tr>
<td>exclude</td>
<td>2907</td>
</tr>
<tr>
<td>exit</td>
<td>2909</td>
</tr>
<tr>
<td>CSCF Crypto Template Configuration Mode Commands</td>
<td>2911</td>
</tr>
<tr>
<td>end</td>
<td>2912</td>
</tr>
<tr>
<td>exit</td>
<td>2913</td>
</tr>
<tr>
<td>ipsec</td>
<td>2914</td>
</tr>
<tr>
<td>CSCF Diameter Selection Configuration Mode Commands</td>
<td>2915</td>
</tr>
<tr>
<td>aaa-group</td>
<td>2916</td>
</tr>
<tr>
<td>end</td>
<td>2919</td>
</tr>
<tr>
<td>exit</td>
<td>2920</td>
</tr>
<tr>
<td>CSCF EATF Configuration Mode Commands</td>
<td>2921</td>
</tr>
<tr>
<td>e-stn-sr</td>
<td>2922</td>
</tr>
<tr>
<td>end</td>
<td>2923</td>
</tr>
<tr>
<td>exit</td>
<td>2924</td>
</tr>
<tr>
<td>CSCF Emergency-CSCF Configuration Mode Commands</td>
<td>2925</td>
</tr>
<tr>
<td>eatf</td>
<td>2926</td>
</tr>
<tr>
<td>end</td>
<td>2927</td>
</tr>
<tr>
<td>exit</td>
<td>2928</td>
</tr>
<tr>
<td>plani</td>
<td>2929</td>
</tr>
<tr>
<td>privacy</td>
<td>2931</td>
</tr>
<tr>
<td>psap-file</td>
<td>2932</td>
</tr>
<tr>
<td>CSCF Enforce Codec Policy Configuration Mode Commands</td>
<td>2933</td>
</tr>
<tr>
<td>dynamic-codec</td>
<td>2934</td>
</tr>
<tr>
<td>end</td>
<td>2936</td>
</tr>
<tr>
<td>exit</td>
<td>2937</td>
</tr>
<tr>
<td>static-codec</td>
<td>2938</td>
</tr>
<tr>
<td>CSCF IFC SPT Group Mode Commands</td>
<td>2941</td>
</tr>
<tr>
<td>end</td>
<td>2942</td>
</tr>
<tr>
<td>exit</td>
<td>2943</td>
</tr>
<tr>
<td>spt-condition</td>
<td>2944</td>
</tr>
<tr>
<td>CSCF IFC Trigger Point Mode Commands</td>
<td>2945</td>
</tr>
<tr>
<td>end</td>
<td>2946</td>
</tr>
<tr>
<td>exit</td>
<td>2947</td>
</tr>
<tr>
<td>spt-group</td>
<td>2948</td>
</tr>
<tr>
<td>CSCF ISC Template Configuration Mode Commands</td>
<td>2949</td>
</tr>
<tr>
<td>cnsa</td>
<td>2950</td>
</tr>
<tr>
<td>end</td>
<td>2952</td>
</tr>
<tr>
<td>exit</td>
<td>2953</td>
</tr>
<tr>
<td>filter-criteria</td>
<td>2954</td>
</tr>
<tr>
<td>CSCF Last Route Profile Criteria Configuration Mode Commands</td>
<td>2955</td>
</tr>
<tr>
<td>Contents</td>
<td></td>
</tr>
<tr>
<td>---------</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>county-name</td>
<td>2956</td>
</tr>
<tr>
<td>end</td>
<td>2957</td>
</tr>
<tr>
<td>exit</td>
<td>2958</td>
</tr>
<tr>
<td><strong>CSCF NPDB Client Configuration Mode Commands</strong></td>
<td>2959</td>
</tr>
<tr>
<td>bind</td>
<td>2960</td>
</tr>
<tr>
<td>end</td>
<td>2962</td>
</tr>
<tr>
<td>exit</td>
<td>2963</td>
</tr>
<tr>
<td>npdb-primary-server</td>
<td>2964</td>
</tr>
<tr>
<td>npdb-secondary-server</td>
<td>2965</td>
</tr>
<tr>
<td>timeout</td>
<td>2966</td>
</tr>
<tr>
<td><strong>CSCF PCRF-Policy-Control Configuration Mode Commands</strong></td>
<td>2969</td>
</tr>
<tr>
<td>authorization inactive-media</td>
<td>2970</td>
</tr>
<tr>
<td>authorization mediatype</td>
<td>2971</td>
</tr>
<tr>
<td>authorization policy-interworking-failure</td>
<td>2973</td>
</tr>
<tr>
<td>end</td>
<td>2974</td>
</tr>
<tr>
<td>exit</td>
<td>2975</td>
</tr>
<tr>
<td>signaling-bearer-loss</td>
<td>2976</td>
</tr>
<tr>
<td><strong>CSCF Peer Servers Configuration Mode Commands</strong></td>
<td>2979</td>
</tr>
<tr>
<td>end</td>
<td>2980</td>
</tr>
<tr>
<td>exit</td>
<td>2981</td>
</tr>
<tr>
<td>hunting-method</td>
<td>2982</td>
</tr>
<tr>
<td>server</td>
<td>2983</td>
</tr>
<tr>
<td><strong>CSCF Peer Servers Group Configuration Mode Commands</strong></td>
<td>2985</td>
</tr>
<tr>
<td>end</td>
<td>2986</td>
</tr>
<tr>
<td>exit</td>
<td>2987</td>
</tr>
<tr>
<td>peer-servers</td>
<td>2988</td>
</tr>
<tr>
<td><strong>CSCF Peer Server Monitoring Configuration Mode Commands</strong></td>
<td>2989</td>
</tr>
<tr>
<td>dummy-as</td>
<td>2990</td>
</tr>
<tr>
<td>end</td>
<td>2991</td>
</tr>
<tr>
<td>exit</td>
<td>2992</td>
</tr>
<tr>
<td>ims-capable</td>
<td>2993</td>
</tr>
<tr>
<td>lro-selection-profile</td>
<td>2994</td>
</tr>
<tr>
<td>mode</td>
<td>2995</td>
</tr>
<tr>
<td>monitor-status</td>
<td>2996</td>
</tr>
<tr>
<td>nw-session-template</td>
<td>2998</td>
</tr>
<tr>
<td>registration</td>
<td>2999</td>
</tr>
<tr>
<td>tps-rate</td>
<td>3000</td>
</tr>
<tr>
<td><strong>CSCF Policy Configuration Mode Commands</strong></td>
<td>3001</td>
</tr>
<tr>
<td>aor-policy-rules</td>
<td>3002</td>
</tr>
<tr>
<td>end</td>
<td>3003</td>
</tr>
<tr>
<td>exit</td>
<td>3004</td>
</tr>
<tr>
<td>service-policy-rules</td>
<td>3005</td>
</tr>
<tr>
<td><strong>CSCF Policy Rules Configuration Mode Commands</strong></td>
<td>3007</td>
</tr>
<tr>
<td>allow-noauth</td>
<td>3008</td>
</tr>
<tr>
<td>allow-unsecure</td>
<td>3009</td>
</tr>
<tr>
<td>authorization</td>
<td>3010</td>
</tr>
<tr>
<td>end</td>
<td>3012</td>
</tr>
<tr>
<td>enforce-codec-policy</td>
<td>3013</td>
</tr>
<tr>
<td>exit</td>
<td>3014</td>
</tr>
<tr>
<td>max-cscf-concurrent-sessions</td>
<td>3015</td>
</tr>
</tbody>
</table>
CSCF Service Configuration Mode Commands
policy .................................................................................................................. 3016
qos .................................................................................................................. 3018
signalling-bearing-loss .......................................................... 3020
video-sessions ....................................................................................... 3021

CSCF Prefix Table Configuration Mode Commands .................. 3023
delay ........................................................................................................... 3025
exit ............................................................................................................... 3026

CSCF Proxy-CSCF Configuration Mode Commands ............ 3029
allow rfc3261-ua-interworking ...................................................... 3030
atc-atgw ............................................................................................... 3031
core-reg-expiry-time .......................................................... 3032
diameter .................................................................................................. 3033
equipment ............................................................................................... 3034
emergency ............................................................................................... 3035
emergency-call-mode .......................................................... 3036
end ............................................................................................................... 3037
exit ............................................................................................................... 3038
interrogating-cscf-role ............................................................... 3039
message-max-size .............................................................. 3040
network-id ............................................................................................... 3041
originator ................................................................................................. 3042
pcrf-policy-control .................................................................................. 3043
peer-sbc .................................................................................................. 3044
plmn-id ...................................................................................................... 3045
reg-preloaded-route .............................................................................. 3046
reg-service-route .................................................................................. 3047
reliable-prov-resp .................................................................................. 3048
restoration-procedure ........................................................................... 3049
security-parameters ............................................................................ 3050
sigcomp ..................................................................................................... 3051
sip-header ............................................................................................... 3052
sip-param .................................................................................................. 3053
store-session-path .................................................................................. 3054

CSCF Routes Configuration Mode Commands .................. 3057
after ............................................................................................................. 3058
before ........................................................................................................ 3059
end ............................................................................................................... 3060
exit ............................................................................................................... 3061
route .......................................................................................................... 3062

CSCF Security Configuration Mode Commands .................. 3071
auth-failure-weight .................................................................................. 3072
bad-request-weight ................................................................................ 3073
dos-prevention ......................................................................................... 3074
end ............................................................................................................... 3075
exit ............................................................................................................... 3076
forking-contact-limit ............................................................................... 3077
greystlist-duration .................................................................................. 3078
per-aor-failure-limit .............................................................................. 3079
per-ip-failure-limit ................................................................................. 3080
threshold-rate ........................................................................................ 3081

CSCF Service Configuration Mode Commands .................. 3085
RetryAfter-header-value ....................................................................... 3086
CSCF Serving-CSCF Configuration Mode Commands ....................... 3157
  3gpp .............................................................................. 3158
  allow rfc3261-ua-interworking ........................................ 3160
  as-call invite-request-uri update ...................................... 3161
  authentication .......................................................... 3162
  bgcf-proxy ............................................................... 3165
  diversion-info .......................................................... 3166
  end ............................................................................ 3167
  exit ............................................................................ 3168
  forking ....................................................................... 3169
  interrogating-cscf-role ............................................... 3170
  lir-failure .................................................................... 3171
  local-call-features ...................................................... 3172
  network-id .................................................................. 3173
  npdb-client ................................................................... 3174
  policy ........................................................................... 3175
  registration lifetime ..................................................... 3176
  reliable-prov-resp ....................................................... 3178
  server-name .................................................................. 3179
  sfc ............................................................................. 3180
  sip-header insert .......................................................... 3181
  sip-request ..................................................................... 3182
  tas .............................................................................. 3184
  tas-service .................................................................... 3185
  user-authorization ........................................................ 3186

CSCF Session Template Configuration Mode Commands ................. 3187
  end ............................................................................. 3188
  exit ............................................................................. 3189
  inbound-cscf-acl .......................................................... 3190
  outbound-cscf-acl ........................................................ 3191
  policy-profile ............................................................. 3192
  route-list ....................................................................... 3193
  translation-list ............................................................. 3194
  urn-service-list ........................................................... 3195

CSCF Signalling Compression Configuration Mode Commands .......... 3197
  compression-mode ........................................................ 3198
  decompression-memory-size .......................................... 3200
  end ............................................................................. 3201
  exit ............................................................................. 3202
  state-memory-size ........................................................ 3203

CSCF SIP Proxy Configuration Mode Commands ............................ 3205
  as-call ......................................................................... 3206
  authentication ............................................................ 3207
  diversion-info ............................................................. 3209
  emergency ..................................................................... 3210
  end ............................................................................. 3212
  exit ............................................................................. 3213
  registration ................................................................. 3214
  reliable-prov-resp ........................................................ 3216
  sfc .............................................................................. 3217
  sigcomp ....................................................................... 3218
  tas .............................................................................. 3219
<table>
<thead>
<tr>
<th>Commands</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSCF Subdomain-route List Configuration Mode Commands</td>
<td>3221</td>
</tr>
<tr>
<td>CSCF URI Readdress Configuration Mode Commands</td>
<td>3234</td>
</tr>
<tr>
<td>CSCF URI Readdress Configuration Mode Commands</td>
<td>3237</td>
</tr>
<tr>
<td>CSCF URN List Configuration Mode Commands</td>
<td>3243</td>
</tr>
<tr>
<td>DHCP Client Profile Configuration Mode Commands</td>
<td>3247</td>
</tr>
<tr>
<td>DHCP Server Profile Configuration Mode Commands</td>
<td>3255</td>
</tr>
<tr>
<td>DHCP Service Configuration Mode Commands</td>
<td>3263</td>
</tr>
</tbody>
</table>
max-retransmissions .......................................................... 3286
retransmission-timeout ................................................... 3287
T1-threshold .................................................................. 3288
T2-threshold .................................................................. 3289

**DHCPv6 Client Configuration Mode Commands** .................. 3291
deend .............................................................................. 3292
exit ................................................................................. 3293
max-retransmissions .......................................................... 3294
server-dead-time ............................................................. 3295
server-ipv6-address ......................................................... 3296
server-resurrect-time ....................................................... 3298

**DHCPv6 Server Configuration Mode Commands** ................. 3299
deend .............................................................................. 3300
exit ................................................................................. 3301
ipv6 ............................................................................... 3302
preferred-lifetime .............................................................. 3303
prefix-delegation ............................................................... 3304
rebind-time .................................................................... 3305
renew-time ....................................................................... 3306
valid-lifetime .................................................................... 3307

**DHCPv6 Service Configuration Mode Commands** ............... 3309
bind ............................................................................... 3310
deadtime ......................................................................... 3311
detect-dead-server ............................................................ 3313
dhcpv6-client .................................................................. 3315
dhcpv6-server .................................................................. 3316
deend .............................................................................. 3317
exit ................................................................................. 3318
server ............................................................................. 3319

**Diameter Endpoint Configuration Mode Commands** ............. 3321
app-level-retransmission .................................................... 3322
associate ......................................................................... 3324
cea-timeout ....................................................................... 3326
connection retry-timeout ................................................... 3327
connection timeout ............................................................ 3328
destination-host-avp .......................................................... 3329
device-watchdog-request ..................................................... 3331
dpa-timeout ....................................................................... 3332
dscp ............................................................................... 3333
dynamic-peer-discovery ..................................................... 3334
dynamic-peer-failure-retry-count .......................................... 3336
dynamic-peer-realm ............................................................ 3337
dynamic-route .................................................................... 3338
deend .............................................................................. 3339
exit ................................................................................. 3340
load-balancing-algorithm .................................................... 3341
max-outstanding ................................................................. 3342
origin address ................................................................... 3343
origin host ......................................................................... 3344
origin realm ....................................................................... 3346
peer ............................................................................... 3347
peer-backoff-timer ............................................................. 3350
Diameter Failure Handling Template Configuration Mode Commands .................................................. 3367
end .............................................................................................................................................. 3368
exit ............................................................................................................................................ 3369
msg-type .................................................................................................................................... 3370
Diameter Host Select Configuration Mode Commands ................................................................. 3373
end .............................................................................................................................................. 3374
exit ............................................................................................................................................ 3375
host-select row-precedence ........................................................................................................ 3376
host-select table ........................................................................................................................ 3377
DLCI Configuration Mode Commands ......................................................................................... 3381
bind link ....................................................................................................................................... 3382
end .............................................................................................................................................. 3383
exit ............................................................................................................................................ 3384
shaping ......................................................................................................................................... 3385
shutdown ..................................................................................................................................... 3386
DNS Client Configuration Mode Commands ................................................................................. 3387
bind .............................................................................................................................................. 3388
cache algorithm ........................................................................................................................ 3389
cache size ................................................................................................................................... 3390
cache ttl ...................................................................................................................................... 3391
case-sensitive ............................................................................................................................ 3392
end .............................................................................................................................................. 3393
exit ............................................................................................................................................ 3394
resolver ....................................................................................................................................... 3395
round-robin answers .................................................................................................................. 3396
DSCP Template Configuration Mode Commands ........................................................................... 3397
control-packet ........................................................................................................................... 3398
end .............................................................................................................................................. 3400
exit ............................................................................................................................................ 3401
data-packet ................................................................................................................................. 3402
EAP Authentication Configuration Mode Commands ................................................................. 3405
eap-aka .......................................................................................................................................... 3406
eap-gtc .......................................................................................................................................... 3407
eap-md5 .......................................................................................................................................... 3408
end .............................................................................................................................................. 3409
exit ............................................................................................................................................ 3410
EAP Configuration Mode Commands ........................................................................................ 3411
end .............................................................................................................................................. 3412
exit ............................................................................................................................................ 3413
max-retry ..................................................................................................................................... 3414
ip ospf authentication-key .......................................................... 3502
ip ospf authentication-type ......................................................... 3503
ip ospf bfd ........................................................................... 3504
ip ospf cost ......................................................................... 3505
ip ospf dead-interval .............................................................. 3506
ip ospf hello-interval ............................................................. 3507
ip ospf message-digest-key ..................................................... 3508
ip ospf network .................................................................. 3509
ip ospf priority ................................................................. 3511
ip ospf retransmit-interval .................................................... 3512
ip ospf transmit-delay ......................................................... 3513
ipv6 access-group ................................................................ 3514
ipv6 address ....................................................................... 3516
ipv6 ospf ............................................................................ 3517
ipv6 router advertisement ..................................................... 3519
logical-port-statistics ........................................................... 3520
mpls ip ............................................................................ 3521
policy-forward .................................................................. 3522
pool-share-protocol ............................................................ 3524
port-switch-on-L3-fail .......................................................... 3526
vlan-map ........................................................................... 3528

Ethernet Port Configuration Mode Commands ................................ 3529
bind interface .................................................................... 3530
boxertap ............................................................................ 3531
default ............................................................................... 3532
description ...................................................................... 3534
end ...................................................................................... 3535
exit ..................................................................................... 3536
fault-unidirect-mode ........................................................... 3537
flow-control ....................................................................... 3538
ingress-mode .................................................................... 3539
link-aggregation ................................................................. 3540
media .................................................................................. 3543
medium ............................................................................. 3544
preferred slot ................................................................. 3545
shutdown ........................................................................... 3547
snmp trap link-status .......................................................... 3548
srp virtual-mac-address ...................................................... 3549
threshold high-activity .......................................................... 3550
threshold monitoring .......................................................... 3552
threshold rx-utilization ....................................................... 3554
threshold tx-utilization ....................................................... 3556
vlan ................................................................................... 3558

Exec Mode Commands (A-C) ........................................................ 3561
aaa test .............................................................................. 3562
abort ................................................................................. 3564
active-charging service .......................................................... 3565
alarm ............................................................................... 3566
aps ....................................................................................... 3567
autoconfirm .................................................................... 3568
bulkstats force ................................................................. 3570
call-home send ................................................................. 3571
call-home test ................................................................. 3572
card busy-out ................................................................. 3573
card halt ................................................................. 3575
card migrate ............................................................ 3577
card reboot ............................................................. 3577
card restart ............................................................ 3578
card switch ............................................................. 3580
card upgrade ........................................................... 3582
cdr-push ................................................................. 3584
chassis ................................................................. 3586
clear aaa ................................................................. 3587
clear active-charging analyzer statistics ......................... 3588
clear active-charging charging-action statistics ............... 3589
clear active-charging content-filtering server-group statistics 3590
clear active-charging credit-control statistics ................. 3591
clear active-charging dns-learnt-ip-addresses .................. 3592
clear active-charging edr-format statistics ....................... 3593
clear active-charging edr-udr-file statistics ........................ 3594
clear active-charging firewall statistics ......................... 3595
clear active-charging firewall track-list ........................ 3596
clear active-charging fw-and-nat policy statistics ............. 3597
clear active-charging group-of-ruledefs statistics .............. 3598
clear active-charging nat statistics ............................... 3599
clear active-charging regex statistics ............................ 3600
clear active-charging rulebase statistics ........................ 3601
clear active-charging ruledef statistics .......................... 3602
clear active-charging subsystem ................................. 3603
clear active-charging tcp-proxy statistics ....................... 3604
clear active-charging tethering-detection statistics .......... 3605
clear active-charging tpo policy statistics ...................... 3606
clear active-charging tpo profile statistics ........................ 3607
clear active-charging url-blacklisting statistics ............... 3608
clear active-charging video detailed-statistics ................. 3609
clear administrator .................................................... 3610
clear alarm ............................................................. 3611
clear alcap ............................................................. 3612
clear asngw-service .................................................. 3613
clear asnp-c-service .................................................. 3614
clear apn statistics .................................................... 3615
clear bcmcs statistics ................................................ 3616
clear blacklisted-gtpu-bind-address ................................ 3617
clear bssap+ statistics ................................................ 3618
clear bssgp statistics .................................................. 3619
clear bulkstats .......................................................... 3620
clear cae-group statistics server .................................... 3621
clear call-home statistics ............................................ 3622
clear cdr statistics ...................................................... 3623
clear cli history .......................................................... 3624
clear cmp cert-name ................................................... 3625
clear cmp statistics .................................................... 3626
clear config ............................................................. 3627
clear congestion-control statistics .................................. 3628
clear content-filtering category statistics ....................... 3629
clear crash .............................................................. 3630
clear credit-control statistics ....................................... 3631
clear crypto ................................................................. 3643
clear cs-network statistics ............................................ 3645
clear csf service ......................................................... 3646
clear csf sessions ....................................................... 3648
clear csf sip ........................................................... 3649
clear csf subscription .................................................. 3650
clear dhcp statistics ..................................................... 3651
clear dhcpv6 statistics ................................................ 3652
clear diameter aaa-statistics ......................................... 3653
clear diameter route .................................................... 3654
clear diameter statistics ............................................... 3656
clear diameter-service ................................................ 3658
clear dns-client ......................................................... 3660
clear dns-proxy statistics ............................................. 3661
clear dynamic-policy statistics ..................................... 3662
clear egtpc ............................................................... 3664
clear event-notif statistics ............................................ 3666
clear firewall ........................................................... 3667
clear fng-service statistics ........................................... 3668
clear gmb statistics ..................................................... 3669
clear gmm-sm statistics ............................................... 3670
clear gprsns statistics ................................................ 3673
clear gprssf statistics ................................................ 3675
clear gtpc statistics .................................................... 3676
clear gtpo statistics .................................................... 3678
clear gtpo storage-server local file statistics .................. 3679
clear gtpo storage-server statistics ................................. 3680
clear gtpu statistics .................................................... 3681
clear hd-storage-policy ............................................... 3682
clear henbgw-access-service statistics ............................ 3683
clear henbgw-network-service statistics .......................... 3685
clear henbgw sessions .................................................. 3686
clear hnbgw statistics .................................................. 3688
clear hsgw-service ..................................................... 3690
clear hss-peer-service ................................................ 3691
clear ims-authorization ............................................... 3692
clear ims-sh-service statistics ...................................... 3693
clear ip access-group statistics ..................................... 3694
clear ip arp ............................................................. 3695
clear ip bgp peer ......................................................... 3696
clear ip localhosts ....................................................... 3698
clear ip ospf process .................................................... 3699
clear ipne statistics ..................................................... 3700
clear ipsg statistics ..................................................... 3701
clear ipv6 neighbors .................................................... 3702
clear ipv6 ospf process ................................................ 3703
clear l2tp ................................................................. 3704
clear lawful-intercept .................................................. 3706
clear llc statistics ....................................................... 3707
clear lma-service statistics .......................................... 3708
clear local-policy ....................................................... 3709
clear local-user ......................................................... 3710
clear location-service ................................................ 3711
clear mag-service statistics ......................................... 3712
Contents

cli ........................................................................... 3793
clock set ............................................................... 3795
cmp enroll current-cert ........................................ 3796
cmp fetch cert-name ............................................. 3798
cmp initialize ....................................................... 3799
cmp poll ............................................................... 3801
cmp update .......................................................... 3802
commandguard ..................................................... 3804
configure ............................................................. 3805
context ................................................................. 3807
copy .................................................................. 3808
.crash copy ........................................................... 3811
crypto blacklist file update ..................................... 3813
crypto rsa-keygen modulus ..................................... 3814
crypto whitelist file update .................................... 3815
crypto-group ......................................................... 3816

Exec Mode Commands (D-S) .................................................. 3817
debug ................................................................. 3818
debug bfd ............................................................ 3819
debug ip ............................................................... 3820
debug ip bgp ........................................................ 3821
debug ip ospf all ................................................... 3823
debug ip ospf event ............................................... 3824
debug ip ospf ism .................................................. 3826
debug ip ospf lsa .................................................... 3827
debug ip ospf nsm .................................................. 3829
debug ip ospf packet .............................................. 3830
debug ip ospf route ............................................... 3832
debug ip ospf router .............................................. 3833
debug ipv6 ospf all ............................................... 3834
debug ipv6 ospf event ............................................ 3835
debug ipv6 ospf ifsm .............................................. 3836
debug ipv6 ospf lsa ............................................... 3837
debug ipv6 ospf nsm .............................................. 3839
debug ipv6 ospf packet ......................................... 3840
debug ipv6 ospf route ............................................ 3842
default terminal ..................................................... 3843
delete .................................................................. 3844
delete support record .......................................... 3846
dhcp force ............................................................ 3847
dhcp test .............................................................. 3848
diameter disable endpoint ..................................... 3849
diameter enable endpoint ..................................... 3850
diameter reset connection ..................................... 3851
diameter reset route failure .................................. 3852
directory ............................................................... 3854
disable radius ....................................................... 3856
dns-client ............................................................ 3857
egtpc test echo .................................................... 3859
enable radius ....................................................... 3861
exit .................................................................... 3862
filesystem ............................................................ 3863
filesystem synchronize .......................................... 3865
get context-list ..................................................... 3867
<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>get ip</td>
<td>3868</td>
</tr>
<tr>
<td>get ipv6</td>
<td>3870</td>
</tr>
<tr>
<td>get port info</td>
<td>3872</td>
</tr>
<tr>
<td>gtpc test echo</td>
<td>3873</td>
</tr>
<tr>
<td>gtpp test</td>
<td>3874</td>
</tr>
<tr>
<td>gtpu test echo</td>
<td>3877</td>
</tr>
<tr>
<td>gtpv0 test echo</td>
<td>3879</td>
</tr>
<tr>
<td>gtpp test</td>
<td>3880</td>
</tr>
<tr>
<td>gtpp storage-server commit</td>
<td>3881</td>
</tr>
<tr>
<td>gtpp storage-server streaming start</td>
<td>3883</td>
</tr>
<tr>
<td>gtpp interim now</td>
<td>3885</td>
</tr>
<tr>
<td>gtpp interim now active-charging egcdr</td>
<td>3886</td>
</tr>
<tr>
<td>hd raid</td>
<td>3889</td>
</tr>
<tr>
<td>install plugin</td>
<td>3890</td>
</tr>
<tr>
<td>interface</td>
<td>3891</td>
</tr>
<tr>
<td>lawful-interpret</td>
<td>3892</td>
</tr>
<tr>
<td>lawful-interpret packet-cable</td>
<td>3893</td>
</tr>
<tr>
<td>lawful-interpret ssdf</td>
<td>3894</td>
</tr>
<tr>
<td>link-aggregation port switch to</td>
<td>3895</td>
</tr>
<tr>
<td>logging active</td>
<td>3896</td>
</tr>
<tr>
<td>logging filter</td>
<td>3897</td>
</tr>
<tr>
<td>logging trace</td>
<td>3898</td>
</tr>
<tr>
<td>logs checkpoint</td>
<td>3907</td>
</tr>
<tr>
<td>lsp-ping</td>
<td>3909</td>
</tr>
<tr>
<td>lsp-traceroute</td>
<td>3910</td>
</tr>
<tr>
<td>mmdir</td>
<td>3911</td>
</tr>
<tr>
<td>mme disconnect</td>
<td>3912</td>
</tr>
<tr>
<td>mme offload</td>
<td>3913</td>
</tr>
<tr>
<td>mme paging cache clear</td>
<td>3914</td>
</tr>
<tr>
<td>mme relocate-ue imsi</td>
<td>3916</td>
</tr>
<tr>
<td>mme reset</td>
<td>3917</td>
</tr>
<tr>
<td>monitor interface</td>
<td>3918</td>
</tr>
<tr>
<td>monitor protocol</td>
<td>3919</td>
</tr>
<tr>
<td>monitor subscriber</td>
<td>3920</td>
</tr>
<tr>
<td>newcall policy</td>
<td>3924</td>
</tr>
<tr>
<td>password change</td>
<td>3925</td>
</tr>
<tr>
<td>patch plugin</td>
<td>3926</td>
</tr>
<tr>
<td>ping</td>
<td>3927</td>
</tr>
<tr>
<td>ping6</td>
<td>3928</td>
</tr>
<tr>
<td>port switch to</td>
<td>3929</td>
</tr>
<tr>
<td>ppp echo-test</td>
<td>3931</td>
</tr>
<tr>
<td>radius interim accounting now</td>
<td>3932</td>
</tr>
<tr>
<td>radius test</td>
<td>3933</td>
</tr>
<tr>
<td>reload</td>
<td>3934</td>
</tr>
<tr>
<td>rename</td>
<td>3935</td>
</tr>
<tr>
<td>reset alcap-service</td>
<td>3936</td>
</tr>
<tr>
<td>reveal disabled commands</td>
<td>3937</td>
</tr>
<tr>
<td>rlogin</td>
<td>3938</td>
</tr>
<tr>
<td>rmdir</td>
<td>3939</td>
</tr>
<tr>
<td>rollback module</td>
<td>3940</td>
</tr>
<tr>
<td>rotate-hd-file</td>
<td>3941</td>
</tr>
<tr>
<td>save configuration</td>
<td>3942</td>
</tr>
<tr>
<td>save logs</td>
<td>3943</td>
</tr>
<tr>
<td>session trace</td>
<td>3944</td>
</tr>
</tbody>
</table>
session trace signaling ................................................................. 3974
session trace random ................................................................. 3975
setup ................................................................................................ 3977
sgs offload ....................................................................................... 3978
sgs vlr-failure .................................................................................. 3980
sgs vlr-recover .................................................................................. 3982
sgsn clear-detached-subscriptions ..................................................... 3984
sgsn imsimgr ...................................................................................... 3985
sgsn offload ....................................................................................... 3987
sgsn op ............................................................................................... 3990
sgsn retry-unavailable-ggsn ................................................................. 3994
sgtpc test echo sgsn-address ............................................................. 3995
shutdown ......................................................................................... 3996
sleep ................................................................................................. 3997
srp initiate-switchover ...................................................................... 3998
srp reset-auth-probe-fail ................................................................. 3999
srp reset-diameter-fail ................................................................. 4000
srp terminate-post-process ............................................................... 4001
srp validate-configuration ............................................................... 4002
srp validate-switchover ................................................................. 4003
ssh ................................................................................................. 4004
start crypto security-association ......................................................... 4005
system ............................................................................................ 4006

**Exec Mode Commands (T-Z)** ........................................................ 4009

tcpdump kernel ................................................................................. 4010
telnet ................................................................................................. 4011
telnet6 ............................................................................................... 4012
terminal ............................................................................................ 4013
test alarm .......................................................................................... 4014
test ipcf bindmux ............................................................................. 4015
test ipsec tunnel ip-pool .................................................................... 4016
test mobile tunnel .............................................................................. 4017
timestamps ......................................................................................... 4019
traceroute .......................................................................................... 4020
traceroute6 ......................................................................................... 4022
update active-charging ..................................................................... 4024
update ciscf ....................................................................................... 4026
update firewall policy ....................................................................... 4028
update ip access-list ...................................................................... 4029
update ipv6 access-list .................................................................... 4030
update local-user database ............................................................... 4031
update module ................................................................................ 4032
update qos policy map ..................................................................... 4033
update qos tft ................................................................................... 4035
upgrade ............................................................................................ 4036
upgrade content-filtering .................................................................. 4038
upgrade tethering-detection ............................................................. 4039
upgrade url-blacklisting database ...................................................... 4041

**Exec Mode show Commands (A-C)** .............................................. 4043

show aaa ......................................................................................... 4044
show active-charging analyzer statistics ........................................... 4046
show active-charging bandwidth-policy .......................................... 4056
show active-charging charging-action .............................................. 4057
<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>show asnpc-service session counters</td>
<td>4167</td>
</tr>
<tr>
<td>show asnpc-service session counters verbose</td>
<td>4169</td>
</tr>
<tr>
<td>show asnpc-service statistics</td>
<td>4171</td>
</tr>
<tr>
<td>show asnpc-service statistics verbose</td>
<td>4172</td>
</tr>
<tr>
<td>show banner</td>
<td>4174</td>
</tr>
<tr>
<td>show bcmcs counters</td>
<td>4175</td>
</tr>
<tr>
<td>show bcmcs statistics</td>
<td>4176</td>
</tr>
<tr>
<td>show boot</td>
<td>4177</td>
</tr>
<tr>
<td>show bssap+ statistics</td>
<td>4178</td>
</tr>
<tr>
<td>show bssgp statistics</td>
<td>4180</td>
</tr>
<tr>
<td>show bssgp status</td>
<td>4182</td>
</tr>
<tr>
<td>show bulkstats</td>
<td>4183</td>
</tr>
<tr>
<td>show ca-certificate</td>
<td>4188</td>
</tr>
<tr>
<td>show ca-crl</td>
<td>4189</td>
</tr>
<tr>
<td>show call-group server</td>
<td>4190</td>
</tr>
<tr>
<td>show call-control-profile</td>
<td>4191</td>
</tr>
<tr>
<td>show call-home</td>
<td>4193</td>
</tr>
<tr>
<td>show camel-service</td>
<td>4195</td>
</tr>
<tr>
<td>show card</td>
<td>4196</td>
</tr>
<tr>
<td>show cbs counters</td>
<td>4198</td>
</tr>
<tr>
<td>show cbs sessions</td>
<td>4199</td>
</tr>
<tr>
<td>show cbs statistics</td>
<td>4201</td>
</tr>
<tr>
<td>show cbs-service</td>
<td>4203</td>
</tr>
<tr>
<td>show cdr</td>
<td>4204</td>
</tr>
<tr>
<td>show certificate</td>
<td>4205</td>
</tr>
<tr>
<td>show cgw-service</td>
<td>4206</td>
</tr>
<tr>
<td>show cli</td>
<td>4207</td>
</tr>
<tr>
<td>show clock</td>
<td>4208</td>
</tr>
<tr>
<td>show cmp history</td>
<td>4209</td>
</tr>
<tr>
<td>show cmp outstanding-req</td>
<td>4210</td>
</tr>
<tr>
<td>show cmp statistics</td>
<td>4211</td>
</tr>
<tr>
<td>show configuration</td>
<td>4212</td>
</tr>
<tr>
<td>show configuration errors</td>
<td>4216</td>
</tr>
<tr>
<td>show congestion-control</td>
<td>4220</td>
</tr>
<tr>
<td>show connectedapps</td>
<td>4223</td>
</tr>
<tr>
<td>show content-filtering category database</td>
<td>4224</td>
</tr>
<tr>
<td>show content-filtering category policy-id</td>
<td>4226</td>
</tr>
<tr>
<td>show content-filtering category statistics</td>
<td>4227</td>
</tr>
<tr>
<td>show content-filtering category url</td>
<td>4229</td>
</tr>
<tr>
<td>show content-filtering server-group</td>
<td>4231</td>
</tr>
<tr>
<td>show context</td>
<td>4232</td>
</tr>
<tr>
<td>show cpu</td>
<td>4233</td>
</tr>
<tr>
<td>show crash</td>
<td>4235</td>
</tr>
<tr>
<td>show credit-control sessions</td>
<td>4236</td>
</tr>
<tr>
<td>show credit-control statistics</td>
<td>4237</td>
</tr>
<tr>
<td>show crypto blacklist file</td>
<td>4238</td>
</tr>
<tr>
<td>show crypto group</td>
<td>4239</td>
</tr>
<tr>
<td>show crypto ikev1</td>
<td>4241</td>
</tr>
<tr>
<td>show crypto ikev2-ikesa security-associations</td>
<td>4243</td>
</tr>
<tr>
<td>show crypto ikev2-ikesa transform-set</td>
<td>4245</td>
</tr>
<tr>
<td>show crypto ipsec security-associations</td>
<td>4247</td>
</tr>
<tr>
<td>show crypto ipsec transform-set</td>
<td>4250</td>
</tr>
<tr>
<td>show crypto isakmp keys</td>
<td>4252</td>
</tr>
<tr>
<td>show crypto isakmp policy</td>
<td>4253</td>
</tr>
</tbody>
</table>
show crypto isakmp security-associations .................................................. 4254
show crypto managers ............................................................................. 4255
show crypto map ......................................................................................... 4257
show crypto statistics .................................................................................. 4259
show crypto template .................................................................................. 4261
show crypto whitelist file ............................................................................. 4263
show cs-network ........................................................................................... 4264
show cs-network counters ........................................................................... 4265
show cs-network statistics ........................................................................... 4266
show csf ifc .................................................................................................... 4268
show csf nat ................................................................................................... 4269
show csf npdb-servers .................................................................................. 4270
show csf peer-servers .................................................................................. 4271
show csf peer-servers-group ....................................................................... 4273
show csf service ............................................................................................ 4274
show csf sessions .......................................................................................... 4277
show csf sip .................................................................................................... 4280
show csf tcp ................................................................................................... 4282
show css delivery-sequence ....................................................................... 4284
show css server .............................................................................................. 4285
show css service ........................................................................................... 4286

**Exec Mode show Commands (D-G) ............................................................ 4287**
show dhcp .................................................................................................... 4288
show dhcp-service ....................................................................................... 4291
show dhcpv6 .................................................................................................. 4292
show dhcpv6-client-profile ........................................................................ 4294
show dhcpv6-server-profile ....................................................................... 4295
show dhcpv6-service .................................................................................... 4296
show diameter aaa-statistics ....................................................................... 4297
show diameter accounting servers aaa-group .......................................... 4298
show diameter authentication servers aaa-group ..................................... 4299
show diameter dynamic-dictionary ............................................................... 4300
show diameter endpoint ............................................................................. 4302
show diameter endpoints ............................................................................ 4303
show diameter message-queue .................................................................... 4304
show diameter peers .................................................................................... 4306
show diameter route status ......................................................................... 4308
show diameter route table .......................................................................... 4310
show diameter statistics .............................................................................. 4311
show diameter-service ............................................................................... 4312
show dns-client ............................................................................................. 4314
show dynamic-policy statistics ................................................................... 4316
show egtpc peers .......................................................................................... 4318
show egtpc sessions ...................................................................................... 4320
show egtpc statistics .................................................................................... 4322
show egtp-service ........................................................................................ 4325
show epdg-service ......................................................................................... 4326
show event-notif server .............................................................................. 4328
show event-notif statistics ........................................................................... 4329
show external-inline-servers ....................................................................... 4330
show fa-service ............................................................................................. 4331
show fa-spi-list ............................................................................................. 4332
show fans ....................................................................................................... 4333
show file ........................................................................................................ 4334
show firewall flows ................................................................. 4336
show firewall ruledef ............................................................ 4337
show firewall statistics .......................................................... 4338
show fng-service ................................................................. 4339
show fng-service session ....................................................... 4341
show fng-service statistics ..................................................... 4343
show freeze-ptmsi imsi .......................................................... 4344
show ggsn sessmgr ............................................................... 4345
show ggsn-service ............................................................... 4346
show ggsn-service sgsn-table .................................................. 4347
show global-title-translation .................................................. 4348
show gmb statistics .............................................................. 4349
show gmm-sm statistics ........................................................ 4350
show gprsns statistics .......................................................... 4353
show gprsns status .............................................................. 4355
show gprs-service ............................................................... 4356
show gprsssf ..................................................................... 4358
show gs-service ................................................................. 4360
show gtpc ....................................................................... 4361
show gtpc statistics ............................................................. 4363
show gtpp ....................................................................... 4365
show gtpp accounting .......................................................... 4366
show gtpp counters ............................................................. 4367
show gtpp group ................................................................. 4368
show gtpp statistics ............................................................. 4369
show gtpp storage-server ..................................................... 4371
show gtpu ....................................................................... 4373
show gtpu-service ............................................................. 4375

**Exec Mode show Commands (H-L)** .............................................. 4377

show ha-service ............................................................... 4378
show ha-spi-list ............................................................... 4379
show hardware ................................................................. 4380
show hd raid ................................................................... 4382
show hd-storage-policy ....................................................... 4383
show hnbgw ................................................................. 4384
show hnbgw-access-service .................................................. 4386
show hnbgw-network-service .................................................. 4388
show hnbgw access-control-db ............................................. 4390
show hnbgw counters .......................................................... 4391
show hnbgw-global ............................................................ 4392
show hnbgw sessions .......................................................... 4393
show hnbgw statistics hnbgw-service ..................................... 4396
show hnbgw statistics hnbid .................................................. 4398
show hnbgw-service .......................................................... 4400
show hsgw-service ............................................................ 4401
show hss-peer-service ........................................................ 4403
show imei-profile ............................................................. 4405
show ims-authorization policy-control .................................... 4406
show ims-authorization policy-gate ....................................... 4408
show ims-authorization servers ............................................. 4410
show ims-authorization service ............................................. 4411
show ims-authorization sessions ........................................... 4413
show inventory ............................................................... 4415
show ip access-group statistics ............................................. 4416
show ip access-list
show ip arp
show ip as-path-access-list
show ip bgp
show ip igmp group
show ip interface
show ip ipsp
show ip localhosts
show ip ospf
show ip prefix-list
show ip route
show ip route-access-list
show ip static-route
show ip vrf
show ip vrf-list
show ipms status
show ipsg service
show ipsg sessions
show ipsg statistics
show ipv6 access-group statistics
show ipv6 access-list
show ipv6 interface
show ipv6 neighbors
show ipv6 ospf
show ipv6 pool
show ipv6 prefix-list
show ipv6 route
show ipv6 route-access-list
show lups-service
show l2tp sessions
show l2tp statistics
show l2tp tunnels
show lac-service
show lawful-intercept
show lawful-intercept ssdf statistics
show ldap connection all
show leds
show license information
show linecard
show linkmgr
show l1c statistics
show l1c status
show lma-service
show lns-service
show local-policy
show local-user
show location-service
show logging
show logical-port utilization table
show logs
show lte-policy

Exec Mode show Commands (M-P)
show mag-service .............................................................. 4504
show map-service .......................................................... 4506
show map statistics ......................................................... 4507
show maximum-temperatures ........................................... 4508
show mbms bearer-service .............................................. 4509
show mipfa ................................................................ 4511
show mipha ................................................................ 4514
show mipv6ha ................................................................. 4517
show mme-service .......................................................... 4519
show mme-service db record ............................................ 4520
show mme-service db statistics ......................................... 4522
show mme-service enodeb-association .............................. 4523
show mme-service id ....................................................... 4525
show mme-service session ............................................... 4526
show mme-service statistics .......................................... 4529
show module .................................................................. 4531
show mpls cross-connect ................................................ 4532
show mpls fn ................................................................. 4533
show mpls ilm ................................................................. 4534
show mpls idp ................................................................. 4535
show mpls nexthop-label-forwarding-entry ...................... 4537
show mrme-service ........................................................ 4538
show mseg-config .......................................................... 4539
show mseg-service ........................................................ 4540
show multicast-sessions .................................................. 4541
show network-requested-pdp-context ............................... 4544
show network-service-entity ........................................... 4545
show npu error-counters .................................................. 4546
show npu utilization ....................................................... 4547
show ntp .................................................................... 4548
show nw-reachability server ............................................ 4549
show operator-policy ...................................................... 4550
show orbem .................................................................. 4552
show patch progress ........................................................ 4554
show pcc-af service ....................................................... 4555
show pcc-af session ........................................................ 4557
show pcc-policy service .................................................. 4559
show pcc-policy session .................................................. 4561
show pcc-service .......................................................... 4563
show pcc-service session ................................................ 4564
show pcc-service statistics ............................................. 4566
show pcc-sp-endpoint .................................................... 4567
show pcc-sp-endpoint connection ................................... 4569
show pdg-service .......................................................... 4571
show pdg-service statistics ............................................. 4572
show pdf-service .......................................................... 4573
show pdsn-service ........................................................ 4574
show peer-profile .......................................................... 4576
show pgw-service .......................................................... 4578
show plugin .................................................................. 4579
show port .................................................................... 4580
show power .................................................................. 4582
show ppp .................................................................... 4583
show prepaid 3gpp2 ......................................................... 4585
show prepaid wimax ................................................................. 4587
show profile-id-qci-mapping ....................................................... 4589
show ps-network ................................................................. 4590
show ps-network counters ......................................................... 4591
show ps-network statistics ....................................................... 4592

**Exec Mode show Commands (Q-S)** ........................................ 4595

- show qos npu inter-subscriber traffic ................................ 4596
- show radius ........................................................................ 4597
- show radius charging servers ............................................... 4599
- show radius client ............................................................ 4600
- show radius counters .......................................................... 4601
- show resources ................................................................... 4603
- show rf-context-statistics ...................................................... 4604
- show rf-memcache-statistics .................................................. 4606
- show rf-template ............................................................... 4607
- show rohc counters ............................................................ 4608
- show rohc statistics ............................................................. 4610
- show route-map .................................................................. 4612
- show rp .............................................................................. 4613
- show rp service-option ......................................................... 4615
- show rp statistics ............................................................... 4616
- show rsvp counters ............................................................ 4618
- show rsvp statistics ............................................................ 4619
- show saegw-service ............................................................ 4620
- show samog-service ............................................................ 4622
- show sccp-network ............................................................. 4623
- show sccp statistics ............................................................. 4624
- show sctp-param-template .................................................... 4626
- show service all .................................................................. 4627
- show session counters historical .......................................... 4628
- show session counters pcf-summary ...................................... 4631
- show session disconnect-reasons .......................................... 4632
- show session duration ......................................................... 4634
- show session progress ........................................................ 4637
- show session recovery status ............................................... 4640
- show session setuptime ....................................................... 4641
- show session subsystem ...................................................... 4643
- show session trace ............................................................. 4646
- show session-event-record ................................................... 4648
- show sf ........................................................................... 4649
- show sgs-service ............................................................... 4650
- show s4-sgsn statistics ......................................................... 4652
- show sgn fsf-statistics .......................................................... 4653
- show sgn sssmgr ............................................................... 4654
- show sgn-fast-path ............................................................. 4655
- show sgn-map-app ............................................................. 4656
- show sgn-mode ................................................................. 4657
- show sgn-operator-policy ..................................................... 4658
- show sgn-pool ................................................................. 4659
- show sgn-service .............................................................. 4660
- show sgtp-service ............................................................. 4661
- show sgtpc statistics ........................................................... 4663
- show sgtpu statistics ........................................................... 4665
- show sgw-service .............................................................. 4667
show sms statistics
show sndcp statistics
show snmp
show srp
show ss7-routing-domain
show ssh key
show ssl cipher-suite
show ssl connection
show ssl map
show ssl statistics
show subscribers
show subscribers samog-only
show subscribers wsg-service
show super-charger
show supplementary-service statistics
show support collection
show support details
show support record
show system uptime

Exec Mode show Commands (T-Z) ....................................................... 4751

show tacacs ................................................................. 4752
show task ................................................................. 4754
show tcap statistics ...................................................... 4759
show temperature ........................................................ 4760
show terminal ............................................................. 4761
show threshold ........................................................... 4762
show timing ................................................................. 4763
show upgrade .............................................................. 4764
show url-blacklisting database ......................................... 4765
show version ............................................................... 4767
show wsg-lookup .......................................................... 4769
show wsg-service .......................................................... 4770

FA Service Configuration Mode Commands .................................... 4771

advertise ................................................................. 4772
authentication aaa ....................................................... 4774
authentication mn-aaa .................................................. 4775
authentication mn-ha ..................................................... 4777
bind ........................................................................... 4778
challenge-window ........................................................ 4780
default subscriber .......................................................... 4781
dynamic-ha-assignment .................................................. 4782
dynamic-mip-key-update .................................................. 4783
encapsulation allow gre .................................................. 4784
dynamic ................................................................. 4785
exit ........................................................................ 4786
fa-ha-spi ................................................................... 4787
gre ............................................................................ 4787
ha-monitor ................................................................. 4790
idle-timeout-mode .......................................................... 4792
ignore-mip-key-data ....................................................... 4794
ignore-stale-challenge ..................................................... 4795
ip local-port ............................................................... 4797
isakmp .................................................................... 4798
limit-reg-lifetime ................................................................. 4800
max-challenge-len .............................................................. 4801
mn-aaa-removal-indication ................................................... 4802
multiple-reg ........................................................................ 4803
optimize tunnel-reassembly ................................................... 4804
private-address allow-no-reverse-tunnel ................................. 4805
proxy-mip ............................................................................ 4806
reg-timeout ......................................................................... 4809
reverse-tunnel ........................................................................ 4810
revocation ............................................................................... 4811
threshold reg-reply-error ....................................................... 4813
Firewall-and-NAT Action Configuration Mode Commands ............ 4815
end ....................................................................................... 4816
exit ....................................................................................... 4817
flow check-point ................................................................. 4818
Firewall-and-NAT Policy Configuration Mode Commands ............. 4821
access-rule ........................................................................... 4822
end ....................................................................................... 4826
exit ....................................................................................... 4827
firewall dos-protection .......................................................... 4828
firewall flooding ................................................................. 4832
firewall icmp-checksum-error .................................................. 4834
firewall icmp-destination-unreachable-message-threshold .......... 4835
firewall icmp-echo-id-zero ..................................................... 4837
firewall icmp-fsm ............................................................... 4838
firewall ip-reassembly-failure ............................................... 4839
firewall malformed-packets ................................................... 4840
firewall max-ip-packet-size ................................................... 4841
firewall mime-flood ............................................................. 4843
firewall policy ................................................................. 4845
firewall tcp-checksum-error .................................................... 4847
firewall tcp-first-packet-non-syn ......................................... 4848
firewall tcp-fsm ............................................................... 4849
firewall tcp-idle-timeout-action ............................................ 4850
firewall tcp-options-error .................................................... 4851
firewall tcp-partial-connection-timeout .................................. 4852
firewall tcp-reset-message-threshold .................................... 4853
firewall tcp-syn-flood-intercept ............................................. 4854
firewall tcp-syn-with-ecn-cwr .............................................. 4856
firewall udp-checksum-error ............................................... 4857
firewall validate-ip-options .................................................. 4858
nat binding-record ............................................................. 4859
nat check-point-info ............................................................ 4860
nat icsr-flow-recovery ........................................................ 4862
nat policy ............................................................................. 4863
nat private-ip-flow-timeout ................................................... 4865
nat suppress-aaa-update ...................................................... 4866
Firewall-and-NAT Access Ruledef Configuration Mode Commands ..... 4867
bearer 3gpp apn .................................................................. 4868
bearer 3gpp imsi .................................................................. 4870
bearer username .................................................................. 4872
create-log-record ............................................................... 4874
FNG Service Configuration Mode Commands

aaa aggregation .......................... 4911
aaa authentication .......................... 4912
bind .......................................... 4914
default .......................................... 4915
duplicate-session-detection .................. 4916
duplicate-session ............................ 4918
duplicate-session-detection .......................... 4919
exit .......................................... 4920
ip source-violation .......................... 4921
setup-timeout ................................ 4923

FTP Configuration Mode Commands ................. 4925

accounting ................................ 4932
associate gtpu-service .................. 4933
associate peer-map .......................... 4934
associate pgw-service .................. 4935
authorize-with-hss .......................... 4936
bind .......................................... 4937
customer-service ................................ 4938
default .......................................... 4939
dns-client ....................................... 4942
echo-interval ................................... 4944

GGSN Service Configuration Mode Commands ............ 4931
Global Configuration Mode Commands (A-K) ................................................. 4993

aaa accounting-overload-protection ......................................................... 4994
aaa default-domain ............................................................................. 4995
aaa domain-matching ignore-case .......................................................... 4996
aaa domain-matching imsi-prefix ............................................................ 4997
aaa large-configuration ........................................................................ 4998
aaa last-resort ....................................................................................... 5000
aaa tacacs+ ............................................................................................ 5002
aaa username-format ............................................................................ 5003
active-charging service ......................................................................... 5005
alarm ....................................................................................................... 5006
apn-profile ............................................................................................. 5007
apn-remap-table .................................................................................... 5008
arp ............................................................................................................ 5009
autoconfirm ............................................................................................ 5010
autoless ................................................................................................... 5011
banner ..................................................................................................... 5012
boot delay ............................................................................................... 5014
boot interface ......................................................................................... 5015
boot nameserver .................................................................................... 5017
boot networkconfig .............................................................................. 5018
boot system priority ............................................................................... 5020
bulkstats ................................................................................................. 5023
certificate ............................................................................................... 5025
### Contents

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>ca-crl</td>
<td>5027</td>
</tr>
<tr>
<td>call-control-profile</td>
<td>5029</td>
</tr>
<tr>
<td>card</td>
<td>5030</td>
</tr>
<tr>
<td>card-standby-priority</td>
<td>5031</td>
</tr>
<tr>
<td>cdr-multi-mode</td>
<td>5032</td>
</tr>
<tr>
<td>certificate</td>
<td>5033</td>
</tr>
<tr>
<td>cli</td>
<td>5035</td>
</tr>
<tr>
<td>cli-encrypt-algorithm</td>
<td>5038</td>
</tr>
<tr>
<td>clock</td>
<td>5039</td>
</tr>
<tr>
<td>cmp auto-fetch</td>
<td>5042</td>
</tr>
<tr>
<td>cmp cert-store location</td>
<td>5043</td>
</tr>
<tr>
<td>cmp cert-trap time</td>
<td>5044</td>
</tr>
<tr>
<td>commandguard</td>
<td>5045</td>
</tr>
<tr>
<td>congestion-control</td>
<td>5046</td>
</tr>
<tr>
<td>congestion-control overload-disconnect</td>
<td>5048</td>
</tr>
<tr>
<td>congestion-control policy</td>
<td>5050</td>
</tr>
<tr>
<td>congestion-control threshold</td>
<td>5056</td>
</tr>
<tr>
<td>congestion-control threshold license-utilization</td>
<td>5060</td>
</tr>
<tr>
<td>congestion-control threshold max-sessions-per-service-utilization</td>
<td>5062</td>
</tr>
<tr>
<td>congestion-control threshold message-queue-utilization</td>
<td>5064</td>
</tr>
<tr>
<td>congestion-control threshold message-queue-wait-time</td>
<td>5066</td>
</tr>
<tr>
<td>congestion-control threshold port-rx-utilization</td>
<td>5068</td>
</tr>
<tr>
<td>congestion-control threshold port-specific</td>
<td>5070</td>
</tr>
<tr>
<td>congestion-control threshold port-rx-utilization</td>
<td>5072</td>
</tr>
<tr>
<td>congestion-control threshold port-tx-utilization</td>
<td>5074</td>
</tr>
<tr>
<td>congestion-control threshold service-control-cpu-utilization</td>
<td>5076</td>
</tr>
<tr>
<td>congestion-control threshold system-cpu-utilization</td>
<td>5078</td>
</tr>
<tr>
<td>congestion-control threshold system-memory-utilization</td>
<td>5080</td>
</tr>
<tr>
<td>congestion-control threshold tolerance</td>
<td>5082</td>
</tr>
<tr>
<td>connectedapps</td>
<td>5084</td>
</tr>
<tr>
<td>content-filtering category database directory</td>
<td>5085</td>
</tr>
<tr>
<td>content-filtering category database max-versions</td>
<td>5086</td>
</tr>
<tr>
<td>content-filtering category database override</td>
<td>5087</td>
</tr>
<tr>
<td>context</td>
<td>5088</td>
</tr>
<tr>
<td>crash enable</td>
<td>5089</td>
</tr>
<tr>
<td>crypto blacklist file</td>
<td>5091</td>
</tr>
<tr>
<td>crypto remote-secret-list</td>
<td>5093</td>
</tr>
<tr>
<td>crypto whitelist file</td>
<td>5094</td>
</tr>
<tr>
<td>cs-network</td>
<td>5096</td>
</tr>
<tr>
<td>css acsmgr-selection-attempts</td>
<td>5098</td>
</tr>
<tr>
<td>css delivery-sequence</td>
<td>5099</td>
</tr>
<tr>
<td>css service</td>
<td>5100</td>
</tr>
<tr>
<td>default</td>
<td>5101</td>
</tr>
<tr>
<td>diameter dynamic-dictionary</td>
<td>5109</td>
</tr>
<tr>
<td>diameter-host-template</td>
<td>5111</td>
</tr>
<tr>
<td>diameter-proxy ram-disk</td>
<td>5113</td>
</tr>
<tr>
<td>ecmp-lag hash</td>
<td>5114</td>
</tr>
<tr>
<td>end</td>
<td>5115</td>
</tr>
<tr>
<td>enforce imsi-min equivalence</td>
<td>5116</td>
</tr>
<tr>
<td>exit</td>
<td>5118</td>
</tr>
<tr>
<td>fa-spi-list</td>
<td>5119</td>
</tr>
<tr>
<td>failure-handling-template</td>
<td>5120</td>
</tr>
<tr>
<td>get context-list</td>
<td>5122</td>
</tr>
<tr>
<td>get ip</td>
<td>5123</td>
</tr>
</tbody>
</table>
Global Configuration Mode Commands (T-threshold phspc)............ 5271

tacacs mode........................................ 5272
task facility acsmgr.................................. 5273
task facility imsimgr................................. 5274
task facility ipsecmgr................................ 5276
task facility linkmgr................................... 5277
task facility mmedemux................................ 5278
task facility sessmgr.................................. 5279
task resource cpu-memory-low...................... 5281
tech-support test-commands password.............. 5283
terminal ................................................ 5285
threshold 10sec-cpu-utilization..................... 5287
threshold aaa-acct-archive-queue-size............. 5289
threshold aaa-acct-archive-size................... 5291
threshold aaa-acct-failure.......................... 5293
threshold aaa-acct-failure-rate.................... 5295
threshold aaa-auth-failure........................... 5297
Global Configuration Mode Commands (threshold poll commands A - N)

threshold poll 10sec-cpu-utilization interval ........................................ 5454
threshold poll a11-ppp-send-discard interval ........................................ 5455
threshold poll a11-rac-msg-discard interval ........................................ 5457
threshold poll aa11-rrp-failure interval .............................................. 5459
threshold poll a11-rrq-msg-discard interval ......................................... 5460
threshold poll aaa-acct-archive-queue-size interval .............................. 5462
threshold poll aaa-acct-archive-size interval ........................................ 5464
threshold poll aaa-acct-failure interval .............................................. 5465
threshold poll aaa-acct-failure-rate interval ....................................... 5466
threshold poll aaa-auth-failure interval .............................................. 5467
threshold poll aaa-auth-failure-rate interval ....................................... 5468
threshold poll aaa-retry-rate interval ................................................. 5469
threshold poll aamgr-request-queue interval ........................................ 5470
threshold poll active-subscriber interval ............................................. 5472
threshold poll asngw-auth-failure interval ........................................... 5473
threshold poll asngw-handoff-denial interval ....................................... 5475
threshold poll asngw-max-eap-retry interval ........................................ 5476
threshold poll asngw-network-entry-denial interval ................................ 5478
threshold poll asngw-session-setup-timeout interval .............................. 5480
threshold poll asngw-session-timeout interval ...................................... 5481
threshold poll asnc-idle-mode-timeout interval ..................................... 5482
threshold poll asnc-im-entry-denial interval ........................................ 5483
threshold poll asnc-lu-denial interval ................................................ 5484
threshold poll asnc-session-setup-timeout interval ................................ 5485
threshold poll available-ip-pool-group interval .................................... 5487
threshold poll call-reject-no-resource interval .................................... 5488
threshold poll call-setup interval ....................................................... 5489
threshold poll call-setup-failure interval ............................................ 5490
threshold poll call-setup-failures interval .......................................................... 5491
threshold poll call-total-active interval ............................................................ 5492
threshold poll card-temperature-near-power-off-limit interval .............................. 5493
threshold poll cdr-file-space interval ............................................................... 5494
threshold poll conffilt-block interval ............................................................... 5495
threshold poll conffilt-rating interval ............................................................. 5496
threshold poll cpu-available-memory interval .................................................. 5497
threshold poll cpu-load interval ....................................................................... 5498
threshold poll cpu-memory-usage interval ......................................................... 5499
threshold poll cpu-orbs-crit interval .................................................................. 5500
threshold poll cpu-orbs-warn interval ............................................................... 5501
threshold poll cpu-session-throughput interval ................................................ 5503
threshold poll cpu-utilization interval .............................................................. 5505
threshold poll csf-invite-rcvd interval ............................................................. 5506
threshold poll csf-reg-rcvd interval .................................................................. 5507
threshold poll csf-service-route-failures interval ............................................. 5509
threshold poll dccca-bad-answers interval ....................................................... 5510
threshold poll dccca-protocol-error interval ..................................................... 5512
threshold poll dccca-rating-failed interval ....................................................... 5513
threshold poll dccca-unknown-rating-group interval ....................................... 5514
threshold poll dereq-reply-error interval ......................................................... 5515
threshold poll diameter-retry-rate interval ....................................................... 5517
threshold poll edr-file-space interval .............................................................. 5518
threshold poll edr-udr-dropped-flow-control interval ....................................... 5519
threshold poll epdg-current-sessions interval ................................................... 5520
threshold poll error-no-resource interval ......................................................... 5521
threshold poll error-presence interval ............................................................. 5522
threshold poll error-reg-auth interval .............................................................. 5523
threshold poll error-tcp interval ...................................................................... 5524
threshold poll fa-reg-reply-error interval ......................................................... 5525
threshold poll fng-current-active-sessions interval ......................................... 5526
threshold poll fng-current-sessions interval ..................................................... 5527
threshold poll fw-deny-rule interval .............................................................. 5528
threshold poll fw-dos-attack interval ................................................................ 5529
threshold poll fw-drop-packet interval ............................................................. 5530
threshold poll fw-no-rule interval .................................................................... 5531
threshold poll ha-init-rrq-rrcvd-rate interval ............................................... 5532
threshold poll ha-svc-init-rrq-rrcvd-rate interval ........................................... 5533
threshold poll hengbw-paging-messages interval ............................................. 5534
threshold poll ip-pool-free interval .................................................................. 5535
threshold poll ip-pool-hold interval .................................................................. 5536
threshold poll ip-pool-release interval ............................................................. 5537
threshold poll ip-pool-used interval .............................................................. 5538
threshold poll ipsec-call-req-rej interval ......................................................... 5539
threshold poll ipsec-ike-failrate interval ......................................................... 5540
threshold poll ipsec-ike-failures interval ......................................................... 5541
threshold poll ipsec-ike-requests interval ....................................................... 5542
threshold poll ipsec-tunnels-established interval ............................................ 5543
threshold poll ipsec-tunnels-setup interval .................................................... 5544
threshold poll license-remaining-session interval ............................................ 5545
threshold poll mgmt-cpu-memory-usage interval ............................................. 5546
threshold poll mgmt-cpu-utilization interval ..................................................... 5547
threshold poll mme-auth-failures interval ......................................................... 5548
threshold poll mme-attach-failure interval ....................................................... 5550
## Global Configuration Mode Commands (threshold poll commands O - Z)

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>threshold poll nat-port-chunks-usage interval</td>
<td>5552</td>
</tr>
<tr>
<td>threshold poll npu-utilization interval</td>
<td>5553</td>
</tr>
<tr>
<td>threshold poll packets-filtered-dropped interval</td>
<td>5556</td>
</tr>
<tr>
<td>threshold poll packets-forwarded-to-cpu interval</td>
<td>5557</td>
</tr>
<tr>
<td>threshold poll pdg-current-forwarded-to-cpu interval</td>
<td>5558</td>
</tr>
<tr>
<td>threshold poll pdg-current-remote-usage interval</td>
<td>5559</td>
</tr>
<tr>
<td>threshold poll pdg-current-active-usage interval</td>
<td>5560</td>
</tr>
<tr>
<td>threshold poll pdg-current-remote-usage interval</td>
<td>5561</td>
</tr>
<tr>
<td>threshold poll pdg-current-remote-active-usage interval</td>
<td>5562</td>
</tr>
<tr>
<td>threshold poll pdg-current-remote-active-usage interval</td>
<td>5563</td>
</tr>
<tr>
<td>threshold poll per-service-asngw-sessions interval</td>
<td>5564</td>
</tr>
<tr>
<td>threshold poll per-service-ggsn-sessions interval</td>
<td>5565</td>
</tr>
<tr>
<td>threshold poll per-service-gprs-pdp-sessions interval</td>
<td>5566</td>
</tr>
<tr>
<td>threshold poll per-service-gprs-sessions interval</td>
<td>5567</td>
</tr>
<tr>
<td>threshold poll per-service-ha-sessions interval</td>
<td>5568</td>
</tr>
<tr>
<td>threshold poll per-service-lns-sessions interval</td>
<td>5569</td>
</tr>
<tr>
<td>threshold poll per-service-pdg-sessions interval</td>
<td>5570</td>
</tr>
<tr>
<td>threshold poll per-service-pdsn-sessions interval</td>
<td>5571</td>
</tr>
<tr>
<td>threshold poll per-service-sgn-remote-sizing interval</td>
<td>5572</td>
</tr>
<tr>
<td>threshold poll per-service-sgn-sessions interval</td>
<td>5573</td>
</tr>
<tr>
<td>threshold poll phsgw-auth-failure interval</td>
<td>5574</td>
</tr>
<tr>
<td>threshold poll phsgw-eapol-auth-failure interval</td>
<td>5575</td>
</tr>
<tr>
<td>threshold poll phsgw-handoff-denial interval</td>
<td>5576</td>
</tr>
<tr>
<td>threshold poll phsgw-max-eap-retry interval</td>
<td>5577</td>
</tr>
<tr>
<td>threshold poll phsgw-max-eap-retry interval</td>
<td>5578</td>
</tr>
<tr>
<td>threshold poll phsgw-network-entry-denial interval</td>
<td>5579</td>
</tr>
<tr>
<td>threshold poll phsgw-session-setup-timeout interval</td>
<td>5580</td>
</tr>
<tr>
<td>threshold poll phsgw-session-timeout-interval</td>
<td>5581</td>
</tr>
<tr>
<td>threshold poll phspc-session-setup-timeout interval</td>
<td>5582</td>
</tr>
<tr>
<td>threshold poll phspc-sleep-mode-timeout interval</td>
<td>5583</td>
</tr>
<tr>
<td>threshold poll phspc-sm-entry-denial interval</td>
<td>5584</td>
</tr>
<tr>
<td>threshold poll port-high-activity interval</td>
<td>5585</td>
</tr>
<tr>
<td>threshold poll port-rx-utilization interval</td>
<td>5586</td>
</tr>
<tr>
<td>threshold poll port-tx-utilization</td>
<td>5587</td>
</tr>
<tr>
<td>threshold poll ppp-setup-fail-rate interval</td>
<td>5588</td>
</tr>
<tr>
<td>threshold poll reg-reply-error interval</td>
<td>5589</td>
</tr>
<tr>
<td>threshold poll reg-total-active interval</td>
<td>5590</td>
</tr>
<tr>
<td>threshold poll rereg-reply-error interval</td>
<td>5591</td>
</tr>
<tr>
<td>threshold poll route-service interval</td>
<td>5592</td>
</tr>
<tr>
<td>threshold poll rp-setup-fail-rate interval</td>
<td>5593</td>
</tr>
<tr>
<td>threshold poll sess-flow-count interval</td>
<td>5595</td>
</tr>
<tr>
<td>threshold poll storage-utilization interval</td>
<td>5596</td>
</tr>
<tr>
<td>threshold poll system-capacity interval</td>
<td>5597</td>
</tr>
<tr>
<td>threshold poll total-asngw-sessions interval</td>
<td>5598</td>
</tr>
<tr>
<td>threshold poll total-ggsn-sessions interval</td>
<td>5599</td>
</tr>
<tr>
<td>threshold poll total-gprs-pdp-sessions interval</td>
<td>5601</td>
</tr>
<tr>
<td>threshold poll total-gprs-sessions interval</td>
<td>5603</td>
</tr>
<tr>
<td>threshold poll total-ha-sessions interval</td>
<td>5605</td>
</tr>
<tr>
<td>threshold poll total-henbgw-henb-sessions</td>
<td>5606</td>
</tr>
<tr>
<td>threshold poll total-henbgw-ue-sessions</td>
<td>5607</td>
</tr>
<tr>
<td>threshold poll total-henbgw-ue-sessions</td>
<td>5608</td>
</tr>
<tr>
<td>threshold poll total-henbgw-ue-sessions</td>
<td>5608</td>
</tr>
<tr>
<td>threshold poll total-henbgw-ue-sessions</td>
<td>5609</td>
</tr>
<tr>
<td>threshold poll total-henbgw-ue-sessions</td>
<td>5611</td>
</tr>
<tr>
<td>threshold poll total-henbgw-ue-sessions</td>
<td>5613</td>
</tr>
</tbody>
</table>
threshold poll total-hsgw-sessions interval .......................................................... 5615
threshold poll total-lma-sessions interval ......................................................... 5617
threshold poll total-Ins-sessions interval ......................................................... 5619
treshold poll total-mme-sessions ................................................................. 5621
threshold poll total-pdsn-sessions interval ....................................................... 5622
threshold poll total-pgw-sessions interval ......................................................... 5624
threshold poll total-saegw-sessions interval .................................................... 5626
threshold poll total-sgsn-pdp-sessions interval ............................................. 5627
threshold poll total-sgsn-sessions interval ....................................................... 5629
threshold poll total-sgw-sessions interval ......................................................... 5630
threshold poll total-subscriber interval ......................................................... 5632
threshold poll tpo-dns-failure ......................................................................... 5634
threshold poll tpo-low-compression-gain ......................................................... 5635
threshold poll tpo-rto-timeout ......................................................................... 5636

Global Configuration Mode Commands (threshold ppp - url-blacklisting) 5637
threshold ppp-setup-fail-rate ........................................................................... 5638
threshold route-service bgp-routes ................................................................ 5640
threshold rp-setup-fail-rate ........................................................................... 5642
threshold sess-flow-count ................................................................................ 5644
threshold spc-cpu-memory-usage .................................................................... 5645
threshold spc-cpu-utilization ........................................................................... 5646
threshold storage-utilization ............................................................................ 5647
threshold subscriber active ............................................................................... 5649
threshold subscriber total ................................................................................ 5651
threshold system-capacity ................................................................................ 5653
threshold total-asngw-sessions ....................................................................... 5655
threshold total-ggsn-sessions ......................................................................... 5657
threshold total-gprs-pdp-sessions ................................................................. 5659
threshold total-gprs-sessions ......................................................................... 5661
threshold total-ha-sessions ............................................................................. 5663
threshold total-hnbgw-hnb-sessions ............................................................... 5665
threshold total-hnbgw-iu-sessions .................................................................. 5667
threshold total-hnbgw-ue-sessions .................................................................. 5669
threshold total-hsgw-sessions ......................................................................... 5671
threshold total-lma-sessions ........................................................................... 5673
threshold total-Ins-sessions ............................................................................ 5675
threshold total-mme-sessions ........................................................................... 5677
threshold total-pdsn-sessions ......................................................................... 5679
threshold total-pgw-sessions ........................................................................... 5681
threshold total-saegw-sessions ....................................................................... 5683
threshold total-sgsn-pdp-sessions ................................................................. 5685
threshold total-sgsn-sessions ......................................................................... 5687
threshold total-sgw-sessions ........................................................................... 5689
threshold tpo-dns-failure ................................................................................. 5691
threshold tpo-low-compression-gain ............................................................... 5692
threshold tpo-rto-timeout ................................................................................ 5693
timestamps ........................................................................................................ 5694
upgrade limit .................................................................................................... 5695
url-blacklisting database .................................................................................. 5697
wsg-lookup ....................................................................................................... 5699

GPRS Service Configuration Mode Commands .............................................. 5701
accounting ........................................................................................................ 5702
admin-disconnect-behavior ............................................................................. 5704
associate........................................................................................................... 5706
associate-dscp-template ................................................................. 5710
associate-service ........................................................................ 5712
cc profile ......................................................................................... 5714
check-imei ........................................................................................ 5716
check-imei-timeout-action ................................................................. 5718
ciphering-algorithm ........................................................................ 5719
dns isau-mcc-mnc-encoding .............................................................. 5722
end ........................................................................................................ 5723
exit ........................................................................................................ 5724
gmm ................................................................................................. 5725
llc ................................................................................................. 5730
network-sharing ............................................................................... 5734
nri .................................................................................................... 5736
paging-policy ................................................................................. 5738
peer-nsei ........................................................................................ 5740
plmn ............................................................................................... 5742
reporting-action event-record .......................................................... 5744
setup-timeout .................................................................................. 5745
sgsn-context-request ....................................................................... 5746
sgsn-number ................................................................................... 5747
sm .................................................................................................... 5748
sndcp ............................................................................................... 5751

**GRE Tunnel Interface Configuration Mode Commands** .................. 5753
destination ........................................................................................ 5754
destination ........................................................................................ 5755
exit .................................................................................................... 5756
keepalive .......................................................................................... 5757
source ............................................................................................. 5759
tos .................................................................................................... 5760
ttl ...................................................................................................... 5762

**Gs Service Configuration Mode Commands** .............................. 5763
associate-sccp-network .................................................................... 5764
bssap+ ............................................................................................ 5765
end .................................................................................................... 5766
exit .................................................................................................... 5767
max-retransmission ......................................................................... 5768
non-pool-area .................................................................................. 5770
pool-area ......................................................................................... 5772
sgsn-number ................................................................................... 5773
timeout ................................................................................................ 5774
vlr .................................................................................................... 5776

**GT-Format1 Configuration Mode Commands** ............................ 5779
destination ........................................................................................ 5780
exit .................................................................................................... 5781
nature-of-address .............................................................................. 5782
odd-even-indicator ........................................................................... 5783

**GT-Format2 Configuration Mode Commands** ............................ 5785
destination ........................................................................................ 5786
exit .................................................................................................... 5787
translation-type ................................................................................ 5788
GT-Format3 Configuration Mode Commands .................................................. 5789
  encoding-scheme ........................................................................ 5790
  end ........................................................................ 5791
  exit ........................................................................ 5792
  numbering-plan ....................................................................... 5793
  translation-type ...................................................................... 5794
GT-Format4 Configuration Mode Commands .......................................... 5795
  encoding-scheme ....................................................................... 5796
  end ........................................................................ 5797
  exit ........................................................................ 5798
  nature-of-address .................................................................. 5799
  numbering-plan ....................................................................... 5800
  translation-type ...................................................................... 5801
GTTP Server Group Configuration Mode Commands .......................... 5803
  end ........................................................................ 5804
  exit ........................................................................ 5805
  gtpp attribute ....................................................................... 5806
  gtpp charging-agent ................................................................ 5814
  gtpp data-request sequence-numbers ....................................... 5816
  gtpp deadtime ....................................................................... 5817
  gtpp dead-server suppress-cdrs .............................................. 5818
  gtpp detect-dead-server ........................................................ 5819
  gtpp dictionary ...................................................................... 5821
  gtpp duplicate-hold-time ......................................................... 5824
  gtpp echo-interval .................................................................. 5825
  gtpp egcdr ........................................................................... 5827
  gtpp error-response .................................................................. 5830
  gtpp max-cdrs ....................................................................... 5831
  gtpp max-pdu-size .................................................................. 5833
  gtpp max-retries ..................................................................... 5835
  gtpp mbms bucket .................................................................. 5837
  gtpp mbms interval .................................................................. 5838
  gtpp mbms tariff ..................................................................... 5839
  gtpp mbms volume .................................................................. 5840
  gtpp redirection-allowed .......................................................... 5841
  gtpp redirection-disallowed ....................................................... 5842
  gtpp server ........................................................................... 5843
  gtpp source-port-validation ....................................................... 5845
  gtpp storage-server ................................................................ 5846
  gtpp storage-server local file ..................................................... 5847
  gtpp storage-server max-retries ................................................ 5851
  gtpp storage-server mode .......................................................... 5852
  gtpp storage-server timeout ....................................................... 5854
  gtpp suppress-cdrs zero-volume ............................................... 5855
  gtpp suppress-cdrs zero-volume-and-duration ............................. 5857
  gtpp timeout ......................................................................... 5858
  gtpp transport-layer ................................................................ 5859
  gtpp trigger ............................................................................ 5860
GTP-U Service Configuration Mode Commands ................................. 5865
  bind .............................................................................. 5866
  echo-interval ......................................................................... 5868
  echo-retransmission-timeout .................................................... 5870
end .................................................................................................................. 5871
exit .................................................................................................................. 5872
extension-header .......................................................................................... 5873
ip qos-dscp .................................................................................................... 5874
ipsec-allow-error-ind-in-clear ................................................................. 5876
ipsec-tunnel-idle-timeout ........................................................................... 5877
max-retransmissions ................................................................................... 5878
path-failure clear-trap ................................................................................ 5879
path-failure detection-policy ....................................................................... 5880
retransmission-timeout .............................................................................. 5881
sequence-number ....................................................................................... 5882
udp-checksum .............................................................................................. 5883

HA Proxy DNS Configuration Mode Commands ........................................... 5885
end .................................................................................................................. 5886
exit .................................................................................................................. 5887
pass-thru ....................................................................................................... 5888
redirect ........................................................................................................... 5889

HA Service Configuration Mode Commands ............................................. 5891
a11-signalling-packets ................................................................................ 5892
aaa .................................................................................................................. 5893
access-network ........................................................................................... 5895
associate ....................................................................................................... 5896
authentication .............................................................................................. 5897
bind .................................................................................................................. 5899
capsulation ...................................................................................................... 5901
end .................................................................................................................. 5903
exit .................................................................................................................. 5904
fa-ha-spi ......................................................................................................... 5905
gre ...................................................................................................................... 5907
idle-timeout-mode ......................................................................................... 5909
ikev1 .................................................................................................................. 5910
ip context-name ........................................................................................... 5912
ip local-port ................................................................................................... 5913
ip pool .............................................................................................................. 5914
min-reg-lifetime ............................................................................................ 5915
mn-ha-spi ......................................................................................................... 5916
nat-traversal .................................................................................................. 5918
optimize tunnel-reassembly ....................................................................... 5919
per-domain statistics-collection .................................................................. 5920
policy bc-query-result .................................................................................. 5921
policy nw-reachability-fail ......................................................................... 5922
policy overload .............................................................................................. 5924
reg-lifetime .................................................................................................... 5926
reverse-tunnel ............................................................................................... 5927
revocation ....................................................................................................... 5929
setup-timeout ............................................................................................... 5931
simul-bindings ............................................................................................. 5932
threshold dereg-reply-error ......................................................................... 5933
threshold init-rrq-rcvd-rate ......................................................................... 5935
threshold ipsec-call-req-rej ......................................................................... 5937
threshold ipsec-ike-failrate .......................................................................... 5939
threshold ipsec-ike-failures ......................................................................... 5941
threshold ipsec-ike-requests ........................................................................ 5943
threshold ipsec-tunnels-established ................................................................. 5945
threshold ipsec-tunnels-setup ............................................................................. 5947
threshold reg-reply-error ...................................................................................... 5949
treshold rereg-reply-error ..................................................................................... 5951
wimax-3gpp2 interworking ..................................................................................... 5953

HD Storage Policy Configuration Mode Commands ........................................ 5955
directory .............................................................................................................. 5956
directory .............................................................................................................. 5957
exit ....................................................................................................................... 5958
file ....................................................................................................................... 5959

HeNB-GW Access Service Configuration Mode Commands ....................... 5961
associate henbgw-network-service .................................................................... 5962
associate sctp-param-template .......................................................................... 5963
associate x2gw-service ....................................................................................... 5964
bind s1-mme ........................................................................................................ 5965
csg-optimized-paging ......................................................................................... 5966
end ....................................................................................................................... 5967
exit ....................................................................................................................... 5968
mme-id ................................................................................................................ 5969
plmn .................................................................................................................... 5970
s1-mme ip qos-dscp ............................................................................................ 5971
s1-mme sctp port ................................................................................................ 5973
s1u-relay ............................................................................................................. 5974
security-gateway ................................................................................................. 5975
timeout ................................................................................................................ 5977

HeNB-GW Network Service Configuration Mode Commands .................... 5979
anr-info-retrieval ............................................................................................... 5980
associate sctp-param-template .......................................................................... 5981
default-paging-drx .............................................................................................. 5982
default-paging-drx .............................................................................................. 5983
exit ....................................................................................................................... 5984
logical-erb .......................................................................................................... 5985
paging-rate-control ............................................................................................ 5987
pws ...................................................................................................................... 5988
s1ap-max-retransmissions .................................................................................. 5989
s1ap-retransmission-timeout .............................................................................. 5990

HSGW Service Configuration Mode Commands ............................................ 5991
a11-signalling-packets ......................................................................................... 5992
associate ............................................................................................................. 5993
bind address ........................................................................................................ 5994
ccontext-retention-timer ..................................................................................... 5996
data-available-indicator ...................................................................................... 5997
data-over-signaling ............................................................................................. 5998
dns-pgw .............................................................................................................. 5999
end ....................................................................................................................... 6001
exit ....................................................................................................................... 6002
fqdn ...................................................................................................................... 6003
fragment .............................................................................................................. 6005
gre ....................................................................................................................... 6006
ip ......................................................................................................................... 6009
lifetimetime ........................................................................................................... 6012
max-retransmissions ........................................................................................... 6103
mobile-access-gateway .......................................................... 6014
network-initiated-qos .......................................................... 6015
plmn id ................................................................. 6016
policy overload ......................................................... 6017
profile-id-qci-mapping .................................................. 6019
registration-deny ..................................................... 6020
retransmission-timeout .................................................. 6022
rsvp ................................................................. 6023
setup-timeout .......................................................... 6024
spi remote-address ..................................................... 6025
ue-initiated-qos ....................................................... 6027
unauthorized-flows ..................................................... 6028

HSGW Service RoHC Configuration Mode Commands .................... 6029
  cid-mode ......................................................... 6030
  end .............................................................. 6031
  exit .............................................................. 6032
  mrru ............................................................ 6033
  profile .......................................................... 6034

HLR Configuration Mode Commands ......................................... 6037
  acn-version-retention .................................................. 6038
  end .............................................................. 6039
  exit .............................................................. 6040
  imsi ............................................................. 6041
  policy routing .................................................... 6043
  release-compliance ................................................. 6044

HNB-CS Network Configuration Mode Commands .......................... 6045
  associate alcap-service .......................................... 6046
  associate rtp pool ................................................. 6048
  associate sccp-network .......................................... 6050
  end .............................................................. 6051
  exit .............................................................. 6052
  global-nc-id ..................................................... 6053
  map core-network-id ............................................ 6054
  map idnns .......................................................... 6056
  map lac ........................................................... 6058
  map nri ............................................................ 6060
  msc deadtime ..................................................... 6062
  msc point-code .................................................. 6064
  nri length .......................................................... 6066
  null-nri ............................................................ 6068
  offload-msc ...................................................... 6069
  ranap reset .......................................................... 6071

HNB-GW Global Configuration Mode Commands ............................ 6073
  access-control-db .................................................. 6074
  end .............................................................. 6076
  exit .............................................................. 6077
  paging hybrid-hnb .................................................. 6078
  paging open-hnb .................................................. 6080
  scgp ............................................................. 6082
  trans-timer .......................................................... 6084

HNB-GW Service Configuration Mode Commands ............................ 6085
associate cs-network .......................................................... 6164
associate ps-network .......................................................... 6165
authorised-macro-lai .......................................................... 6166
end ................................................................................. 6168
exit ................................................................................. 6169
mnc-id ............................................................................. 6170

HSS Peer Service Configuration Mode Commands ................ 6171
auth-request ....................................................................... 6172
diameter hss-dictionary ..................................................... 6173
diameter hss-endpoint ....................................................... 6175
diameter suppress ............................................................ 6177
diameter update-dictionary-avps ..................................... 6178
dynamic-destination-realm ................................................. 6179
end ................................................................................. 6180
exit ................................................................................. 6181
failure-handling ................................................................. 6182
request timeout ................................................................. 6185
zone-code-format ............................................................... 6186

IGMP Profile Configuration Mode Commands ................... 6187
default ip igmp ................................................................... 6188
end ................................................................................. 6189
exit ................................................................................. 6190
ip igmp query .................................................................... 6191
ip igmp require router-alert ............................................ 6192
ip igmp robustness ........................................................... 6193
ip igmp unsolicited-report-interval .................................. 6194
ip igmp version ................................................................ 6195

IKEv2 Security Association Configuration Mode Commands .. 6197
default .............................................................................. 6198
encryption ....................................................................... 6199
end ................................................................................. 6201
exit ................................................................................. 6202
group .............................................................................. 6203
hmac .............................................................................. 6205
lifetime ........................................................................... 6207
prf .................................................................................. 6208

IMEI Profile Configuration Mode ...................................... 6211
associate .......................................................................... 6212
blacklist .......................................................................... 6213
description ...................................................................... 6214
direct-tunnel .................................................................... 6215
end ................................................................................. 6216
exit ................................................................................. 6217
ggsn-address .................................................................... 6218
pdp-activate .................................................................... 6219

IMS Authorization Service Configuration Mode Commands ....... 6221
end ................................................................................. 6222
exit ................................................................................. 6223
p-cscf discovery ................................................................. 6224
p-cscf table ....................................................................... 6226
policy-control ................................................................. 6228
<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>qos-update-timeout</td>
<td>6229</td>
</tr>
<tr>
<td>signaling-flag</td>
<td>6230</td>
</tr>
<tr>
<td>signaling-flow</td>
<td>6232</td>
</tr>
<tr>
<td>traffic-policy</td>
<td>6234</td>
</tr>
<tr>
<td><strong>IPMS Client Configuration Mode Commands</strong></td>
<td>6257</td>
</tr>
<tr>
<td>end</td>
<td>6258</td>
</tr>
<tr>
<td>exit</td>
<td>6259</td>
</tr>
<tr>
<td>export keys</td>
<td>6260</td>
</tr>
<tr>
<td>heartbeat</td>
<td>6261</td>
</tr>
<tr>
<td>server</td>
<td>6262</td>
</tr>
<tr>
<td>source</td>
<td>6264</td>
</tr>
<tr>
<td><strong>IPSec Transform Set Configuration Mode Commands</strong></td>
<td>6265</td>
</tr>
<tr>
<td>encryption</td>
<td>6266</td>
</tr>
<tr>
<td>end</td>
<td>6268</td>
</tr>
<tr>
<td>exit</td>
<td>6269</td>
</tr>
<tr>
<td>group</td>
<td>6270</td>
</tr>
<tr>
<td>hmac</td>
<td>6272</td>
</tr>
<tr>
<td>mode</td>
<td>6274</td>
</tr>
<tr>
<td><strong>IPSG RADIUS Server Configuration Mode Commands</strong></td>
<td>6277</td>
</tr>
<tr>
<td>accounting-context</td>
<td>6278</td>
</tr>
<tr>
<td>associate sgtp-service</td>
<td>6279</td>
</tr>
<tr>
<td>bind</td>
<td>6281</td>
</tr>
<tr>
<td>connection authorization</td>
<td>6284</td>
</tr>
<tr>
<td>end</td>
<td>6285</td>
</tr>
<tr>
<td>exit</td>
<td>6286</td>
</tr>
<tr>
<td>gtp max-contexts-per-imsi</td>
<td>6287</td>
</tr>
<tr>
<td>gtp peer-ip-address</td>
<td>6288</td>
</tr>
<tr>
<td>ip</td>
<td>6289</td>
</tr>
<tr>
<td>map ue-mac-to-imei</td>
<td>6292</td>
</tr>
<tr>
<td>overlapping-ip-address</td>
<td>6293</td>
</tr>
<tr>
<td>plmn id</td>
<td>6294</td>
</tr>
<tr>
<td>profile</td>
<td>6295</td>
</tr>
<tr>
<td>radius accounting</td>
<td>6297</td>
</tr>
<tr>
<td>radius dictionary</td>
<td>6301</td>
</tr>
<tr>
<td>sess-replacement</td>
<td>6303</td>
</tr>
<tr>
<td>setup-timeout</td>
<td>6305</td>
</tr>
<tr>
<td>w-apn</td>
<td>6306</td>
</tr>
<tr>
<td><strong>IPMS Client Configuration Mode Commands</strong></td>
<td>6245</td>
</tr>
<tr>
<td>associate l2-mapping-table</td>
<td>6246</td>
</tr>
<tr>
<td>end</td>
<td>6248</td>
</tr>
<tr>
<td>exit</td>
<td>6249</td>
</tr>
<tr>
<td>ip guarantee</td>
<td>6250</td>
</tr>
<tr>
<td>ip maximum-routes</td>
<td>6251</td>
</tr>
<tr>
<td>mpls map-dscp-to-exp</td>
<td>6252</td>
</tr>
<tr>
<td>mpls map-exp-to-dscp</td>
<td>6254</td>
</tr>
<tr>
<td><strong>IPMS Client Configuration Mode Commands</strong></td>
<td>6237</td>
</tr>
<tr>
<td>diameter</td>
<td>6238</td>
</tr>
<tr>
<td>exit</td>
<td>6240</td>
</tr>
<tr>
<td>failure-handling</td>
<td>6242</td>
</tr>
<tr>
<td>request</td>
<td>6244</td>
</tr>
<tr>
<td><strong>IPMS Client Configuration Mode Commands</strong></td>
<td>6229</td>
</tr>
</tbody>
</table>
IPSG RADIUS Snoop Configuration Mode Commands ...................... 6309
bind .......................................................... 6310
collection authorization ............................................... 6311
def ............................................................. 6312
de ............................................................. 6313
exit .................................................................. 6314
radius ............................................................. 6315
set ............................................................... 6317
setup-timeout .................................................... 6319

IPSP Configuration Mode Commands .................................. 6321
dead-interval .................................................... 6322
def ............................................................. 6323
de ............................................................. 6324
de ............................................................. 6325
ip .................................................................. 6326
ip .................................................................. 6327

IPv6 ACL Configuration Mode Commands ............................. 6327
deny/permit (by source IP address masking) ......................... 6328
deny/permit (by any) ............................................... 6329
deny/permit (by host IP address) ...................................... 6330
deny/permit (by source ICMP packets) .............................. 6331
deny/permit (by IP packets) ......................................... 6332
deny/permit (by TCP/UDP packets) .................................. 6333
de ............................................................... 6334
de ............................................................... 6335
de ............................................................... 6336
de ............................................................... 6337
de ............................................................... 6338
de ............................................................... 6339
de ............................................................... 6340
de ............................................................... 6341
de ............................................................... 6342
de ............................................................... 6343
de ............................................................... 6344
de ............................................................... 6345
de ............................................................... 6346
de ............................................................... 6347
de ............................................................... 6348
de ............................................................... 6349
de ............................................................... 6350
redirect context (by IP address masking) ......................... 6351
redirect context (by source IP address masking) ................. 6352
redirect context (by host IP address) .............................. 6353
redirect context (by source ICMP packets) ......................... 6354
redirect context (by IP packets) ...................................... 6355
redirect context (by TCP/UDP packets) ............................ 6356
redirect css service (any) ........................................... 6357
redirect css service (by host IP address) ......................... 6358
redirect css service (by source IP address masking) ........... 6359
redirect css service (by source ICMP packets) .................. 6360
redirect css service (by IP packets) ............................... 6361
redirect css service (for downlink, by any) ....................... 6362
redirect css service (for downlink, by host IP address) ...... 6363
redirect css service (for downlink, by ICMP packets) ........ 6364
redirect css service (for downlink, by IP packets) ............. 6365
redirect css service (for downlink, by source IP address masking) 6366
redirect css service (for downlink, by TCP/UDP packets) .... 6367
redirect css service (for uplink, by any) ......................... 6368
redirect css service (for uplink, by host IP address) .......... 6369
redirect css service (for uplink, by ICMP packets) ............ 6370
redirect css service (for uplink, by IP packets) ................. 6371
redirect css service (for uplink, by source IP address masking) 6372
redirect css service (for uplink, by TCP/UDP packets) ....... 6373
redirect next-hop (by any) ...................................... 6374
redirect next-hop (by host IP address) ........................... 6375
redirect next-hop (by IP address masking) ....................... 6376
redirect next-hop (by TCP/UDP packets) ......................... 6377
redirect nexthop (by source ICMP packets) ............................................................. 6435
redirect nexthop (by IP packets) ............................................................................ 6439
redirect nexthop (by TCP/UDP packets) ................................................................. 6442
IPv6 to IPv4 Tunnel Interface Configuration Mode Commands...................... 6447
destination address ................................................................................................. 6448
end ............................................................................................................................ 6449
exit ......................................................................................................................... 6450
mode ...................................................................................................................... 6451
source ..................................................................................................................... 6452
tos ........................................................................................................................... 6453
ttl ............................................................................................................................. 6454
ISAKMP Configuration Mode Commands ............................................................. 6455
authentication ....................................................................................................... 6456
encryption .............................................................................................................. 6457
end ............................................................................................................................ 6458
exit ......................................................................................................................... 6459
group ...................................................................................................................... 6460
hash ....................................................................................................................... 6461
lifetime .................................................................................................................. 6462
IuPS Service Configuration Mode Commands ..................................................... 6465
access-protocol ..................................................................................................... 6466
associate............................................................................................................... 6467
blacklist-timeout-gtpu-bind-addresses ................................................................. 6468
empty-cr .................................................................................................................. 6469
end ............................................................................................................................ 6470
exit ......................................................................................................................... 6471
force-authenticate consecutive-security-failure .................................................... 6472
gtpu ......................................................................................................................... 6473
inter-mc-procedures .............................................................................................. 6474
iu-hold-connection ................................................................................................. 6475
iu-recovery ............................................................................................................ 6476
iu-release-complete-timeout .................................................................................. 6477
loss-of-radio-coverage ranap-cause ..................................................................... 6478
mbms ...................................................................................................................... 6479
network-sharing cs-ps-coordination ................................................................... 6480
network-sharing failure-code ............................................................................... 6481
network-sharing non-shared ............................................................................... 6482
plmn ......................................................................................................................... 6483
rab-assignment-response-timeout ....................................................................... 6484
radio-network-controller ...................................................................................... 6485
relocation-alloc-timeout ...................................................................................... 6486
relocation-complete-timeout ................................................................................. 6487
reset ....................................................................................................................... 6488
rnc ........................................................................................................................... 6489
security-mode-complete-timeout ......................................................................... 6490
service-request-follow-on .................................................................................... 6491
srns-context-response-timeout ............................................................................. 6492
tigoc-timeout ......................................................................................................... 6493
tintc-timeout ......................................................................................................... 6494
LAC Service Configuration Mode Commands ..................................................... 6503
allow ....................................................................................................................... 6504
bind ......................................................................................................................... 6505
data sequence-number ................................................................. 6507
default ............................................................................. 6508
end .................................................................................... 6510
exit ..................................................................................... 6511
hide-attributes ..................................................................... 6512
keepalive-interval ................................................................. 6513
load-balancing ..................................................................... 6515
local-receive-window ......................................................... 6517
max-retransmission .............................................................. 6518
max-session-per-tunnel ....................................................... 6519
max-tunnel-challenge-length ............................................. 6520
max-tunnels ......................................................................... 6521
peer-lns .............................................................................. 6522
proxy-lcp-authentication .................................................... 6524
retransmission-timeout-first ................................................. 6525
retransmission-timeout-max ................................................ 6526
single-port-mode ................................................................. 6527
snoop framed-ip-address .................................................... 6528
trap .................................................................................... 6529
tunnel selection-key ............................................................. 6530
tunnel-authentication .......................................................... 6532

Line Configuration Mode Commands ......................................... 6533
  default ............................................................................. 6534
  end .................................................................................... 6535
  exit ..................................................................................... 6536
  length ............................................................................. 6537
  width .................................................................................. 6538

Link Configuration Mode Commands ........................................ 6539
  arbitration ......................................................................... 6540
  end .................................................................................... 6541
  exit ..................................................................................... 6542
  mtp2-aerm-emergency-threshold ....................................... 6543
  mtp2-aerm-normal-threshold ........................................... 6544
  mtp2-eim-decrement ........................................................ 6545
  mtp2-eim-increment ........................................................ 6546
  mtp2-eim-threshold .......................................................... 6547
  mtp2-error-correction ....................................................... 6548
  mtp2-issu-len .................................................................... 6549
  mtp2-max-outstand-frames ............................................... 6550
  mtp2-suerm-threshold ........................................................ 6551
  mtp3-discard-priority ....................................................... 6552
  mtp3-max-slt-try ............................................................... 6553
  mtp3-msg-priority ............................................................ 6554
  mtp3-msg-size ................................................................. 6555
  mtp3-p1-qlen .................................................................... 6556
  mtp3-p2-qlen .................................................................... 6557
  mtp3-p3-qlen .................................................................... 6558
  mtp3-test-pattern ............................................................. 6559
  priority ............................................................................... 6560
  signaling-link-code .......................................................... 6561
  sscf-nni-n1 ...................................................................... 6562
  sscop-max-cc ................................................................... 6563
  sscop-max-pd .................................................................... 6564
LNS Service Configuration Mode Commands .................................................. 6566
  timeout ................................................................................................. 6566
Linkset Configuration Mode Commands ......................................................... 6571
  adjacent-point-code ........................................................................... 6572
  end ....................................................................................................... 6573
  exit ....................................................................................................... 6574
  link ....................................................................................................... 6575
  self-point-code .................................................................................... 6577
LMA Service Configuration Mode Commands ............................................... 6579
  aaa accounting ................................................................................. 6580
  bind address ....................................................................................... 6581
  end ....................................................................................................... 6583
  exit ....................................................................................................... 6584
  heartbeat ............................................................................................. 6585
  mobility-option-type-value ............................................................... 6587
  refresh-advice-option ....................................................................... 6588
  refresh-interval-percent ................................................................... 6589
  reg-lifetime ......................................................................................... 6590
  revocation .......................................................................................... 6591
  sequence-number-validate .................................................................. 6593
  setup-timeout ..................................................................................... 6594
  signalling-packets ............................................................................. 6595
  simul-bindings .................................................................................... 6596
  standalone .......................................................................................... 6597
  timestamp-option-validation ............................................................. 6598
  timestamp-replay-protection .............................................................. 6599
LNS Service Configuration Mode Commands ............................................... 6601
  aaa accounting ................................................................................. 6602
  authentication .................................................................................... 6603
  avp map called-number apn ............................................................... 6605
  bind ....................................................................................................... 6606
  data sequence-number ...................................................................... 6607
  default ................................................................................................ 6608
  end ....................................................................................................... 6611
  exit ....................................................................................................... 6612
  ip source-violation ........................................................................... 6613
  keepalive-interval ............................................................................. 6615
  local-receive-window ....................................................................... 6616
  max-retransmission ........................................................................... 6617
  max-session-per-tunnel ..................................................................... 6618
  max-tunnel-challenge-length ............................................................... 6619
  max-tunnels ....................................................................................... 6620
  nai-construction-domain ................................................................. 6621
  newcall ............................................................................................... 6622
  peer-lac ............................................................................................... 6623
  proxy-lcp-authentication ................................................................... 6625
  retransmission-timeout-first ............................................................... 6626
  retransmission-timeout-max .............................................................. 6627
  setup-timeout ..................................................................................... 6628
  single-port-mode .............................................................................. 6629
  trap ........................................................................................................ 6630
  tunnel-authentication ......................................................................... 6631
LTE Forbidden Location Area Configuration Mode Commands ........... 6703
end.............................................................................................................. 6704
exit.............................................................................................................. 6705
lac.............................................................................................................. 6706
LTE Forbidden Tracking Area Configuration Mode Commands ........... 6707
end.............................................................................................................. 6708
exit.............................................................................................................. 6709
tac.............................................................................................................. 6710
LTE Foreign PLMN GUTI Management Database Configuration Mode Commands.............................................................................................................. 6711
end.............................................................................................................. 6712
exit.............................................................................................................. 6713
plmn.............................................................................................................. 6714
LTE Handover Restriction List Configuration Mode Commands ........... 6717
end.............................................................................................................. 6718
exit.............................................................................................................. 6719
forbidden................................................................................................... 6720
LTE Network Global MME ID Management Database Configuration Mode Commands.............................................................................................................. 6723
end.............................................................................................................. 6724
exit.............................................................................................................. 6725
plmn.............................................................................................................. 6726
LTE Paging Map Configuration Mode Commands................................. 6729
end.............................................................................................................. 6730
exit.............................................................................................................. 6731
precedence............................................................................................... 6732
LTE Paging Profile Configuration Mode Commands............................... 6735
end.............................................................................................................. 6736
exit.............................................................................................................. 6737
paging-stage............................................................................................. 6738
LTE Peer Map Configuration Mode Commands................................. 6740
end.............................................................................................................. 6741
exit.............................................................................................................. 6742
precedence............................................................................................... 6743
LTE Policy Configuration Mode Commands............................................ 6747
cause-code-group................................................................................... 6748
congestion-action-profile........................................................................ 6749
end.............................................................................................................. 6750
exit.............................................................................................................. 6751
foreign-plmn-guti-mgmt-db................................................................. 6752
henbgw mme-pool................................................................................... 6753
henbgw overload-control......................................................................... 6754
ho-restrict-list......................................................................................... 6755
lte-emergency-profile........................................................................... 6756
mme paging cache.................................................................................. 6757
network-global-mme-id-mgmt-db......................................................... 6758
paging-map......................................................................................... 6760
paging-profile....................................................................................... 6761
<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>MIP HA Assignment Table Configuration Mode Commands</td>
<td>6835</td>
</tr>
<tr>
<td>end</td>
<td>6836</td>
</tr>
<tr>
<td>exit</td>
<td>6837</td>
</tr>
<tr>
<td>hoa-range</td>
<td>6838</td>
</tr>
<tr>
<td>MIPv6 HA Service Configuration Mode Commands</td>
<td>6841</td>
</tr>
<tr>
<td>aaa accounting</td>
<td>6842</td>
</tr>
<tr>
<td>bind</td>
<td>6843</td>
</tr>
<tr>
<td>default</td>
<td>6845</td>
</tr>
<tr>
<td>end</td>
<td>6847</td>
</tr>
<tr>
<td>exit</td>
<td>6848</td>
</tr>
<tr>
<td>refresh-advice-option</td>
<td>6849</td>
</tr>
<tr>
<td>refresh-interval-percent</td>
<td>6850</td>
</tr>
<tr>
<td>reg-lifetime</td>
<td>6851</td>
</tr>
<tr>
<td>sequence-number-validate</td>
<td>6852</td>
</tr>
<tr>
<td>setup-timeout</td>
<td>6853</td>
</tr>
<tr>
<td>simul-bindings</td>
<td>6854</td>
</tr>
<tr>
<td>timestamp-replay-protection tolerance</td>
<td>6855</td>
</tr>
<tr>
<td>MME LAC Pool Area Configuration Mode Commands</td>
<td>6857</td>
</tr>
<tr>
<td>end</td>
<td>6858</td>
</tr>
<tr>
<td>exit</td>
<td>6859</td>
</tr>
<tr>
<td>hash-value</td>
<td>6860</td>
</tr>
<tr>
<td>lac</td>
<td>6862</td>
</tr>
<tr>
<td>plmnid</td>
<td>6863</td>
</tr>
<tr>
<td>MME MSC Pool Area Configuration Mode Commands</td>
<td>6865</td>
</tr>
<tr>
<td>end</td>
<td>6866</td>
</tr>
<tr>
<td>exit</td>
<td>6867</td>
</tr>
<tr>
<td>hash-value</td>
<td>6868</td>
</tr>
<tr>
<td>plmn-id</td>
<td>6870</td>
</tr>
<tr>
<td>use-msc</td>
<td>6872</td>
</tr>
<tr>
<td>LTE HeNBGW MME Pool Configuration Mode Commands</td>
<td>6873</td>
</tr>
<tr>
<td>end</td>
<td>6874</td>
</tr>
<tr>
<td>exit</td>
<td>6875</td>
</tr>
<tr>
<td>mme</td>
<td>6876</td>
</tr>
<tr>
<td>MME Service Configuration Mode Commands</td>
<td>6879</td>
</tr>
<tr>
<td>associate</td>
<td>6880</td>
</tr>
<tr>
<td>bind s1-mme</td>
<td>6884</td>
</tr>
<tr>
<td>csg-change-notification</td>
<td>6886</td>
</tr>
<tr>
<td>dns</td>
<td>6887</td>
</tr>
<tr>
<td>emm</td>
<td>6889</td>
</tr>
<tr>
<td>enb-cache-timeout</td>
<td>6897</td>
</tr>
<tr>
<td>encryption-algorithm-lte</td>
<td>6898</td>
</tr>
<tr>
<td>end</td>
<td>6900</td>
</tr>
<tr>
<td>esm</td>
<td>6901</td>
</tr>
<tr>
<td>exit</td>
<td>6904</td>
</tr>
<tr>
<td>gtpv2</td>
<td>6905</td>
</tr>
<tr>
<td>heuristic-paging</td>
<td>6906</td>
</tr>
<tr>
<td>integrity-algorithm-lte</td>
<td>6908</td>
</tr>
<tr>
<td>inter-rat-nnsf</td>
<td>6910</td>
</tr>
<tr>
<td>isr-capability</td>
<td>6912</td>
</tr>
<tr>
<td>local-cause-code-mapping apn-mismatch</td>
<td>6913</td>
</tr>
</tbody>
</table>
local-cause-code-mapping apn-not-subscribed .................................................. 6915
local-cause-code-mapping auth-failure .............................................................. 6916
local-cause-code-mapping congestion .............................................................. 6918
local-cause-code-mapping ctx-xfer-fail-mme ...................................................... 6920
local-cause-code-mapping ctx-xfer-fail-sgsn ..................................................... 6922
local-cause-code-mapping gw-unreachable ....................................................... 6924
local-cause-code-mapping hss-unavailable ....................................................... 6926
local-cause-code-mapping newcall-policy-restrict ............................................ 6928
local-cause-code-mapping no-active-bearers ................................................... 6930
local-cause-code-mapping peer-node-unknown .................................................. 6932
local-cause-code-mapping pgw-selection-failure .............................................. 6934
local-cause-code-mapping restricted-zone-code .............................................. 6936
local-cause-code-mapping sgw-selection-failure ............................................. 6938
local-cause-code-mapping vlr-down ............................................................... 6940
local-cause-code-mapping vlr-unreachable ...................................................... 6942
location-reporting ......................................................................................... 6944
mapping ........................................................................................................... 6945
max-bearers per-subscriber ............................................................................... 6947
max-paging-attempts ....................................................................................... 6948
max-pdns per-subscriber .................................................................................. 6949
mme-id ............................................................................................................ 6950
mmemgr-recovery ............................................................................................ 6951
msc .................................................................................................................... 6952
nas-max-retransmission .................................................................................... 6954
network-sharing ............................................................................................... 6955
nri ....................................................................................................................... 6957
peer-mme .......................................................................................................... 6958
peer-sgsn ......................................................................................................... 6960
pgw-address ..................................................................................................... 6962
plmn-id .............................................................................................................. 6964
policy attach ..................................................................................................... 6966
policy idle-mode ............................................................................................... 6968
policy inter-rat ................................................................................................... 6969
policy network .................................................................................................. 6971
policy overcharge-protection ............................................................................ 6972
policy overload .................................................................................................. 6974
policy pdn-reconnection .................................................................................... 6975
policy s1-reset ................................................................................................... 6977
policy sctp-down ............................................................................................... 6978
policy service-request ....................................................................................... 6979
policy tau ........................................................................................................... 6981
pool-area ............................................................................................................ 6983
relative-capacity ............................................................................................... 6985
s1-mme ip ........................................................................................................... 6986
s1-mme sctp port ............................................................................................... 6988
setup-timeout ..................................................................................................... 6989
snmp trap ........................................................................................................... 6990
ue-db ................................................................................................................... 6991

MME SGs Service Configuration Mode Commands ........................................... 6993
associate ............................................................................................................. 6994
bind ..................................................................................................................... 6995
dead .................................................................................................................... 6996
exit ....................................................................................................................... 6997
<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>network-service-entity</td>
<td>6998</td>
</tr>
<tr>
<td>pool-area</td>
<td>7000</td>
</tr>
<tr>
<td>scap</td>
<td>7001</td>
</tr>
<tr>
<td>tac-to-lac-mapping</td>
<td>7002</td>
</tr>
<tr>
<td>timer</td>
<td>7003</td>
</tr>
<tr>
<td>vlr</td>
<td>7005</td>
</tr>
<tr>
<td><strong>MPLS-IP Configuration Mode Commands</strong></td>
<td>7007</td>
</tr>
<tr>
<td>end</td>
<td>7008</td>
</tr>
<tr>
<td>exit</td>
<td>7009</td>
</tr>
<tr>
<td>protocol ldp</td>
<td>7010</td>
</tr>
<tr>
<td><strong>MPLS-LDP Configuration Mode Commands</strong></td>
<td>7011</td>
</tr>
<tr>
<td>advertise-labels</td>
<td>7012</td>
</tr>
<tr>
<td>discovery</td>
<td>7014</td>
</tr>
<tr>
<td>enable</td>
<td>7016</td>
</tr>
<tr>
<td>end</td>
<td>7017</td>
</tr>
<tr>
<td>exit</td>
<td>7018</td>
</tr>
<tr>
<td>router-id</td>
<td>7019</td>
</tr>
<tr>
<td>session</td>
<td>7020</td>
</tr>
<tr>
<td><strong>MRME Service Configuration Mode Commands</strong></td>
<td>7023</td>
</tr>
<tr>
<td>attribute</td>
<td>7024</td>
</tr>
<tr>
<td>bind</td>
<td>7025</td>
</tr>
<tr>
<td>disconnect</td>
<td>7027</td>
</tr>
<tr>
<td>dns-pgw</td>
<td>7028</td>
</tr>
<tr>
<td>end</td>
<td>7030</td>
</tr>
<tr>
<td>exit</td>
<td>7031</td>
</tr>
<tr>
<td>fqdn</td>
<td>7032</td>
</tr>
<tr>
<td>radius</td>
<td>7033</td>
</tr>
<tr>
<td>setup-timeout</td>
<td>7035</td>
</tr>
<tr>
<td><strong>Network Service Entity - Peer NSEI Configuration Mode Commands</strong></td>
<td>7037</td>
</tr>
<tr>
<td>bssgp-timer</td>
<td>7038</td>
</tr>
<tr>
<td>end</td>
<td>7039</td>
</tr>
<tr>
<td>exit</td>
<td>7040</td>
</tr>
<tr>
<td>ns-reset-mode</td>
<td>7041</td>
</tr>
<tr>
<td>ns-vc</td>
<td>7043</td>
</tr>
<tr>
<td><strong>Network Service Entity- IP Local Configuration Mode Commands</strong></td>
<td>7045</td>
</tr>
<tr>
<td>all-nsvc-failure-action</td>
<td>7046</td>
</tr>
<tr>
<td>associate</td>
<td>7047</td>
</tr>
<tr>
<td>bssgp-timer</td>
<td>7049</td>
</tr>
<tr>
<td>end</td>
<td>7050</td>
</tr>
<tr>
<td>exit</td>
<td>7051</td>
</tr>
<tr>
<td>max-nsv-retransmissions</td>
<td>7052</td>
</tr>
<tr>
<td>ns-timer</td>
<td>7053</td>
</tr>
<tr>
<td>nsvc-failure-action</td>
<td>7054</td>
</tr>
<tr>
<td>ns-lv</td>
<td>7055</td>
</tr>
<tr>
<td>peer-network-service-entity</td>
<td>7056</td>
</tr>
<tr>
<td>retry-count</td>
<td>7057</td>
</tr>
<tr>
<td>timer</td>
<td>7058</td>
</tr>
<tr>
<td><strong>Network Service Virtual Connection Configuration Mode Commands</strong></td>
<td>7059</td>
</tr>
<tr>
<td>end</td>
<td>7060</td>
</tr>
<tr>
<td>exit</td>
<td>7061</td>
</tr>
</tbody>
</table>
Network Service Virtual Link Configuration Mode Commands .......... 7063
  end ................................................................................. 7064
  exit ............................................................................. 7065
  nsvl-address .................................................................. 7066
  weight .......................................................................... 7067
NTP Configuration Mode Commands .............................................. 7069
  enable ........................................................................... 7070
  end ............................................................................. 7071
  exit ............................................................................. 7072
  server .......................................................................... 7073
Operator Policy Configuration Mode ............................................. 7075
  apn .............................................................................. 7076
  associate ....................................................................... 7078
  description ..................................................................... 7079
  end ............................................................................. 7080
  exit ............................................................................. 7081
  imei ............................................................................ 7082
ORBEM Configuration Mode Commands ........................................ 7085
  activate ......................................................................... 7086
  client ........................................................................... 7087
  default ......................................................................... 7089
  end ............................................................................. 7091
  event-notif-iop-port ...................................................... 7092
  event-notif-service ......................................................... 7093
  event-notif-siop-port ...................................................... 7102
  exit ............................................................................. 7103
  iop-port ......................................................................... 7104
  iop-transport .................................................................. 7105
  iop-address ..................................................................... 7106
  max-attempt .................................................................... 7107
  session-timeout ............................................................... 7108
  siop-port ........................................................................ 7109
  ssl-auth-policy .............................................................. 7110
  ssl-certificate ................................................................. 7111
  ssl-private-key ................................................................. 7113
OSPF Configuration Mode Commands ......................................... 7115
  area authentication .......................................................... 7116
  area default-cost ............................................................. 7117
  area nssa ........................................................................ 7118
  area stub ......................................................................... 7120
  area virtual-link .............................................................. 7121
  area virtual link authentication .......................................... 7122
  area virtual-link authentication-key .................................... 7124
  area virtual link intervals .................................................. 7126
  area virtual link message-digest-key .................................... 7128
  bfd-all-interfaces ............................................................ 7130
  capability graceful-restart .................................................. 7131
  default-information originate .............................................. 7132
  default-metric ................................................................. 7134
  distance ........................................................................ 7135
  distribute-list .................................................................. 7137
end ................................................................. 7139
exit ............................................................... 7140
ip vrf ............................................................ 7141
neighbor ......................................................... 7142
network area ................................................... 7143
ospf graceful-restart ......................................... 7144
ospf router-id .................................................. 7145
passive-interface .............................................. 7146
redistribute ..................................................... 7147
refresh timer ................................................... 7149
router-id ......................................................... 7150
timers spf ....................................................... 7151

OSPFv3 Configuration Mode Commands .................. 7153
area ................................................................. 7154
default-metric .................................................. 7156
distance .......................................................... 7157
distribute-list ................................................... 7158
end ................................................................. 7159
exit ................................................................. 7160
neighbor ......................................................... 7162
timers spf ....................................................... 7163

OSPF VRF Configuration Mode Commands ............... 7165
area ................................................................. 7166
default-information originate ............................... 7170
default-metric .................................................. 7171
distance .......................................................... 7173
distribute-list ................................................... 7175
edge ............................................................... 7176
exit ................................................................. 7177
neighbor ......................................................... 7178
network area ................................................... 7179
ospf router-id .................................................. 7181
passive-interface .............................................. 7182
redistribute ..................................................... 7183
refresh timer ................................................... 7185
timers spf ....................................................... 7186

Out-Address Configuration Mode Commands ............... 7189
end ................................................................. 7190
exit ................................................................. 7191
gateway .......................................................... 7192
gate ............................................................... 7193
ni-identifier ..................................................... 7194
point-code ....................................................... 7195
routing-identifier ............................................ 7196
ssf ................................................................. 7197
ssn ................................................................. 7198

PCC-Action-Set Configuration Mode Commands ............ 7199
af-media-type ................................................... 7200
associate monitoring-key .................................... 7202
authorize ........................................................ 7204
dissociate monitoring-key ................................... 7206

Cisco ASR 5x00 Command Line Interface Reference
dynamic-rule-install ................................................................. 7208
dynamic-rule-uninstall ............................................................. 7212
end ....................................................................................... 7214
exit ....................................................................................... 7215
log-event ............................................................................... 7216
notify-user ............................................................................. 7217
offline-charging-server ............................................................... 7219
online-charging-server ............................................................... 7221
request-usage-report monitoring-key .......................................... 7223
rule-activate ......................................................................... 7224
rule-deactivate ....................................................................... 7226
rulebase-activate .................................................................... 7228
rulebase-deactivate .................................................................. 7230
service-tag ........................................................................... 7232
terminate-session .................................................................... 7233
usage-monitor ......................................................................... 7234

PCC-AF-Service Configuration Mode Commands ............................. 7237
associate pcc-service ................................................................. 7238
diameter dictionary ................................................................... 7239
diameter origin end-point .......................................................... 7240
end ....................................................................................... 7242
exit ....................................................................................... 7243

PCC-Condition-Group Configuration Mode Commands ................... 7245
af-application-id ....................................................................... 7246
af-media-codec ........................................................................ 7248
af-media-type .......................................................................... 7250
af-service-urn ......................................................................... 7252
an-gw-address ........................................................................ 7254
authorized-qci ....................................................................... 7256
base-station-id ........................................................................ 7258
bearer-count ........................................................................... 7260
connectivity-access-network .................................................... 7262
end ....................................................................................... 7264
eval-condition-group ................................................................. 7265
event-time ............................................................................... 7267
exit ....................................................................................... 7269
imsi ....................................................................................... 7271
msisdn ................................................................................... 7272
multi-line-or ........................................................................... 7274
nai ......................................................................................... 7276
out-of-credit rulename ............................................................... 7279
out-of-credit rulebase-name ....................................................... 7280
pcef-address ............................................................................ 7281
pdn-id ..................................................................................... 7283
profile-attribute ...................................................................... 7285
radio-access-technology ............................................................ 7287
sgsn-ip .................................................................................... 7289
sgsn-mcc-mnc ......................................................................... 7291
subscription-attribute ............................................................... 7293
spr-profile-not-found ............................................................... 7295
threshold-condition usage-monitor ............................................. 7296
user-access-network ............................................................... 7299
<table>
<thead>
<tr>
<th>Command Name</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>user-equipment-info esn</td>
<td>7301</td>
</tr>
<tr>
<td>user-equipment-info eui64</td>
<td>7303</td>
</tr>
<tr>
<td>user-equipment-info imeisv</td>
<td>7305</td>
</tr>
<tr>
<td>user-equipment-info mac</td>
<td>7307</td>
</tr>
<tr>
<td>user-equipment-info meid</td>
<td>7309</td>
</tr>
<tr>
<td>user-equipment-info modified-eui64</td>
<td>7311</td>
</tr>
<tr>
<td>user-location-info</td>
<td>7313</td>
</tr>
<tr>
<td><strong>PCC-Data-Service Configuration Mode Commands</strong></td>
<td><strong>7317</strong></td>
</tr>
<tr>
<td>end</td>
<td>7318</td>
</tr>
<tr>
<td>exit</td>
<td>7319</td>
</tr>
<tr>
<td>flow direction in</td>
<td>7320</td>
</tr>
<tr>
<td>flow direction out</td>
<td>7322</td>
</tr>
<tr>
<td>metering-method</td>
<td>7324</td>
</tr>
<tr>
<td>monitoring-key</td>
<td>7325</td>
</tr>
<tr>
<td>precedence</td>
<td>7326</td>
</tr>
<tr>
<td>qos-profile</td>
<td>7327</td>
</tr>
<tr>
<td>rating-group</td>
<td>7328</td>
</tr>
<tr>
<td>reporting-level</td>
<td>7329</td>
</tr>
<tr>
<td>service-identifier</td>
<td>7330</td>
</tr>
<tr>
<td><strong>PCC-Event-Notification-Interface-Endpoint Configuration Mode Commands</strong></td>
<td><strong>7331</strong></td>
</tr>
<tr>
<td>address</td>
<td>7332</td>
</tr>
<tr>
<td>end</td>
<td>7333</td>
</tr>
<tr>
<td>exit</td>
<td>7334</td>
</tr>
<tr>
<td>peer name</td>
<td>7335</td>
</tr>
<tr>
<td>peer select-algorithm</td>
<td>7336</td>
</tr>
<tr>
<td>peer select-peer</td>
<td>7337</td>
</tr>
<tr>
<td>peer select-peer</td>
<td>7338</td>
</tr>
<tr>
<td><strong>PCC-Policy-Service Configuration Mode Commands</strong></td>
<td><strong>7339</strong></td>
</tr>
<tr>
<td>associate pcc-service</td>
<td>7340</td>
</tr>
<tr>
<td>diameter dictionary</td>
<td>7341</td>
</tr>
<tr>
<td>diameter origin end-point</td>
<td>7343</td>
</tr>
<tr>
<td>ehrpd-access-bcm</td>
<td>7345</td>
</tr>
<tr>
<td>end</td>
<td>7347</td>
</tr>
<tr>
<td>exit</td>
<td>7348</td>
</tr>
<tr>
<td>gprs-access-bcm</td>
<td>7349</td>
</tr>
<tr>
<td>max policy-sessions</td>
<td>7351</td>
</tr>
<tr>
<td>subscriber-binding-identifier</td>
<td>7352</td>
</tr>
<tr>
<td>subscription-id-absence-action</td>
<td>7354</td>
</tr>
<tr>
<td>unsolicited-provisioning</td>
<td>7356</td>
</tr>
<tr>
<td><strong>PCC-QoS-Profile Configuration Mode Commands</strong></td>
<td><strong>7357</strong></td>
</tr>
<tr>
<td>arp-priority</td>
<td>7358</td>
</tr>
<tr>
<td>end</td>
<td>7360</td>
</tr>
<tr>
<td>exit</td>
<td>7361</td>
</tr>
<tr>
<td>guaranteed-bitrate</td>
<td>7362</td>
</tr>
<tr>
<td>max-bitrate</td>
<td>7363</td>
</tr>
<tr>
<td>qci</td>
<td>7364</td>
</tr>
<tr>
<td><strong>PCC-Service-Profile Configuration Mode Commands</strong></td>
<td><strong>7365</strong></td>
</tr>
<tr>
<td>default-rulebase-name</td>
<td>7366</td>
</tr>
<tr>
<td>end</td>
<td>7367</td>
</tr>
<tr>
<td>eval-priority</td>
<td>7368</td>
</tr>
<tr>
<td>exit</td>
<td>7370</td>
</tr>
<tr>
<td>service-tag</td>
<td>7371</td>
</tr>
</tbody>
</table>
timeout long-duration ................................................................. 7373
usage-monitor ................................................................. 7375
unknown-services-treatment .................................................. 7377

PCC-Service Configuration Mode Commands ...................................... 7379
action-set ........................................................................ 7380
charging method .................................................................. 7382
charging server .................................................................... 7384
condition-group .................................................................. 7386
data-service ........................................................................ 7388
emergency-apn-map-profile .................................................. 7390
end ...................................................................................... 7392
exit ...................................................................................... 7393
map-profile priority ............................................................ 7394
monitoring-key .................................................................... 7396
multiple-pcef-per-subscriber ................................................ 7398
profile ............................................................................... 7399
qos-profile ......................................................................... 7401
spr-failure .......................................................................... 7403
ssc-usage-update-policy ....................................................... 7404
timedef ............................................................................... 7406
timeout idle ......................................................................... 7408
timeout setup ....................................................................... 7410
timeout long-duration ............................................................ 7411

PCC-Sp-Endpoint Configuration Mode Commands .................................... 7413
access-type ......................................................................... 7414
diameter dictionary .............................................................. 7415
diameter origin end-point ....................................................... 7417
diameter peer-select .............................................................. 7418
end ...................................................................................... 7421
exit ...................................................................................... 7422
profile-data ......................................................................... 7423
profile-update-notification ................................................... 7425
spr subscriber identifier ......................................................... 7426

PCC-TimeDef Configuration Mode Commands ...................................... 7429
end ...................................................................................... 7430
exit ...................................................................................... 7431
start date ............................................................................. 7432
start day .............................................................................. 7434
start time .............................................................................. 7436
time-slot ............................................................................. 7438

PCC-Usage-Monitor Configuration Mode Commands .................................. 7443
end ...................................................................................... 7444
exit ...................................................................................... 7445
usage-limit time .................................................................... 7446
usage-limit volume ............................................................... 7447

PCP Configuration Mode Commands ............................................... 7449
end ...................................................................................... 7450
exit ...................................................................................... 7451
policy-control ...................................................................... 7452
server ................................................................................. 7453

PCP Policy Control Configuration Mode Commands .................................. 7455
PDG Service Configuration Mode Commands ........................................ 7463
  aaa attribute ................................................................. 7464
  associate sgtp-service ................................................... 7465
  certificate-selection ...................................................... 7466
  bind ................................................................................. 7467
  end ................................................................................. 7469
  exit ................................................................................. 7470
  ip gnp-qos-dscp ............................................................... 7471
  ip qos-dscp ...................................................................... 7475
  ip source-violation ............................................................ 7478
  max-tunnels-per-ue ............................................................. 7480
  plmn id ............................................................................. 7481
  setup-timeout .................................................................... 7482

PDIF Service Configuration Mode Commands ...................................... 7483
  aaa attribute ................................................................. 7484
  aaa authentication ......................................................... 7486
  bind ................................................................................. 7488
  default .............................................................................. 7489
  duplicate-session-detection ............................................... 7491
  end ................................................................................. 7492
  exit ................................................................................. 7493
  hss .................................................................................. 7494
  ims-sh-service ................................................................. 7496
  ip source-violation ............................................................ 7497
  mobile-ip .......................................................................... 7499
  setup-timeout .................................................................... 7500
  username ....................................................................... 7501

PDSN Service Configuration Mode Commands ................................... 7503
  a11-signalling-packets ....................................................... 7504
  aaa 3gpp2-service-option ................................................ 7505
  aaa nas-ip-address ............................................................ 7506
  access-flow traffic-validation ............................................ 7507
  access-network .................................................................. 7508
  airlink bad-sequence-number ............................................ 7509
  allow alt-ppp ..................................................................... 7511
  always-on-indication ........................................................... 7512
  associate ....................................................................... 7513
  authentication ................................................................. 7514
  bcmcs ............................................................................ 7516
  bind ................................................................................. 7518
  data-available-indicator ................................................... 7520
  data-over-signaling ........................................................... 7521
  default subscriber ............................................................. 7522
  direct-lte-indicator ............................................................ 7523
  dormant-transition ............................................................ 7524
  end ................................................................................. 7525
  enhanced-pcf-redirection ................................................ 7526
  exit ................................................................................. 7527
fragment .......................................................... 7528
gre ................................................................. 7529
inter-pdsn-handoff mobility-event-indicator .................. 7532
inter-pdsn-handover ............................................ 7533
ip header-compression rohc .................................. 7534
ip local-port .................................................... 7535
ip source-violation ............................................. 7536
lifetime ........................................................... 7538
max-retransmissions ............................................ 7539
mobile-ip foreign-agent context ................................ 7540
mobile-ipv6 ...................................................... 7541
msid length ....................................................... 7542
nai-construction .................................................. 7543
new-call conflict ................................................. 7544
pcf-monitor ....................................................... 7545
pcf-session-id-change restart-ppp ............................. 7547
pdsn type0-ttl attempt-inner-match ............................ 7548
peer-pcf .......................................................... 7549
pma-capability-indicator ...................................... 7550
policy .............................................................. 7551
ppp ............................................................... 7554
qos-profile-id-mapping ....................................... 7556
qos update ........................................................ 7558
registration-accept .............................................. 7560
registration-ack-deny terminate-session-on-error ........... 7561
registration-deny ................................................ 7562
registration-discard ............................................ 7565
registration-update ............................................. 7567
retransmission-timeout ....................................... 7569
service-option ................................................... 7571
setup-timeout .................................................... 7573
simple-ip allow .................................................. 7574
spi ................................................................. 7575
tft-validation wait-timeout ..................................... 7578
threshold a11-ppp-send-discard ................................ 7579
threshold a11-rac-msg-discard ................................ 7581
threshold a11-rrp-failure ...................................... 7583
threshold a11-rrq-msg-discard ................................ 7585
threshold init-rrq-rovd-rate .................................. 7587

PDSN Service RoHC Configuration Mode Commands .......... 7589
cid-mode .......................................................... 7590
d ................................................................. 7592
exit ................................................................. 7593
mrru ............................................................... 7594
profile ............................................................. 7595

Peer Profile Configuration Mode Commands .................. 7597
description ....................................................... 7598
d ................................................................. 7599
exit ................................................................. 7600
gtpc ............................................................... 7601
lawful-intercept ................................................ 7603

Peer-Server Configuration Mode Commands .................... 7605
end ................................................................. 7606
exit ................................................................. 7607
mode ............................................................... 7608
name .............................................................. 7609
psp ................................................................. 7610
routing-context .................................................. 7611
self-point-code .................................................. 7612

P-GW Service Configuration Mode Commands ....................... 7613
associate ......................................................... 7614
authorize-with-hss ............................................. 7616
dns-client ....................................................... 7617
egt ................................................................. 7618
eend ............................................................... 7620
exit ................................................................. 7621
fqdn ............................................................... 7622
gx-li ............................................................... 7624
newcall ............................................................ 7625
plmn ............................................................... 7626
session-delete-delay ........................................... 7627
setup-timeout .................................................... 7628

Plugin Configuration Mode Commands ................................ 7629
attribute .......................................................... 7630
eend ............................................................... 7631
exit ................................................................. 7632
module priority .................................................. 7633

Policy Control Configuration Mode Commands ....................... 7635
apn-name-to-be-included ....................................... 7636
arp-priority-level ............................................... 7638
associate .......................................................... 7639
cc-profile ........................................................ 7641
custom-reauth-trigger ......................................... 7643
diameter dictionary ............................................ 7645
diameter encode-event-avps ................................... 7647
diameter encode-supported-features .......................... 7648
diameter host-select reselect ................................ 7649
diameter host-select row-precedence .......................... 7651
diameter host-select table ..................................... 7654
diameter host-select-template ................................ 7656
diameter map .................................................... 7658
diameter origin endpoint ...................................... 7660
diameter request-timeout ..................................... 7661
diameter update-dictionary-avps ............................... 7662
eend ............................................................... 7665
endpoint-peer-select ............................................ 7666
event-report-indication ....................................... 7667
event-update .................................................... 7669
exit ................................................................. 7672
failure-handling .................................................. 7673
li-secret ........................................................... 7677
re-auth-trigger .................................................... 7678
subscription-id service-type ..................................... 7680

PVC Configuration Mode Commands ..................................... 7683
bind ................................................................. 7684
encapsulation aal5 ............................................. 7686
end .................................................................. 7687
exit ............................................................... 7688
shaping ............................................................ 7689
shutdown .......................................................... 7691
PVC Interface Configuration Mode Commands ................... 7693
description ................................................................... 7694
end .................................................................. 7695
exit .................................................................. 7696
ip ..................................................................... 7697
ip access-group ................................................... 7698
ip address .................................................................. 7700
ip mtu ................................................................ 7702
ip ospf authentication-key ....................................... 7703
ip ospf authentication-type ....................................... 7704
ip ospf cost .......................................................... 7705
ip ospf dead-interval .............................................. 7706
ip ospf hello-interval .............................................. 7707
ip ospf message-digest-key ...................................... 7708
ip ospf network ..................................................... 7709
ip ospf priority ....................................................... 7710
ip ospf retransmit-interval ....................................... 7711
ip ospf transmit-delay ............................................. 7712
QCI - QoS Mapping Configuration Mode Commands .......... 7713
d ............................................................... 7714
exit .................................................................. 7715
qci .................................................................. 7716
QCI - RAN ID Mapping Configuration Mode Commands .... 7721
d .................................................................. 7722
exit .................................................................. 7723
profile-id .............................................................. 7724
Remote Address List Configuration Mode Commands ........... 7727
d .................................................................. 7728
exit .................................................................. 7729
Remote Secret List Configuration Mode Commands ........... 7731
d .................................................................. 7732
exit .................................................................. 7733
remote-id ............................................................... 7734
Remote Server List Configuration Mode Commands .......... 7737
d .................................................................. 7738
exit .................................................................. 7739
Remote Template Configuration Mode Commands ............. 7741
delay-tolerance ......................................................... 7742
end .................................................................. 7743
exit .................................................................. 7744
msg-rate .............................................................. 7745
threshold .............................................................. 7747
RNC Configuration Mode Commands .............................................. 7749
  associate-gtpu-bind-address ................................................. 7750
  description ................................................................. 7751
  direct-tunnel ............................................................... 7752
  dual-address-pdp ......................................................... 7753
  enb-direct-data-forward .................................................. 7755
  end ......................................................................... 7756
  exit ......................................................................... 7757
  lac ......................................................................... 7758
  mbms ........................................................................ 7759
  overload-action disable .................................................... 7760
  paging-non-searching-indication .......................................... 7762
  pointcode ................................................................. 7763
  pooled .................................................................... 7764
  rab-asymmetry-indicator ................................................. 7765
  rab-modify-procedure .................................................... 7767
  ranap arp-ie ............................................................. 7769
  ranap eutran-service-handover-ie ...................................... 7770
  ranap global-cn-id ...................................................... 7772
  ranap paging-area-id .................................................... 7774
  ranap paging-cause-ie ................................................... 7775
  ranap signalling-indication-ie ......................................... 7778
  ran-information-management ............................................. 7780
  release-compliance ....................................................... 7781
  reset-resource ............................................................ 7783

RoHC Profile Common Options Configuration Mode Commands .......... 7785
  delay-release-hc-context-timer .......................................... 7786
  end ......................................................................... 7787
  exit ......................................................................... 7788
  inactive-traffic-release-hc-context-timer .............................. 7789

RoHC Profile Compression Configuration Mode Commands .............. 7791
  context-timeout .......................................................... 7792
  end ......................................................................... 7793
  exit ......................................................................... 7794
  ipid-history-size .......................................................... 7795
  max-jitter-cd ............................................................. 7796
  max-sliding-window ...................................................... 7797
  multiple-ts-stride ...................................................... 7798
  new-context-blocking-time .............................................. 7799
  num-pkts-ts ............................................................... 8000
  num-pkts-u-mode .......................................................... 8001
  num-updates-ir ............................................................ 8002
  optimistic-repeats ........................................................ 8003
  rtp-sn-p ................................................................. 8004
  rtp-sn-p-override ........................................................ 8005
  rtp-time-stride ........................................................... 8006
  rtp-ts-deviation .......................................................... 8007
  rtp-ts-stride ............................................................ 8008
  sliding-window-ts ....................................................... 8009
  total-jitter-ipv4 ........................................................ 8102
  total-jitter-ipv6 ........................................................ 8103
  unimode-timeout-to-fo-state ........................................... 8112
RoHC Profile Configuration Mode Commands ........................................ 7821
  common-options ........................................................................ 7822
  compression-options ................................................................. 7823
  decompression-options .............................................................. 7824
  end ............................................................................................ 7825
  exit ............................................................................................. 7826
RoHC Profile Decompression Configuration Mode Commands .......... 7827
  accept-delayed-pkts .................................................................. 7828
  context-timeout ......................................................................... 7829
  crc-errors-fo ............................................................................ 7830
  crc-errors-so ............................................................................ 7832
  end ............................................................................................ 7834
  exit ............................................................................................. 7835
  nack-limit ................................................................................ 7836
  optimistic-mode-ack .................................................................. 7837
  optimistic-mode-ack-limit .......................................................... 7838
  piggyback-wait-time ................................................................. 7839
  preferred-feedback-mode ............................................................ 7840
  rtp-sn-p ..................................................................................... 7842
  rtp-sn-p-override ....................................................................... 7843
  sliding-window-ts ..................................................................... 7844
  use-clock-option ........................................................................ 7845
  use-crc-option .......................................................................... 7846
  use-feedback ............................................................................. 7847
  use-jitter-option ....................................................................... 7848
  use-reject-option ...................................................................... 7849
  use-sn-not-valid-option ............................................................. 7850
  use-sn-option ............................................................................ 7851
Route-map Configuration Mode Commands ...................................... 7853
  end ............................................................................................ 7854
  exit ............................................................................................. 7855
  match as-path .......................................................................... 7856
  match interface ......................................................................... 7857
  match ip address ......................................................................... 7858
  match ip next-hop ...................................................................... 7859
  match ipv6 address ................................................................. 7860
  match ipv6 next-hop ............................................................... 7861
  match metric ............................................................................ 7862
  match origin ............................................................................. 7863
  match route-type external .......................................................... 7864
  match tag ................................................................................ 7865
  set as-path ............................................................................... 7866
  set ip next-hop ......................................................................... 7867
  set ipv6 next-hop ..................................................................... 7868
set metric ................................................................. 7869
set metric-type ......................................................... 7870
set origin ............................................................... 7871
set tag ................................................................. 7872
set weight ............................................................. 7873
RS-232 Port Configuration Mode Commands ......................... 7875
default ............................................................... 7876
end ........................................................................... 7877
exit ........................................................................... 7878
preferred slot ........................................................... 7879
snmp trap link-status .................................................. 7881
terminal ..................................................................... 7882
S1AP Cause Code Configuration Mode Commands ................. 7885
class ..................................................................... 7886
end ........................................................................... 7888
exit ........................................................................... 7889
S1-U Relay Configuration Mode Commands ......................... 7891
associate .................................................................. 7892
end ........................................................................... 7894
exit ........................................................................... 7895
ip ............................................................................. 7896
SAEGW Service Configuration Mode Commands ................... 7899
associate .................................................................. 7900
end ........................................................................... 7902
exit ........................................................................... 7903
SaMOG Service Configuration Mode Commands .................. 7905
associate .................................................................. 7906
end ........................................................................... 7908
exit ........................................................................... 7909
max-sessions ............................................................. 7910
timeout ...................................................................... 7911
SCCP Network Configuration Mode Commands ...................... 7913
associate .................................................................. 7914
description ............................................................... 7915
destination ............................................................... 7916
end ........................................................................... 7918
exit ........................................................................... 7919
global-title-translation ............................................... 7920
hop-count .................................................................. 7921
self-point-code .......................................................... 7922
timeout ...................................................................... 7923
SCTP Parameter Template Configuration Mode Commands ....... 7925
end ........................................................................... 7926
exit ........................................................................... 7927
sctp-alpha .................................................................. 7928
sctp-alt-accept-flag .................................................... 7929
sctp-beta .................................................................. 7930
sctp-checksum-type .................................................... 7931
sctp-cookie-life .......................................................... 7932
sctp-max-assoc-retx ..................................................... 7933
Service Redundancy Protocol Configuration Mode Commands ........... 7949
  audit ............................................................... 7950
  bind ............................................................... 7952
  chassis-mode ..................................................... 7953
  checkpoint session ............................................... 7954
  configuration-interval .......................................... 7955
  dead-interval ..................................................... 7956
  delay-interval .................................................... 7957
  delta-route-modifier ............................................ 7958
  end ................................................................. 7959
  exit .................................................................. 7960
  hello-interval ...................................................... 7961
  internal-switchover-retry-interval ...................... 7962
  monitor authentication-probe ................................ 7963
  monitor bfd .......................................................... 7965
  monitor bgp .......................................................... 7967
  monitor diameter ................................................... 7969
  num-internal-switchover-retry ................................ 7971
  peer-ip-address .................................................... 7972
  priority .............................................................. 7973
  route-modifier ..................................................... 7974
Session Event Module Configuration Mode Commands ................. 7975
  end ................................................................. 7976
  event ................................................................ 7977
  exit .................................................................. 7980
  file .................................................................. 7981
SGSN ASP Configuration Mode Commands ................................ 7985
  end ................................................................. 7986
  end-point ............................................................ 7987
  exit .................................................................. 7989
SGSN Global Configuration Mode Commands .............................. 7991
  aggregate-ipc-msg ............................................... 7992
  apn-resolve-dns-query snaptr .................................. 7994
  bssgp-message ms-flow-control-from-unknown-ms .......... 7995
  bssgp-message ptp-bvc-reset .................................. 7997
  bssgp-timer ......................................................... 7998
  bvc-unblock ........................................................ 7999
  dscp-template ...................................................... 8001
  dual-address-pdp ................................................... 8003

Cisco ASR 5x00 Command Line Interface Reference
SGSN Service Configuration Mode Commands ........................................... 8073
  accounting ................................................. 8074
  admin-disconnect-behavior ......................... 8076
  associate .................................................. 8078
  cc profile ................................................. 8081
  check-imei ................................................. 8083
  check-imei-timeout-action ......................... 8085
  core-network ............................................. 8086
  disable/enable super-charger ....................... 8087
  dns israu-mcc-mnc-encoding ......................... 8088
  end .......................................................... 8090
  exit .......................................................... 8091
  gmm .......................................................... 8092
  gs-service .................................................. 8096
  lac ........................................................... 8098
  max-pdp-contexts ........................................... 8099
  mobile-application-part ............................... 8100
  network-sharing cs-ps-coordination ................ 8102
  nri length ................................................. 8103
  override-lac-li ............................................ 8105
  override-rac-li ............................................ 8106
  rac ........................................................... 8107
  qos-modification .......................................... 8108
  ran-protocol .............................................. 8110
  reporting-action event-record ...................... 8111
  sgsn-number ................................................ 8112
  sgtp-service .............................................. 8113
  sm ........................................................... 8114

SGTP Service Configuration Mode Commands ........................................... 8117
  direct-tunnel-disabled-ggsn ............................ 8118
  disable-remote-restart-counter-verification .......... 8120
  end .......................................................... 8122
  exit .......................................................... 8123
  ggsn-fail-retry-timer .................................... 8124
  gn-delay-monitoring ...................................... 8125
  gtpc .......................................................... 8127
  gtpu .......................................................... 8131
  ignore-remote-restart-counter-change ................. 8134
  max-remote-restart-counter-change ................... 8135
  mbms .......................................................... 8137
  path-failure ................................................. 8138
  pool ............................................................ 8139

S-GW Service Configuration Mode Commands ........................................... 8141
  accounting context ........................................... 8142
  accounting mode ............................................ 8144
  accounting stop-trigger ................................... 8145
  associate ...................................................... 8146
  ddn failure-action ....................................... 8148
<table>
<thead>
<tr>
<th>Configuration Mode Commands</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subscriber Configuration</td>
<td>8203</td>
</tr>
<tr>
<td>(aaa)</td>
<td></td>
</tr>
<tr>
<td>access-link-ip-fragmentation</td>
<td></td>
</tr>
<tr>
<td>accounting-mode</td>
<td></td>
</tr>
<tr>
<td>active-charging-bw-policy</td>
<td>8206</td>
</tr>
<tr>
<td>active-charging-link-monitor</td>
<td></td>
</tr>
<tr>
<td>active-charging-rulebase</td>
<td>8207</td>
</tr>
<tr>
<td>always-on</td>
<td></td>
</tr>
<tr>
<td>asn-header-compression-rohc</td>
<td>8209</td>
</tr>
<tr>
<td>SSH Configuration</td>
<td>8195</td>
</tr>
<tr>
<td>(authorized-key)</td>
<td></td>
</tr>
<tr>
<td>(end)</td>
<td></td>
</tr>
<tr>
<td>(exit)</td>
<td></td>
</tr>
<tr>
<td>(listen)</td>
<td></td>
</tr>
<tr>
<td>(max-servers)</td>
<td></td>
</tr>
<tr>
<td>(subsystem)</td>
<td></td>
</tr>
<tr>
<td>SMS Service Configuration</td>
<td>8169</td>
</tr>
<tr>
<td>(cp-data)</td>
<td></td>
</tr>
<tr>
<td>(end)</td>
<td></td>
</tr>
<tr>
<td>(exit)</td>
<td></td>
</tr>
<tr>
<td>(mo-message-forwarding-dest)</td>
<td>8170</td>
</tr>
<tr>
<td>(smcs-address-restriction)</td>
<td>8171</td>
</tr>
<tr>
<td>(smcs-address-restriction-list)</td>
<td>8172</td>
</tr>
<tr>
<td>(smcs-address-restriction-type)</td>
<td>8173</td>
</tr>
<tr>
<td>(smcs-address-restriction-type-list)</td>
<td>8174</td>
</tr>
<tr>
<td>(smcs-address-selection-prioritization)</td>
<td>8175</td>
</tr>
<tr>
<td>(timeout)</td>
<td>8176</td>
</tr>
<tr>
<td>(timestamp)</td>
<td>8177</td>
</tr>
<tr>
<td>(threshold)</td>
<td>8178</td>
</tr>
<tr>
<td>(threshold1)</td>
<td>8179</td>
</tr>
<tr>
<td>(threshold2)</td>
<td>8180</td>
</tr>
<tr>
<td>(threshold3)</td>
<td>8181</td>
</tr>
<tr>
<td>SS7 Routing Domain</td>
<td>8181</td>
</tr>
<tr>
<td>(asp)</td>
<td></td>
</tr>
<tr>
<td>(description)</td>
<td></td>
</tr>
<tr>
<td>(end)</td>
<td></td>
</tr>
<tr>
<td>(exit)</td>
<td></td>
</tr>
<tr>
<td>(inbound-asp-identifier-validate)</td>
<td>8182</td>
</tr>
<tr>
<td>(linkset)</td>
<td>8183</td>
</tr>
<tr>
<td>(linkset-logical)</td>
<td></td>
</tr>
<tr>
<td>(peer-server)</td>
<td>8184</td>
</tr>
<tr>
<td>(route)</td>
<td>8185</td>
</tr>
<tr>
<td>(routing-context)</td>
<td>8186</td>
</tr>
<tr>
<td>(ssf)</td>
<td>8187</td>
</tr>
<tr>
<td>(vector)</td>
<td>8188</td>
</tr>
<tr>
<td>(vector-logical)</td>
<td></td>
</tr>
<tr>
<td>(vector-logical-logical)</td>
<td></td>
</tr>
<tr>
<td>(vector-logical-set)</td>
<td></td>
</tr>
<tr>
<td>(vector-set)</td>
<td></td>
</tr>
<tr>
<td>(vector-set-logical)</td>
<td></td>
</tr>
<tr>
<td>(vector-set-logical-logical)</td>
<td></td>
</tr>
<tr>
<td>(vector-set-set)</td>
<td></td>
</tr>
<tr>
<td>(vector-set-set-logical)</td>
<td></td>
</tr>
<tr>
<td>(vector-set-set-set)</td>
<td></td>
</tr>
<tr>
<td>(vector-set-set-set-logical)</td>
<td></td>
</tr>
<tr>
<td>(vector-set-set-set-set)</td>
<td></td>
</tr>
<tr>
<td>(vector-set-set-set-set-set)</td>
<td></td>
</tr>
<tr>
<td>(vector-set-set-set-set-set-set)</td>
<td>8189</td>
</tr>
<tr>
<td>Command</td>
<td>Page</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>ipv6 dns</td>
<td>8285</td>
</tr>
<tr>
<td>ipv6 dns-proxy</td>
<td>8287</td>
</tr>
<tr>
<td>ipv6 egress-address-filtering</td>
<td>8288</td>
</tr>
<tr>
<td>ipv6 initial-router-advt</td>
<td>8289</td>
</tr>
<tr>
<td>ipv6 interface-id</td>
<td>8291</td>
</tr>
<tr>
<td>ipv6 minimum-link-mtu</td>
<td>8292</td>
</tr>
<tr>
<td>ipv6 secondary-address</td>
<td>8293</td>
</tr>
<tr>
<td>l2tp send accounting-correlation-info</td>
<td>8294</td>
</tr>
<tr>
<td>l3-to-l2-tunnel address-policy</td>
<td>8295</td>
</tr>
<tr>
<td>loadbalance-tunnel-peers</td>
<td>8297</td>
</tr>
<tr>
<td>long-duration-action</td>
<td>8298</td>
</tr>
<tr>
<td>max-pdn-connections</td>
<td>8300</td>
</tr>
<tr>
<td>mediation-device</td>
<td>8301</td>
</tr>
<tr>
<td>mobile-ip</td>
<td>8303</td>
</tr>
<tr>
<td>mobile-ip ha</td>
<td>8306</td>
</tr>
<tr>
<td>mobile-ip reg-lifetime-override</td>
<td>8307</td>
</tr>
<tr>
<td>mobile-ip send access-technology</td>
<td>8308</td>
</tr>
<tr>
<td>mobile-ip send accounting-correlation-info</td>
<td>8309</td>
</tr>
<tr>
<td>mobile-ip send bsd</td>
<td>8310</td>
</tr>
<tr>
<td>mobile-ip ipv6</td>
<td>8311</td>
</tr>
<tr>
<td>nai-construction-domain</td>
<td>8313</td>
</tr>
<tr>
<td>nbns</td>
<td>8314</td>
</tr>
<tr>
<td>nexthop-forwarding-address</td>
<td>8315</td>
</tr>
<tr>
<td>npu qos</td>
<td>8316</td>
</tr>
<tr>
<td>nw-reachability-server</td>
<td>8318</td>
</tr>
<tr>
<td>outbound</td>
<td>8320</td>
</tr>
<tr>
<td>overload-disconnect</td>
<td>8321</td>
</tr>
<tr>
<td>password</td>
<td>8323</td>
</tr>
<tr>
<td>pdf mobile-ip</td>
<td>8325</td>
</tr>
<tr>
<td>permission</td>
<td>8326</td>
</tr>
<tr>
<td>policy ipv6 tunnel</td>
<td>8327</td>
</tr>
<tr>
<td>policy-group</td>
<td>8328</td>
</tr>
<tr>
<td>ppp</td>
<td>8329</td>
</tr>
<tr>
<td>prepaid 3gpp2</td>
<td>8332</td>
</tr>
<tr>
<td>prepaid custom</td>
<td>8334</td>
</tr>
<tr>
<td>prepaid unclassify</td>
<td>8336</td>
</tr>
<tr>
<td>prepaid voice-push</td>
<td>8337</td>
</tr>
<tr>
<td>prepaid wimax</td>
<td>8338</td>
</tr>
<tr>
<td>proxy-dns intercept list-name</td>
<td>8339</td>
</tr>
<tr>
<td>proxy-mip</td>
<td>8340</td>
</tr>
<tr>
<td>qos apn-ambr</td>
<td>8341</td>
</tr>
<tr>
<td>qos rate-limit</td>
<td>8343</td>
</tr>
<tr>
<td>qos traffic-police</td>
<td>8348</td>
</tr>
<tr>
<td>qos traffic-shape</td>
<td>8350</td>
</tr>
<tr>
<td>radius accounting</td>
<td>8353</td>
</tr>
<tr>
<td>radius group</td>
<td>8356</td>
</tr>
<tr>
<td>radius returned-framed-ip-address</td>
<td>8357</td>
</tr>
<tr>
<td>rohc-profile-name</td>
<td>8358</td>
</tr>
<tr>
<td>secondary ip pool</td>
<td>8359</td>
</tr>
<tr>
<td>send-destination-pgw</td>
<td>8360</td>
</tr>
<tr>
<td>simultaneous</td>
<td>8361</td>
</tr>
<tr>
<td>timeout absolute</td>
<td>8362</td>
</tr>
<tr>
<td>timeout idle</td>
<td>8363</td>
</tr>
<tr>
<td>timeout long-duration</td>
<td>8364</td>
</tr>
</tbody>
</table>
## TFTP Configuration Mode Commands
- tunnel address-policy
- tunnel iip
- tunnel ipsec
- tunnel l2tp
- w-apn

## Telnet Configuration Mode Commands
- telnet max servers

## TACACS+ Configuration Mode Commands
- accounting
- authorization
- end
- exit
- on-authen-fail
- on-network-error
- on-unknown-user
- rem_add client-ip
- server

## Telnet Configuration Mode Commands
- end
- max servers

## TFTP Configuration Mode Commands
- end
- max servers

## Traffic Policy Group Configuration Mode Commands
- end
- exit
- policy

## Traffic Policy-Map Configuration Mode Commands
- 3gpp2 data-over-signaling
- access-control
- accounting suppress
- accounting trigger
- class-map
- end
- exit
- flow-tp-trigger
- ip header-compression
- qos encaps-header
- qos traffic-police
- qos user-datagram dscp-marking
- sess-tp-trigger
- type

## Tunnel Interface Configuration Mode Commands
- description
- end
- exit
- ip address
- ipv6 address
- tunnel-mode

---

**Contents**

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>TFTP Configuration Mode Commands</td>
<td>8366</td>
</tr>
<tr>
<td>Telnet Configuration Mode Commands</td>
<td>8389</td>
</tr>
<tr>
<td>TFTP Configuration Mode Commands</td>
<td>8393</td>
</tr>
<tr>
<td>Traffic Policy Group Configuration Mode Commands</td>
<td>8397</td>
</tr>
<tr>
<td>Traffic Policy-Map Configuration Mode Commands</td>
<td>8403</td>
</tr>
<tr>
<td>Tunnel Interface Configuration Mode Commands</td>
<td>8423</td>
</tr>
</tbody>
</table>
### UDR Format Configuration Mode Commands
- attribute ........................................... 8431
- end .............................................. 8432
- event-label ....................................... 8433
- exit ............................................. 8434
- rule-variable ..................................... 8435
### UDR Module Configuration Mode Commands
- cdr .............................................. 8443
- end .............................................. 8444
- exit ............................................. 8445
- file ............................................. 8446
### Video Group Configuration Mode
- end .............................................. 8450
- exit ............................................. 8451
- keepalive-server .................................. 8460
- local-address .................................... 8462
- server .......................................... 8463
### VLAN Configuration Mode Commands
- bind interface .................................... 8466
- end .............................................. 8467
- exit ............................................. 8468
- ingress-mode .................................... 8469
- priority .......................................... 8470
- shutdown ........................................ 8471
- vlan-map ........................................ 8472
### WSG Lookup Priority List Configuration Mode Commands
- end .............................................. 8473
- exit ............................................. 8474
- priority .......................................... 8475
### WSG Service Configuration Mode Commands
- bind address ..................................... 8477
- deployment-mode .................................. 8478
- end .............................................. 8479
- exit ............................................. 8480
- ip .................................................. 8481
- ipv6 ............................................. 8482
- pre_fragment mtu ................................ 8484
About this Guide

This preface describes the *Cisco ASR 5x00 Command Line Interface Reference*, how it is organized and its document conventions.

This reference describes how to use the command line interface (CLI) to interact with the products supported by the ASR 5000 and ASR 5500. The CLI commands are organized by command modes in the code and in this reference. The command modes are presented alphabetically. The description of each command states the command’s function, describes its syntax, presents limitations when applicable, and offers an example of its usage.
Conventions Used

The following tables describe the conventions used throughout this documentation.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Notice Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>!</td>
<td>Information Note</td>
<td>Provides information about important features or instructions.</td>
</tr>
<tr>
<td>!</td>
<td>Caution</td>
<td>Alerts you of potential damage to a program, device, or system.</td>
</tr>
<tr>
<td>!</td>
<td>Warning</td>
<td>Alerts you of potential personal injury or fatality. May also alert you of potential electrical hazards.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Typeface Conventions</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Text represented as a screen display</td>
<td>This typeface represents displays that appear on your terminal screen, for example: Login:</td>
</tr>
<tr>
<td>Text represented as commands</td>
<td>This typeface represents commands that you enter, for example: show ip access-list. This document always gives the full form of a command in lowercase letters. Commands are not case sensitive.</td>
</tr>
<tr>
<td>Text represented as a command variable</td>
<td>This typeface represents a variable that is part of a command, for example: show card slot_number. slot_number is a variable representing the desired chassis slot number.</td>
</tr>
<tr>
<td>Text represented as menu or sub-menu names</td>
<td>This typeface represents menus and sub-menus that you access within a software application, for example: Click the File menu, then click New</td>
</tr>
</tbody>
</table>
## CLI Command Sections

The following table describes the individual sections in the command descriptions presented in this reference.

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Platform</td>
<td>The platform(s) on which the CLI command is supported.</td>
</tr>
<tr>
<td>Product</td>
<td>The product(s) supporting the CLI command.</td>
</tr>
<tr>
<td>Privilege</td>
<td>The user privilege levels having access to the CLI command. For more</td>
</tr>
<tr>
<td></td>
<td>information on user types and user privileges, refer to the <em>CLI Administrative Users</em> section in the <em>Command Line Interface Overview</em> chapter.</td>
</tr>
<tr>
<td>Mode</td>
<td>The command and configuration mode sequences to the CLI configuration mode for the CLI command. For more information on command modes, refer to the <em>CLI Command Modes</em> section in the <em>Command Line Interface Overview</em> chapter.</td>
</tr>
<tr>
<td>Syntax</td>
<td>The command’s syntax. For more information on CLI command syntax, refer to the <em>CLI Command Syntax</em> section in the <em>Command Line Interface Overview</em> chapter.</td>
</tr>
<tr>
<td>Usage</td>
<td>Information about the command’s usage including dependencies and limitations, if any.</td>
</tr>
<tr>
<td>Example</td>
<td>Example(s) of the command.</td>
</tr>
</tbody>
</table>
Supported Documents and Resources

Related Common Documentation

The following common documents are available:

- Cisco ASR 5000 Installation Guide
- Cisco ASR 5500 Installation Guide
- Cisco ASR 5000 System Administration Guide
- Cisco ASR 5500 System Administration Guide
- Cisco ASR 5x00 AAA Interface Administration and Reference
- Cisco ASR 5x00 GTPP Interface Administration and Reference
- Cisco ASR 5x00 Release Change Reference
- Cisco ASR 5x00 Statistics and Counters Reference
- Cisco ASR 5x00 Thresholding Configuration Guide

Related Product Documentation

The most up-to-date information for related products is available in the product-specific Release Notes provided with each product release.

The following product documents are also available and work in conjunction with this manual:

- Cisco ASR 5000 Application Detection and Control Administration Guide
- Cisco ASR 5000 Content Filtering Services Administration Guide
- Cisco ASR 5000 Enhanced Packet Data Gateway Administration Guide
- Cisco ASR 5000 Enhanced Wireless Access Gateway Administration Guide
- Cisco ASR 5000 External Storage Server Installation and Administration Guide
- Cisco ASR 5000 Intelligent Policy Control Function Administration Guide
- Cisco ASR 5000 IP Services Gateway Administration Guide
- Cisco ASR 5000 Mobile Video Gateway Administration Guide
- Cisco ASR 5000 Mobility Management Entity Administration Guide
- Cisco ASR 5000 Mobility Unified Reporting System Installation and Administration Guide
- Cisco ASR 5000 Packet Data Interworking Function Administration Guide
- Cisco ASR 5000 Personal Stateful Firewall Administration Guide
- Cisco ASR 5000 Policy Provisioning Tool Installation and Configuration Guide
- Cisco ASR 5000 Serving GPRS Support Node Administration Guide
• Cisco ASR 5000 Session Control Manager Administration Guide
• Cisco ASR 5000 Subscriber Service Controller Installation and Configuration Guide
• Cisco ASR 5000 3G Home NodeB Gateway Administration Guide
• Cisco ASR 5x00 Enhanced Charging Services Administration Guide
• Cisco ASR 5x00 Gateway GPRS Support Node Administration Guide
• Cisco ASR 5x00 Home Agent Administration Guide
• Cisco ASR 5x00 HRPD Serving Gateway Administration Guide
• Cisco ASR 5x00 Network Address Translation Administration Guide
• Cisco ASR 5x00 Packet Data Network Gateway Administration Guide
• Cisco ASR 5x00 Packet Data Serving Node Administration Guide
• Cisco ASR 5x00 Serving Gateway Administration Guide
• Cisco ASR 5x00 System Architecture Evolution Gateway Administration Guide

Obtaining Documentation

The most current Cisco documentation is available on the following website: http://www.cisco.com/cisco/web/psa/default.html
Use the following path selections to access the ASR 5x00 documentation:
Products > Wireless > Mobile Internet> Network Functions
Contacting Customer Support

Use the information in this section to contact customer support.

Refer to the support area of http://www.cisco.com for up-to-date product documentation or to submit a service request. A valid username and password are required to access this site. Please contact your Cisco sales or service representative for additional information.
Chapter 1
Command Line Interface Overview

This chapter describes the numerous features in the command line interface (CLI). It includes information about the architecture of the CLI, its command modes and user privileges, how to obtain help within the CLI, and other key items.

The operating system (StarOS™) controls the overall system logic, control processes, and the CLI. The CLI is a multi-threaded user interface that allows you to manipulate, configure, control and query the hardware and software components that make up the system and its hosted services. In addition, the CLI can host multiple instances of management and service configuration sessions. This allows multiple users to simultaneously access and manage multiple hosted services.

This section provides the following information about the CLI:

- CLI Structure
- CLI Command Modes
- CLI Administrative Users
- CLI Contexts
- Understanding the CLI Command Prompt
- CLI Command Syntax
- Entering and Viewing CLI Commands
- Obtaining CLI Help
- Exiting the CLI and CLI Command Modes
- Accessing the CLI
- Platform Related CLI Issues
- IP Address Notation
- Alphanumeric Strings
CLI Structure

CLI commands are strings of commands or keywords and user-specified arguments that set or modify specific parameters of the system. Commands are grouped by function and the various command modes with which they are associated.

The structure of the CLI is hierarchical. All users begin at a specific entry point into the system, called the Exec (Execute) Mode, and then navigate through the CLI according to their defined user privileges (access level) by using other command modes.
CLI Command Modes

There are two primary CLI command modes:

- **Exec (Execute) Mode:** The Exec Mode is the lowest level in the CLI. The Exec Mode is where you execute basic commands such as `show` and `ping`. When you log into the CLI, you are placed in this mode by default.

- **Config (Configuration) Mode:** The Config mode is accessible only by users with administrator and security administrator privileges. If you are an administrative user, in this mode you can add and configure contexts and access the configuration sub-modes to configure protocols, interfaces, ports, services, subscribers and other service-related items.

The entry point into the CLI is called Exec Mode. In the initial CLI login, all users are placed into the default local context, which is the CLI’s default management context. From this context, administrative users can access the Config Mode and define multiple service contexts.

Refer to the mode entry-path diagrams at the beginning of each mode chapter in the *Command Line Interface Reference*.

**Important:** The commands or keywords/variables that are available to the user vary based on platform type, StarOS version and installed license(s).
CLI Administrative Users

This section contains information on the administrative user types and privileges supported by the system.

Administrative User Types

There are two types of administrative users supported by the system:

- **Context-level administrative users**: This user type is configured at the context-level and relies on the AAA subsystems for validating user names and passwords during login. This is true for both administrative user accounts configured locally through a configuration file or on an external RADIUS or TACACS+ server. Passwords for these user types are assigned once and are accessible in the configuration file.

- **Local-users**: This user type provides support for ANSI T1.276-2003 password security protection. Local-user account information, such as passwords, password history, and lockout states, is maintained flash memory by the Shared Configuration Task (SCT). This information is maintained in a separate file, not in configuration files used by the system. As such, the configured local-user accounts are not visible with the rest of the system configuration.

Local-user and context-level administrative accounts can be used in parallel. However, a mechanism is provided to deactivate context-level administrative user accounts, thereby providing access only to local-user accounts.

Authenticating Administrative Users with RADIUS

To authorize users via RADIUS, you must include two RADIUS attributes in the RADIUS Access-Accept message:

- RFC 2865 standard Service-Type
- Starent Vendor-Specific Attribute (VSA) SN-Admin-Permission or SN1-Admin-Permission.

RADIUS SN-Admin-Permission / SN1-Admin-Permission AVP

The possible values for SN-Admin-Permission / SN1-Admin-Permission AVP are as follows:

- None = 0
- CLI = 1
- FTP = 2
- CLI-FTP = 3
- Intercept = 4
- CLI-Intercept = 5
- CLI-Intercept-FTP = 7
- ECS = 8
- CLI-ECS = 9
- CLI-FTP-ECS = 11
- CLI-Intercept-ECS = 13
- CLI-Intercept-FTP-ECS = 15
The default value is 1 (CLI).

**RADIUS Mapping System**

RADIUS server configuration depends on the type of server used and the instructions distributed by the server manufacturer. The following table shows the supported attribute/value mapping system that is constant, regardless of server manufacturer or model:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Framed</td>
<td>2</td>
</tr>
<tr>
<td>Administrative (Administrator)</td>
<td>6</td>
</tr>
<tr>
<td>NAS_Prompt</td>
<td>7</td>
</tr>
<tr>
<td>Authenticate_Only</td>
<td>8</td>
</tr>
<tr>
<td>Authorize_Only</td>
<td>17</td>
</tr>
<tr>
<td>Inspector</td>
<td>19650516</td>
</tr>
<tr>
<td>Security_Admin</td>
<td>19660618</td>
</tr>
</tbody>
</table>

**RADIUS Privileges**

There are four RADIUS privilege roles. The following table shows the relationship between the privilege roles in the CLI configuration and RADIUS Service-Type.

<table>
<thead>
<tr>
<th>CLI Configuration Parameter</th>
<th>RADIUS Service Type</th>
<th>show admin Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>administrator</td>
<td>Security_Admin (19660618)</td>
<td>admin</td>
</tr>
<tr>
<td>config_administrator</td>
<td>Administrative (6)</td>
<td>cfgadm</td>
</tr>
<tr>
<td>operator</td>
<td>NAS_Prompt (7)</td>
<td>oper</td>
</tr>
<tr>
<td>inspector</td>
<td>Inspector (19650516)</td>
<td>inspect</td>
</tr>
</tbody>
</table>

**Authenticating Administrative Users with TACACS+**

The ASR 5x00 or StarOS virtual machine is identified as a Network Access Server (NAS) and remotely accesses the Terminal Access Controller Access Control System+ (TACACS+) server for information about users who can perform administrative operations on the system.
The NAS is defined as a client-side requesting component associated with a specific IP address. StarOS only supports one NAS with one IP address. This NAS processes TACACS+ protocol packets within the local context. Several management services may be associated with a login.

StarOS only supports multiple-connection mode with a TACACS+ server. In a multiple-connection mode, each TACACS+ session opens and maintains a separate and private TCP connection to the server. When the session ends, this connection is always closed.

TACACS+ users and their passwords are defined and stored on the TACACS+ server. They are stored in a persistent space and are always known to the server while the server is running. The users are not directly known to the NAS.

Administrative User Privileges

Regardless of the administrative user type, the system supports four user privilege levels:

- **Inspector**: Inspectors are limited to a small number of read-only Exec Mode commands. The bulk of these are show commands for viewing a variety of statistics and conditions. The Inspector cannot execute show configuration commands and does not have the privilege to enter the Config Mode.

- **Operator**: Operators have read-only privileges to a larger subset of the Exec Mode commands. They can execute all commands that are part of the inspector mode, plus some system monitoring, statistic, and fault management functions. Operators do not have the ability to enter the Config Mode.

- **Administrator**: Administrators have read-write privileges and can execute any command in the CLI except for a few security-related commands that can only be configured by Security Administrators. Administrators can configure or modify system settings and can execute all system commands, including those available to the Operators and Inspectors.

- **Security Administrator**: Security Administrators have read-write privileges and can execute all CLI commands, including those available to Administrators, Operators, and Inspectors.

The following figure represents how user privileges are defined in the CLI configuration modes.

**Figure 1. User Privileges**

![User Privileges Diagram]

Though the privilege levels are the same regardless of user type, the corresponding user type names differ slightly. The following table displays the privilege level to administrative user type mappings:
Table 3. User Privilege to User Type Mapping

<table>
<thead>
<tr>
<th>User Type as Defined by T1.276-2003</th>
<th>Local-User Level User</th>
<th>Context-Level User</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Security Administrator</td>
<td>Security Administrator</td>
<td>Administrator</td>
</tr>
<tr>
<td>Application Security Administrator</td>
<td>Security Administrator</td>
<td>Administrator</td>
</tr>
<tr>
<td>System Administrator</td>
<td>Administrator</td>
<td>Config-Administrator</td>
</tr>
<tr>
<td>Application Administrator</td>
<td>Administrator</td>
<td>Config-Administrator</td>
</tr>
<tr>
<td>Application User/Operator</td>
<td>Operator</td>
<td>Operator</td>
</tr>
<tr>
<td>not applicable</td>
<td>Inspector</td>
<td>Inspector</td>
</tr>
</tbody>
</table>

Configure context-level administrative users in the Context Configuration Mode with the `administrator`, `config-administrator`, `operator`, and `inspector` commands.

Configure local-user administrative users at the Global Configuration Mode with the `local-user username` command.

You can further refine administrative levels to include access to certain features with the following feature-use administrative user options:

- **Lawful Intercept (LI) Administrative User**: To configure and manage LI-related issues, configure at least one administrative user account with LI functionality privileges.

  **Important**: This privilege is available only for context-level administrative users. In addition, to ensure security in accordance with the standards, LI administrative users must access the system through the Secure Shell Protocol (SSH).

- **Enhanced Charging Service (ECS) Administrative User**: To log in and execute ECS-related commands, configure at least one administrative user account with ECS functionality privileges.

All system users can be configured within any context. However, it is recommended that you configure users in the system’s management context called local. Refer to sections later in this chapter for additional information about contexts.

### Allowed Commands per User Type

With the exception of security administrators, all other management users are limited to a subset of the entire command list. This section defines the commands allowed for each management user type.

#### Inspector Mode Commands

In the Exec Mode, system inspectors can access the following commands:

- `abort`
- `autoconfirm`
- `context`
- `crypto-group`
- `default terminal`
• exit
• help
• logs checkpoint
• no logging active
• no logging trace
• no reveal disabled commands
• no timestamps
• no autocomfirm
• ping
• reveal disabled commands
• show (except show snmp communities and show snmp transports)
• sleep
• start crypto security-association
• terminal length
• terminal width
• timestamps
• traceroute

Operator Mode Commands

In the Exec Mode, system operators can access all inspector mode commands plus the following commands:
• aaa test
• alarm cutoff
• bulkstats force
• card
• clear (a subset of all clear command variations)
• debug
• dhcp test
• gtpc test
• gtpp interim
• gtpp test
• gtpu test
• gtpv0 test
• host
• logging active
• logging filter
• logging trace
• monitor protocol
• monitor subscriber
• newcall
• no card
• no debug
• no newcall policy
• port
• ppp echo-test
• radius interim accounting
• radius test
• rlogin
• show access-group
• show access-list
• show access-flow
• show access statistics
• show configuration
• show snmp transports
• ssh
• telnet
• test alarm

Administrator Mode Commands

Administrators can access all system commands except:

• Context Configuration Mode:
  • config-administrator
  • operator
  • inspector
  • administrator

• Global Configuration Mode:
  • snmp community
  • snmp user
  • local-user
  • suspend local-user

• Exec Mode:
  • show snmp communities
  • clear (all clear command variations)
  • show local-user
  • password change local-user
Security Administrator Mode Commands

Security administrators can access all system commands.
CLI Contexts

A context is a group of configuration parameters that apply to the ports, interfaces, and protocols supported by the system. You can configure multiple contexts on the system, each of which resides as a separate, logically independent instance on the same physical device. The CLI can host multiple contexts within a single physical device.

This allows wireless service providers to use the same system to support:

- Different levels of service
- Multiple wholesale or enterprise customers or customer groups
- Different classes of customers based on defined Class of Service (CoS) parameters
- IP address pools across multiple contexts, thus saving IP address allocation
- Enhanced security

Each defined context operates independently from any other context(s) in the system. Each context contains its own CLI instance, IP routing tables, access filters, compression methods, and other configured data.

By default, a single system-wide context called “local”, is used exclusively for the management of the system. Think of the local context as the root directory of the system, since you can define and access all other contexts from this point. You cannot delete the local context.

From this location in the CLI, you can:

- Create and configure other service contexts that contain different service configurations
- Configure system-wide services such as CORBA and SNMP management interfaces, physical management ports, system messages, and others

**Important:** The system requires that you define at least one context in addition to the local context. This isolates system management functions from application or service functions.

Administrative users add contexts through the Global Configuration Mode. A substantial advantage of configuring numerous service contexts is that it allows operators to broadly distribute different subscribers across the system. This greatly enhances the performance of the system and minimizes the loss of sessions should a failure occur.
Understanding the CLI Command Prompt

The CLI provides an intuitive command prompt that informs you of:

- Exactly where you are located within the CLI
- The command mode you are using
- Your user privilege level.

The following figure shows the various components of the command prompt.

Figure 2. CLI Command Prompt
CLI Command Syntax

This section describes the components of the CLI command syntax that you should be familiar with prior to using the CLI. These include:

- **Commands**: Specific words that precede, or initiate, a specific function.
- **Keywords**: Specific words that follow a command to more clearly dictate the command’s function.
- **Variables**: Alphanumeric values that are user-supplied as part of the command syntax. Sometimes referred to as arguments, these terms further specify the command function.
- **Repetitive keywords (+)**: Specific keyword, that when followed by a plus (+) sign, indicates that more than one of the keywords can be entered within a single command.

In the following example, `port_number` and `slot_number` are the command variables for the `info` keyword:

```
show port info slot_number/
```

`port_number/slot_number` is a variable representing a particular Ethernet slot/port on an ASR 5x00 or virtualized platform. See the *System Administration Guide* specific to the platform type for actual slot/port ranges.
Entering and Viewing CLI Commands

This section describes various methods for entering commands into the CLI.
Typing each command keyword, argument, and variable can be time-consuming and increase your chance of making mistakes. The CLI therefore, supports the following features to assist you in entering commands quickly and more accurately. Other features allow you to view the display and review previously entered commands.

Entering Partial CLI Commands

In all of the modes, the CLI recognizes partially-typed commands and keywords, as long as you enter enough characters for the command to be unambiguously recognized by the system. If you do not enter enough characters for the system to recognize a unique command or keyword, it returns a message listing all possible matches for the partial entry.

If you enter the partial command `conf` and press `Enter`, you enter the Global Configuration Mode. If you were to enter only `con`, the system would respond with the message:

Ambiguous Command

CLI Command Auto-completion

Use the command auto-completion feature to automatically complete unique CLI commands. Press the Tab key after entering enough characters to enable this feature.

```
[local]host_name# sho<Tab>
[local]host_name# show
```

If you do not enter enough characters to allow the CLI to determine the appropriate command to use, the CLI displays all commands that match the characters you entered with auto-completion:

```
[local]host_name# sh<Tab>
show shutdown
[local]host_name#
```

Enter a question mark (?) after a partial command to display all of the possible matching commands, and their related help text.

```
[local]host_name# sh?
shutdown - Terminates execution of all tasks within the entire chassis
show - Displays information based on a specified argument
[local]host_name#
```
Using CLI Auto-Pagination

When you enter commands whose expected results exceed the terminal window’s vertical display, the auto-pagination function pauses the display each time the terminal window reaches its display limit. Press any key to display the next screen of results.

By default, auto-pagination functionality is disabled. To enable auto-pagination, type the pipe command: `| more`.

```
[local]host_name# show configuration | more
```

⚠️ **Important:** When auto-pagination is enabled, if a command’s output exceeds the terminal window’s vertical display parameters, you can exit by entering "q". This returns you to the CLI prompt.

Using CLI Autoconfirmation

By default, the system is configured to prompt all administrative users with a confirmation prior to executing certain commands. This functionality serves two purposes:

- Helps ensure that you do not execute an unwanted configuration change.

For example, to save a configuration:

```
[local]host_name# save configuration
Are you sure ? [Yes | No]:
```

- Indicates potential misspellings of names during configuration. The first time you configure an element name (context, subscribers, services, etc.), the prompt is displayed. The prompt is not displayed for subsequent entries of the name. Therefore, if you see the confirmation prompt after entering the name of a previously configured element, it is likely that you misspelled the name.

You create a context named `newcontext`:

```
[local]host_name(config)# context newcontext
Are you sure ? [Yes | No]: yes
[newcontext]host_name(config-ctx)#
```

You revisit the context named `newcontext`:

```
[local]host_name(config)# context newcontext
[newcontext]host_name(config-ctx)#
```

On another occasion, you misspell the context named `newcontext`:

```
[local]host_name(config)# context mewcontext
Are you sure ? [Yes | No]: n
Action aborted
[local]host_name(config)#
```
After aborting the above action, you can again revisit `newcontext`:

```plaintext
[local]host_name(config)# context newcontext
[newcontext]host_name(config-ctx)#
```

You can control CLI autoconfirmation at the following levels:

- **Specific administrative user sessions**: To enable or disable autoconfirmation, use the `[no] autoconfirm` commands while in the Exec Mode.
- **All Future Sessions**: To disable or re-enable autoconfirmation for all future sessions, use the `[no] autoconfirm` commands while in the Global Configuration Mode.
- **For specific commands**: Disable autoconfirmation for various commands that support the `-noconfirm` keyword, such as the save configuration or card reboot commands.

**Regulating the Command Output**

For many CLI commands, you can use `| grep` and/or `| more` keywords to regulate or control the command’s output.

**grep for Regular Expressions**

Use the `| grep` keyword to filter through a command’s output for certain expressions or patterns. Only those portions of the output that contain or exclude the pattern are displayed. The `| grep` has the following syntax:

```
| grep [ -E | -i | -n | -v | --extended-regexp | --ignore-case | --invert-match | --line-number ] expression
```

<table>
<thead>
<tr>
<th>Alternative Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-E</code></td>
<td>Match using extended regular expressions (EREs). Treat each pattern specified as an ERE (“IEEE Std 1003.1-2001, Section 9.4, Extended Regular Expressions”). If any entire ERE pattern matches some part of an input line excluding the terminating <code>&lt;newline&gt;</code>, the line shall be matched. A null ERE shall match every line.</td>
</tr>
<tr>
<td><code>-i</code></td>
<td>Perform pattern matching in searches without regard to case. Lower case matches the same as upper case.</td>
</tr>
<tr>
<td><code>-n</code></td>
<td>Precede each output line by its relative line number in the file, each file starting at line 1. The line number counter is reset for each file processed.</td>
</tr>
<tr>
<td><code>-v</code></td>
<td>Select lines not matching any of the specified patterns. If the <code>-v</code> option is not specified, selected lines shall be those that match any of the specified patterns.</td>
</tr>
<tr>
<td><code>--extended-regexp</code></td>
<td>The long form of the <code>-E</code> option.</td>
</tr>
<tr>
<td><code>--ignore-case</code></td>
<td>The long form of the <code>-i</code> option.</td>
</tr>
<tr>
<td><code>--invert-match</code></td>
<td>The long form of the <code>-v</code> option.</td>
</tr>
<tr>
<td><code>expression</code></td>
<td>Specifies the character pattern to find in the command’s output as an alphanumeric string of 1 to 256 characters.</td>
</tr>
</tbody>
</table>
A regular expression is a pattern that describes a set of strings. Regular expressions are constructed analogously to arithmetic expressions, by using various operators to combine smaller expressions. For additional information, refer to ISO/IEC/IEEE 9945:2009 Information technology – Portable Operating System Interface (POSIX®) Base Specifications, Issue 7.

**more Command**

Use the `| more` keyword to pause the terminal each time the terminal window reaches its display limit. Press any key to display the next screen. The function of this keyword is identical to the `autoless` command, except that you must manually enter it on a command-by-command basis.

**Viewing Command History**

To view a history of all commands line by line, simply scroll up or down with the `<up arrow>` and `<down arrow>` cursor keys on the keyboard.

The operating system supports EMACS-style text editing commands. This standard UNIX text editor format allows you to use keyboard-based shortcut keys for maneuvering around the CLI. The following table lists these available shortcut keys.

<table>
<thead>
<tr>
<th>Shortcut Keys</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;Ctrl + p&gt;</code> and <code>&lt;up arrow&gt;</code></td>
<td>Recalls previous command in the command history</td>
</tr>
<tr>
<td><code>&lt;Ctrl + n&gt;</code> and <code>&lt;down arrow&gt;</code></td>
<td>Recalls next command in the command history</td>
</tr>
<tr>
<td><code>&lt;Ctrl + f&gt;</code> and <code>&lt;right arrow&gt;</code></td>
<td>Moves cursor forward by one character in command line</td>
</tr>
<tr>
<td><code>&lt;Ctrl + b&gt;</code> and <code>&lt;left arrow&gt;</code></td>
<td>Moves cursor backward by one character in command line</td>
</tr>
<tr>
<td><code>&lt;Esc&gt; + &lt;f&gt;</code></td>
<td>Moves cursor forward by one word in command line</td>
</tr>
<tr>
<td><code>&lt;Esc&gt; + &lt;b&gt;</code></td>
<td>Moves cursor backward by one word in command line</td>
</tr>
<tr>
<td><code>&lt;Ctrl&gt; + &lt;a&gt;</code></td>
<td>Moves cursor to the beginning of the command line</td>
</tr>
<tr>
<td><code>&lt;Ctrl&gt; + &lt;e&gt;</code></td>
<td>Moves cursor to the end of the command line</td>
</tr>
<tr>
<td><code>&lt;Ctrl&gt; + &lt;k&gt;</code></td>
<td>Deletes the current command line from the insertion point to the end of the line</td>
</tr>
<tr>
<td><code>&lt;Ctrl&gt; + &lt;u&gt;</code></td>
<td>Deletes the current command line from the insertion point to the beginning of the line</td>
</tr>
<tr>
<td><code>&lt;Ctrl&gt; + &lt;d&gt;</code></td>
<td>Deletes a single character in the current command line</td>
</tr>
<tr>
<td><code>&lt;Esc&gt; + &lt;d&gt;</code></td>
<td>Deletes a word in the current command line</td>
</tr>
<tr>
<td><code>&lt;Ctrl&gt; + &lt;c&gt;</code></td>
<td>Quits editing the current line</td>
</tr>
<tr>
<td><code>&lt;Ctrl&gt; + &lt;l&gt;</code></td>
<td>Refreshes the display</td>
</tr>
<tr>
<td><code>&lt;Ctrl&gt; + &lt;t&gt;</code></td>
<td>Transposes (or switches) the two characters surrounding the insertion point</td>
</tr>
</tbody>
</table>
Obtaining CLI Help

The CLI provides context-sensitive help for every command token and keyword available to you. To obtain, use one of these methods:

- **Command Help**: Command help provides assistance for a specific command. Type a question mark (?) at the end of the specific command to access help.

  ```
  [local]host_name# test?
  test - Performs test on followed mechanism
  ```

- **Keyword Help**: Keyword help provides assistance in determining the next keyword, argument, or option to use in the command syntax. Enter the command keyword, enter a space, and then type a question mark (?).

  ```
  [local]host_name# test alarm ?
  audible - Tests internal audible alarm buzzer on SPC
  central-office - Tests specified central office alarm relays
  <cr> - newline
  ```

- **Variable Help**: Variable help provides the correct format, value, or information type for each variable that is part of the command syntax. For commands with variables, enter the command keyword, enter a space, and then type a question mark (?).

  ```
  [local]host_name# show card info ?
  <Enter card number as an integer ranging 1 to n>
  | - Pipeline
  <cr> - Carriage Return or <Enter> key
  ```
Exiting the CLI and CLI Command Modes

A CLI session is defined as the successful login into the CLI. When you establish a CLI session, you are placed into the system’s Exec Mode. Depending upon your user privilege level, you can:

- Use the local context to perform system management functions.
- Move to an assigned context and work in Exec Mode.
- Move to an assigned context as an administrative user and work in Global Configuration Mode or other configuration sub-mode.

This section addresses how to properly exit the various modes and the CLI.

Exiting Configuration Sub-modes

To exit a configuration sub-mode and return to the next highest configuration sub-mode or Global Configuration Mode, type the exit command at the system prompt.

```
[context_name]host_name(config-ctx)# exit
[local]host_name(config)#
```

**Important:** The CLI supports implicit mode-exits when using configuration files. Therefore, configuration files do not have to contain all of the required exit commands for you to leave various sub-config modes.

To exit a sub-mode and return to the Exec Mode, enter the end command.

```
[local]host_name(config-ctx)# end
[local]host_name#
```

Exiting Global Configuration Mode

To exit Global Configuration Mode, and return to the Exec Mode prompt, type the exit command at the prompt.

Ending a CLI Session

To end a CLI session and exit the CLI, type the exit command at the Exec Mode prompt.
Accessing the CLI

Access the CLI through the following methods:

- Local login through an ASR 5x00 Console port via a serial connection with a management card
- Local login through a vConsole port via the hypervisor that initiated the StarOS virtual machine
- Remote login using Telnet and Secure Shell (SSH) access to the CLI through any IP interface on the system.

You can use remote login methods only after the system has been configured to support the various access methods.

Important: Even though you can access the CLI remotely through any available IP interface, management traffic should be isolated from network traffic by using one of the dedicated management interfaces supported on the ASR 5x00 platform or StarOS virtual machine.

Multiple CLI sessions are supported, but the number of sessions varies based on the amount of available memory. The Resource Manager reserves enough resources so that as a minimum up to 15 CLI sessions are assured. One of the CLI sessions is always reserved for use exclusively by a CLI session on a Console or vConsole interface. Additional CLI sessions beyond the pre-reserved set are permitted if sufficient CPU or vCPU resources are available. If the Resource Manager is unable to reserve additional resources, you are prompted whether to allow the system to create the new CLI session, even without the reserved resources.

Accessing the CLI Locally Using an ASR 5x00 Console Port

This section provides instructions for accessing the CLI locally through a Console port on the ASR 5x00 platform. Establish a connection between the serial Console port on an ASR 5x00 and a workstation that has a communications application that accesses the workstation’s serial port, such as Minicom for Linux or HyperTerminal® for MicroSoft Windows®. Refer to the ASR 5x00 Installation Guide for detailed information on connecting to a serial Console port.

1. Configure the communications application to support the following:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Baud Rate</td>
<td>115,200 bps</td>
</tr>
<tr>
<td>Data Bits</td>
<td>8</td>
</tr>
<tr>
<td>Parity</td>
<td>None</td>
</tr>
<tr>
<td>Stop Bits</td>
<td>1</td>
</tr>
<tr>
<td>Flow Control</td>
<td>None</td>
</tr>
</tbody>
</table>

Important: To change the configuration defined in the table above, modify the terminal command located in the Global Configuration Mode.

2. At the terminal window, press Enter.
3. If no configuration file is present (that is, this is the first time the system is powered), the CLI prompts you as to whether or not you want to use the Quick Setup Wizard. If the system was configured previously, you are prompted to enter a username and password.

**Accessing the CLI Locally Using a vConsole Port**

You connect to a vConsole port via a hypervisor that initiates a virtual machine running StarOS. Refer to the hypervisor user documentation and the VPC *Administration Guide* for additional information.

**Remotely Accessing the CLI**

To remotely access the CLI through a defined management interface, you must first configure the remote access method (such as Telnet or SSH).

You can find examples of how to configure this in the *Getting Started* chapter in the *System Administration Guide*. 
Platform Related CLI Issues

StarOS runs on ASR 5x00 and virtualized platforms. However, all CLI features and functions are not supported by all platforms.

This guide includes descriptions for all commands that have been qualified to run under StarOS. There may be specific instances where a command cannot be run and an error message is generated.

As features become fully qualified on specific or all platforms, this guide will be revised to reflect supported commands. For additional information, refer to the Release Notes provided with each StarOS version.
IP Address Notation

When configuring a port interface via the CLI you may be required to enter an IP address. The CLI always accepts an IPv4 address, and in some cases accepts an IPv6 address as an alternative.

For some configuration commands, the CLI also accepts CIDR notation when entering an IP address. Always view the online Help for the CLI command to verify acceptable forms of IP address notation.

IPv4 Dotted-Decimal Notation

An Internet Protocol Version 4 (IPv4) address consists of 32 bits divided into four octets. These four octets are written in decimal numbers, ranging from 0 to 255, and are concatenated as a character string with full stop delimiters (dots) between each number.

For example, the address of the loopback interface, usually assigned the host name localhost, is 127.0.0.1. It consists of the four binary octets 01111111, 00000000, 00000000, and 00000001, forming the full 32-bit address.

IPv4 allows 32 bits for an Internet Protocol address and can, therefore, support $2^{32}$ (4,294,967,296) addresses.

IPv6 Colon-Separated-Hexadecimal Notation

An Internet Protocol Version 6 (IPv6) address has two logical parts: a 64-bit network prefix, and a 64-bit host address part. An IPv6 address is represented by eight groups of 16-bit hexadecimal values separated by colons (:).

A typical example of a full IPv6 address is 2001:0db8:85a3:0000:0000:8a2e:0370:7334

The hexadecimal digits are case-insensitive.

The 128-bit IPv6 address can be abbreviated with the following rules:

- Leading zeroes within a 16-bit value may be omitted. For example, the address fe80:0000:0000:0000:0202:b3ff:fe1e:8329 may be written as fe80:0:0:0:2:02:b3ff:fe1e:8329
- One group of consecutive zeroes within an address may be replaced by a double colon. For example, fe80:0:0:0:202:b3ff:fe1e:8329 becomes fe80::202:b3ff:fe1e:8329

IPv6 allows 128 bits for an Internet Protocol address and can support $2^{128}$ (340,282,366,920,938,000,000,000,000,000,000,000) internet addresses.

CIDR Notation

Classless Inter-Domain Routing (CIDR) notation is a compact specification of an Internet Protocol address and its associated routing prefix. It is used for both IPv4 and IPv6 addressing in networking architectures.

CIDR is a bitwise, prefix-based standard for the interpretation of IP addresses. It facilitates routing by allowing blocks of addresses to be grouped into single routing table entries. These groups (CIDR blocks) share an initial sequence of bits in the binary representation of their IP addresses.

CIDR notation is constructed from the IP address and the prefix size, the latter being the number of leading 1 bits of the routing prefix. The IP address is expressed according to the standards of IPv4 or IPv6. It is followed by a separator character, the slash (/) character, and the prefix size expressed as a decimal number.
**Important**: On the ASR 5000, routes with IPv6 prefix lengths less than /12 and between the range of /64 and /128 are not supported.

The address may denote a single, distinct, interface address or the beginning address of an entire network. In the latter case the CIDR notation specifies the address block allocation of the network. The maximum size of the network is given by the number of addresses that are possible with the remaining, least-significant bits below the prefix. This is often called the host identifier.

For example:

- the address specification 192.168.100.1/24 represents the given IPv4 address and its associated routing prefix 192.168.100.0, or equivalently, its subnet mask 255.255.255.0.
- the IPv4 block 192.168.0.0/22 represents the 1024 IPv4 addresses from 192.168.0.0 to 192.168.3.255.
- the IPv6 block 2001:DB8::/48 represents the IPv6 addresses from 2001:DB8:0:0:0:0:0:0 to 2001:DB8:0:FFFF:FFFF:FFFF:FFFF:FFFF.
- ::1/128 represents the IPv6 loopback address. Its prefix size is 128, the size of the address itself, indicating that this facility consists of only this one address.

The number of addresses of a subnet defined by the mask or prefix can be calculated as 2, in which the address size for IPv4 is 32 and for IPv6 is 128. For example, in IPv4, a mask of /29 gives 8 addresses.
Alphanumeric Strings

Some CLI commands require the entry of a string of characters that can contain a contiguous collection of alphabetic, numeric, or alphanumeric characters with a defined minimum and maximum length (number of characters).

Character Set

The alphanumeric character set is a combination of alphabetic characters (Latin letters) and numeric characters (Arabic numerals). The set consists of the letters A to Z (uppercase) and a to z (lowercase) and the numbers 0 to 9. The underscore character ( _ ) and dash/hyphen character ( - ) can also be used.

Blank spaces (whitespaces or SPACE characters) should mostly be avoided in alphabetic, numeric, and alphanumeric strings, except in certain ruledef formats, such as time/date stamps.

The following special characters can be used in ruledefs, APNs, license keys and other configuration/display parameters:

- < > (arrow brackets) [less than or greater than]
- * (asterisk) [wildcard]
- : (colon)
- $ (dollar sign) [wildcard]
- . (dot)
- = (equals sign)
- ! (exclamation point)
- % (percent)
- / (slash - forward)
- | (vertical bar)

The following special characters can be used to delimit the domain from the user name for global AAA functions:

- @ (at sign)
- - (dash or hyphen)
- # (hash or pound sign)
- % (percent)
- \ (slash - backward) [must be entered as double slash \\]
- / (slash - forward)

Quoted Strings

If descriptive text requires the use of spaces between words, the string must be entered within double quotation marks (" ").

```
interface "Rack 3 Chassis 1 port 5/2"
```
Chapter 2
AAA Server Group Configuration Mode Commands

The AAA Server Group Configuration Mode is used to create and manage the Diameter/RADIUS server groups within the context or system. AAA server group facilitates management of group (list) of servers at per subscriber/APNrealm level for AAA functionality.

Mode

Exec > Global Configuration > Context Configuration > AAA Server Group Configuration

`configure > context context_name > aaa group group_name`

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-aaa-group)#`

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
diameter accounting

This command configures Diameter accounting parameters.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > AAA Server Group Configuration
configure > context context_name > aaa group group_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-aaa-group)#

Syntax

diameter accounting { dictionary { aaa-custom1 | aaa-custom10 | aaa-custom2 | aaa-custom3 |
  aaa-custom4 | aaa-custom5 | aaa-custom6 | aaa-custom7 | aaa-custom8 | aaa-custom9 |
  dynamic-load | nasreq | rf-plus } | endpoint endpoint_name | hd-mode fall-back-to-local |
  hd-storage-policy hd_policy | max-retries max_retries | max-transmissions |
  max_transmissions | request-timeout request_timeout_duration | server host_name priority |
  upgrade-dict-avps { 3gpp-rel10 | 3gpp-rel9 } }

default diameter accounting { dictionary | hd-mode | max-retries | max-transmissions |
  request-timeout | upgrade-dict-avps }

no diameter accounting { endpoint | hd-mode | hd-storage-policy | max-retries | max-transmissions |
  server host_name | upgrade-dict-avps }

no diameter accounting { endpoint | hd-mode | hd-storage-policy | max-retries | max-transmissions |
  server host_name | upgrade-dict-avps }

endpoint: Removes the configured accounting endpoint, and the default accounting server configured in the
default AAA group will be used.
hd-mode: Sends records to the Diameter server, if all Diameter servers are down or unreachable, then copies
records to the local hard disk drive (HDD) and periodically retries the Diameter server.
hd-storage-policy: Disables use of the specified HD storage policy.
max-retries: Disables the configured retry attempts for Diameter accounting in the current AAA group.
max-transmissions: Disables the configured maximum transmission attempts for Diameter accounting in
the current AAA group.
server host_name: Removes the configured Diameter host host_name from this AAA server group for
Diameter accounting.
upgrade-dict-avps: Sets the release version to 3GPP Rel. 8 for upgrading Diameter accounting dictionary
in the current AAA group.

default diameter accounting { dictionary | hd-mode | max-retries | max-transmissions |
  request-timeout | upgrade-dict-avps }

dictionary: Sets the context’s dictionary as the system default.
**hd-mode**: Sends records to the Diameter server, if all Diameter servers are down or unreachable, then copies records to the local HDD and periodically retries the Diameter server.

**max-retries**: Sets the retry attempts for Diameter accounting in the current AAA group to default 0 (disable).

**max-transmissions**: Sets the configured maximum transmission attempts for Diameter accounting in the current AAA group to default 0 (disable).

**request-timeout**: Sets the timeout duration, in seconds, for Diameter accounting requests in the current AAA group to default 20.

**upgrade-dict-avps**: Sets the release version to 3GPP Rel. 8 for upgrading Diameter accounting dictionary in the current AAA group.

```
dictionary { aaa-custom1 | aaa-custom10 | aaa-custom2 | aaa-custom3 | aaa-custom4 | aaa-custom5 | aaa-custom6 | aaa-custom7 | aaa-custom8 | aaa-custom9 | dynamic-load | nasreq | rf-plus }
```

Specifies the Diameter accounting dictionary.

**aaa-custom1 ... aaa-custom10**: Configures the custom dictionaries. Even though the CLI syntax supports several custom dictionaries, not necessarily all of them have been defined. If a custom dictionary that has not been implemented is selected, the default dictionary will be used.

**dynamic-load**: Configures the dynamically loaded Diameter dictionary. The dictionary name must be an alphanumeric string of 1 through 15 characters. For more information on dynamic loading of Diameter dictionaries, see the [diameter dynamic-dictionary](#) in the Global Configuration Mode Commands chapter of this guide.

**nasreq**: nasreq dictionary—the dictionary as defined by RFC 3588.

**rf-plus**: RF Plus dictionary.

```
endpoint endpoint_name
```

Enables Diameter to be used for accounting, and specifies which Diameter endpoint to use. **endpoint_name** must be a string of 1 through 63 characters.

```
hd-mode fall-back-to-local
```

Specifies that records be copied to the local HDD if the Diameter server is down or unreachable. CDF/CGF will pull the records through SFTP.

```
hd-storage-policy hd_policy
```

Associates the specified HD Storage policy with the AAA group. **hd_policy** must be the name of a configured HD Storage policy, and must be an alphanumeric string of 1 through 63 characters.

HD Storage policies are configured through the Global Configuration Mode. This and the **hd-mode** command are used to enable the storage of Rf Diameter Messages to HDD in case all Diameter Servers are down or unreachable.

```
max-retries max_retries
```

Specifies how many times a Diameter request should be retried with the same server, if the server fails to respond to a request. **max_retries** specifies the maximum number of retry attempts, and must be an integer from 1 through 1000. Default: 0
max-transmissions max_transmissions
Specifies the maximum number of transmission attempts for a Diameter request. Use this in conjunction with
the max-retries max_retries option to control how many servers will be attempted to communicate
with.
max_transmissions must be an integer from 1 through 1000.
Default: 0

request-timeout request_timeout_duration
Specifies the number of seconds the system will wait for a response from a Diameter server before re-
transmitting the request.
request_timeout_duration specifies the number of seconds, and must be an integer from 1 through
3600.
Default: 20

server host_name priority priority
Specifies the current context Diameter accounting server’s host name and priority.
host_name specifies the Diameter host name, and must be an alphanumeric string of 1 through 63
characters.
priority specifies the relative priority of this Diameter host. The priority is used in server selection. The
priority must be an integer from 1 through 1000.

upgrade-dict-avps { 3gpp-rel10 | 3gpp-rel9 }
Specifies to upgrade Diameter accounting dictionary to 3GPP Rel. 9 version or 3GPP Rel. 10 version.
3gpp-rel10: Upgrades the dictionary to 3GPP Rel. 10 version.
3gpp-rel9: Upgrades the dictionary to 3GPP Rel. 9 version.
Default: Sets the release version to 3GPP Rel. 8

Usage
Use this command to manage the Diameter accounting options according to the Diameter server used for the
context.

Example
The following command configures the Diameter accounting dictionary, aaa-custom10:

    diameter accounting dictionary aaa-custom10

The following command configures the Diameter endpoint, EAPI:

    diameter accounting endpoint EAPI

The following commands configure Diameter accounting options:

    diameter accounting max-retries 4
    diameter accounting max-transmissions 2
    diameter accounting request-timeout 10
    diameter accounting server svc priority 1
diameter authentication

This command configures Diameter authentication parameters.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > AAA Server Group Configuration

configure > context context_name > aaa group group_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-aaa-group)#

Syntax

diameter authentication { dictionary { aaa-custom1 | aaa-custom10 | aaa-custom11 | aaa-custom12 | aaa-custom13 | aaa-custom14 | aaa-custom15 | aaa-custom16 | aaa-custom17 | aaa-custom18 | aaa-custom19 | aaa-custom2 | aaa-custom20 | aaa-custom3 | aaa-custom4 | aaa-custom5 | aaa-custom6 | aaa-custom7 | aaa-custom8 | aaa-custom9 | dynamic-load | nasreq } | endpoint endpoint_name | max-retries max_retries | max-transmissions max_transmissions | redirect-host-avp { just-primary | primary-then-secondary } | request-timeout request_timeout_duration | server host_name priority priority | upgrade-dict-avps { 3gpp-rel10 | 3gpp-rel19 } }

default diameter authentication { dictionary | max-retries | max-transmissions | redirect-host-avp | request-timeout | upgrade-dict-avps }

no diameter authentication { endpoint | max-retries | max-transmissions | server host_name | upgrade-dict-avps }

dictionary: Sets the context’s dictionary as the system default.
endpoint: Removes the configured authentication endpoint, and the default server configured in default AAA group will be used.
max-retries: Disables the configured retry attempts for Diameter authentication in the current AAA group.
max-transmissions: Disables the configured maximum transmission attempts for Diameter authentication in the current AAA group.
server host_name: Removes the configured Diameter host host_name from this AAA server group for Diameter authentication.
upgrade-dict-avps: Sets the release version to 3GPP Rel. 8 for upgrading Diameter authentication dictionary in the current AAA group.

default diameter authentication { dictionary | max-retries | max-transmissions | redirect-host-avp | request-timeout | upgrade-dict-avps }

max-retries: Sets the retry attempts for Diameter authentication requests in the current AAA group to default 0 (disable).
max-transmissions: Sets the configured maximum transmission attempts for Diameter authentication in the current AAA group to default 0 (disable).

redirect-host-avp: Sets the redirect choice to default (just-primary).

request-timeout: Sets the timeout duration, in seconds, for Diameter authentication requests in the current AAA group to default 20.

upgrade-dict-avps: Sets the release version to 3GPP Rel. 8 for upgrading Diameter authentication dictionary in the current AAA group.


Specifies the Diameter authentication dictionary.

aaa-custom1 ... aaa-custom8, aaa-custom10 ... aaa-custom20: Configures the custom dictionaries. Even though the CLI syntax supports several custom dictionaries, not necessarily all of them have been defined. If a custom dictionary that has not been implemented is selected, the default dictionary will be used.

Important: aaa-custom11 dictionary is only available in StarOS 8.1 and later releases. aaa-custom12 to aaa-custom20 dictionaries are only available in StarOS 9.0 and later releases.

aaa-custom9: Configures the STa standard dictionary.

dynamic-load: Configures the dynamically loaded Diameter dictionary. The dictionary name must be an alphanumeric string of 1 through 15 characters. For more information on dynamic loading of Diameter dictionaries, see the diameter dynamic-dictionary in the Global Configuration Mode Commands chapter of this guide.

nasreq: nasreq dictionary—the dictionary as defined by RFC 3588.

endpoint endpoint_name

Enables Diameter to be used for authentication, and specifies which Diameter endpoint to use.

endpoint_name must be an alphanumeric string of 1 through 63 characters.

max-retries max_retries

Specifies how many times a Diameter authentication request should be retried with the same server, if the server fails to respond to a request.

max_retries specifies the maximum number of retry attempts, and must be an integer from 1 through 1000.

Default: 0

max-transmissions max_transmissions

Specifies the maximum number of transmission attempts for a Diameter authentication request. Use this in conjunction with the "max-retries max_retries" option to control how many servers will be attempted to communicate with.

max_transmissions specifies the maximum number of transmission attempts, and must be an integer from 1 through 1000.

Default: 0
redirect-host-avp { just-primary | primary-then-secondary }
Specifies whether to use just one returned AVP, or use the first returned AVP as selecting the primary host and the second returned AVP as selecting the secondary host.
just-primary: Redirect only to primary host.
primary-then-secondary: Redirect to primary host, if fails then redirect to the secondary host.
Default: just-primary

request-timeout request_timeout_duration
Specifies how long the system will wait for a response from a Diameter server before re-transmitting the request.
request_timeout_duration specifies the number of seconds the system will wait for a response from a Diameter server before re-transmitting the request, and must be an integer from 1 through 3600.
Default: 20 seconds

server host_name priority priority
Specifies the current context Diameter authentication server’s host name and priority.
host_name specifies the Diameter authentication server’s host name, and must be an alphanumeric string of 1 through 63 characters.
priority specifies the relative priority of this Diameter host. The priority is used in server selection. The priority must be an integer from 1 through 1000.

upgrade-dict-avps { 3gpp-rel10 | 3gpp-rel9 }
Specifies to upgrade Diameter authentication dictionary to 3GPP Rel. 9 version or 3GPP Rel. 10 version.
3gpp-rel10: Upgrades the dictionary to 3GPP Rel. 10 version.
3gpp-rel9: Upgrades the dictionary to 3GPP Rel. 9 version.
Default: Sets the release version to 3GPP Rel. 8

Usage
Use this command to manage the Diameter authentication options according to the Diameter server used for the context.

Example
The following command configures the Diameter authentication dictionary, aaa-custom1:

diameter authentication dictionary aaa-custom1

The following command configures the Diameter endpoint, EAPI:

diameter authentication endpoint EAPI

The following commands configure Diameter authentication options:

diameter authentication max-retries 4
diameter authentication max-transmissions 2
diameter authentication redirect-host-avp primary-then-secondary
diameter authentication server svc priority 1
diameter authentication request-timeout 10
diameter authentication failure-handling

This command configures the failure handling for Diameter authentication requests and Diameter Extensible Authentication Protocol (EAP) requests.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > AAA Server Group Configuration

configure > context context_name > aaa group group_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-aaa-group)#

Syntax

```
diameter authentication failure-handling { authorization-request | eap-request | eap-termination-request } { request-timeout action { continue | retry-and-terminate | terminate } | result-code start_result_code { [ to end_result_code ] action { continue | retry-and-terminate | terminate } } }

no diameter authentication failure-handling { authorization-request | eap-request | eap-termination-request } result-code start_result_code { [ to end_result_code ] }

default diameter authentication failure-handling { authorization-request | eap-request | eap-termination-request } request-timeout action
```

no
Disables Diameter authentication failure handling.

default
Configures the default Diameter authentication failure handling setting.

authorization-request
Specifies that failure handling must be performed on Diameter authorization request (AAR/AAA) messages.

eap-request
Specifies configuring failure handling for EAP requests.

eap-termination-request
Specifies configuring failure handling for EAP termination requests.

request-timeout action { continue | retry-and-terminate | terminate }
Specifies the action to be taken for failures:

*continue: Continues session
• **retry-and-terminate**: First retries, if it fails then terminates the session
• **terminate**: Terminates session

```bash
result-code start_result_code [ to end_result_code ] action { continue | retry-and-terminate | terminate }
```

- **start_result_code**: Specifies the result code number, must be an integer from 1 through 65535.
- **to end_result_code**: Specifies the upper limit of a range of result codes. **to end_result_code** must be greater than **start_result_code**.
- **action { continue | retry-and-terminate | terminate }**: Specifies the action to be taken for failures:
  - **continue**: Continues
  - **retry-and-terminate**: First retries, if it fails then terminates
  - **terminate**: Terminates

**Usage**

Use this command to configure error handling for Diameter EAP, EAP-termination, and authorization requests. Specific actions (continue, retry-and-terminate, or terminate) can be associated with each possible result-code. Ranges of result codes can be defined with the same action, or actions can be specific on a per-result code basis.

**Example**

The following commands configure result codes 5001, 5002, 5004, and 5005 to use “action continue” and result code 5003 to use “action terminate”:

```bash
diameter authentication failure-handling eap-request result-code 5001 to 5005 action continue
diameter authentication failure-handling eap-request result-code 5003 action terminate
```
**diameter dictionary**

This command is deprecated and is replaced by the `diameter accounting dictionary` and `diameter authentication dictionary` commands. See the `diameter accounting` and `diameter authentication` commands respectively.
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**

Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Use this command to return to the parent configuration mode.
radius

This command configures basic RADIUS options.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > AAA Server Group Configuration

```
configure > context context_name > aaa group group_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-aaa-group)#
```

**Syntax**

```
radius { deadtime minutes | detect-dead-server { consecutive-failures consecutive_failures_count | response-timeout response_timeout_duration } | dictionary dictionary | max-outstanding max_messages | max-retries max_retries | max-transmissions max_transmissions | probe-message local-service-address ipv4/ipv6_address | strip-domain { authentication-only | accounting-only } | timeout idle_seconds }

default radius { deadtime | detect-dead-server | dictionary | max-outstanding | max-retries | max-transmissions | timeout }

no radius { detect-dead-server | max-transmissions | radius probe-message local-service-address | strip-domain }
```

---

**no**

Removes the specified configuration.

---

**default**

Configures default setting for the specified keyword.

---

**dictionary dictionary**

Specifies which dictionary to use. The following table describes the possible values for `dictionary`:

<table>
<thead>
<tr>
<th>Dictionary</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>customXX</td>
<td>These are dictionaries that can be customized to fit your needs. Customization information can be attained by contacting your local service representative. XX is the integer value of the custom dictionary.</td>
</tr>
<tr>
<td>standard</td>
<td>This dictionary consists only of the attributes specified in RFC 2865, RFC 2866, and RFC 2869.</td>
</tr>
<tr>
<td>3gpp</td>
<td>This dictionary consists not only of all of the attributes in the standard dictionary, but also all of the attributes specified in 3GPP 32.015.</td>
</tr>
</tbody>
</table>
## Dictionary Description

<table>
<thead>
<tr>
<th>Dictionary</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3gpp2</td>
<td>This dictionary consists not only of all of the attributes in the standard dictionary, but also all of the attributes specified in IS-835-A.</td>
</tr>
<tr>
<td>3gpp2-835</td>
<td>This dictionary consists not only of all of the attributes in the standard dictionary, but also all of the attributes specified in IS-835.</td>
</tr>
<tr>
<td>starent-vsa1</td>
<td>This dictionary consists not only of the 3GPP2 dictionary, but also includes Starent Networks vendor-specific attributes (VSAs) as well. The VSAs in this dictionary support a one-byte wide VSA Type field in order to support certain RADIUS applications. The one-byte limit allows support for only 256 VSAs (0 - 255). This is the default dictionary.</td>
</tr>
<tr>
<td>starent-vsa1-835</td>
<td>This dictionary consists not only of the 3gpp2-835 dictionary, but also includes Starent Networks vendor-specific attributes (VSAs) as well. The VSAs in this dictionary support a one-byte wide VSA Type field in order to support certain RADIUS applications. The one-byte limit allows support for only 256 VSAs (0 - 255). This is the default dictionary.</td>
</tr>
<tr>
<td>starent</td>
<td>This dictionary consists of all of the attributes in the starent-vsa1 dictionary and incorporates additional Starent Networks VSAs by using a two-byte VSA Type field. This dictionary is the master-set of all of the attributes in all of the dictionaries supported by the system.</td>
</tr>
<tr>
<td>starent-835</td>
<td>This dictionary consists of all of the attributes in the starent-vsa1-835 dictionary and incorporates additional Starent Networks VSAs by using a two-byte VSA Type field. This dictionary is the master-set of all of the attributes in all of the -835 dictionaries supported by the system.</td>
</tr>
</tbody>
</table>

**deadtime minutes**

Specifies the number of minutes to wait before changing the state of a RADIUS server from “Down” to “Active”. minutes must be an integer from 0 through 65535.

Default: 10

**Important:** In 12.0 and later releases, no new attributes can be added to the starent-vsa1 dictionary. If there are any new attributes to be added, these can only be added to the starent dictionary. For more information, please contact your Cisco account representative.

**Important:** For a complete explanation of RADIUS server states, if you are using StarOS 12.3 or an earlier release, refer to the RADIUS Server State Behavior appendix in the AAA and GTPP Interface Administration and Reference. If you are using StarOS 14.0 or a later release, refer to the AAA Interface Administration and Reference.

**detect-dead-server**

This parameter should be set to allow enough time to remedy the issue that originally caused the server’s state to be changed to “Down”. After the deadtime timer expires, the system returns the server’s state to “Active” regardless of whether or not the issue has been fixed.

**Important:** For a complete explanation of RADIUS server states, if you are using StarOS 12.3 or an earlier release, refer to the RADIUS Server State Behavior appendix in the AAA and GTPP Interface Administration and Reference. If you are using StarOS 14.0 or a later release, refer to the AAA Interface Administration and Reference.

**detect-dead-server**

```plaintext
deadtime minutes

Specifies the number of minutes to wait before changing the state of a RADIUS server from “Down” to “Active”. minutes must be an integer from 0 through 65535.

Default: 10

**Important:** In 12.0 and later releases, no new attributes can be added to the starent-vsa1 dictionary. If there are any new attributes to be added, these can only be added to the starent dictionary. For more information, please contact your Cisco account representative.

**Important:** For a complete explanation of RADIUS server states, if you are using StarOS 12.3 or an earlier release, refer to the RADIUS Server State Behavior appendix in the AAA and GTPP Interface Administration and Reference. If you are using StarOS 14.0 or a later release, refer to the AAA Interface Administration and Reference.

**detect-dead-server**

```
```plaintext
detect-dead-server { consecutive-failures consecutive_failures_count | keepalive | response-timeout response_timeout_duration } ```

**Important:** For a complete explanation of RADIUS server states, if you are using StarOS 12.3 or an earlier release, refer to the RADIUS Server State Behavior appendix in the AAA and GTPP Interface Administration and Reference. If you are using StarOS 14.0 or a later release, refer to the AAA Interface Administration and Reference.

**detect-dead-server**

```plaintext
detect-dead-server { consecutive-failures consecutive_failures_count | keepalive | response-timeout response_timeout_duration } ```

**Important:** For a complete explanation of RADIUS server states, if you are using StarOS 12.3 or an earlier release, refer to the RADIUS Server State Behavior appendix in the AAA and GTPP Interface Administration and Reference. If you are using StarOS 14.0 or a later release, refer to the AAA Interface Administration and Reference.

**detect-dead-server**

```plaintext
detect-dead-server { consecutive-failures consecutive_failures_count | keepalive | response-timeout response_timeout_duration } ```

**Important:** For a complete explanation of RADIUS server states, if you are using StarOS 12.3 or an earlier release, refer to the RADIUS Server State Behavior appendix in the AAA and GTPP Interface Administration and Reference. If you are using StarOS 14.0 or a later release, refer to the AAA Interface Administration and Reference.

**detect-dead-server**

```plaintext
detect-dead-server { consecutive-failures consecutive_failures_count | keepalive | response-timeout response_timeout_duration } ```

**Important:** For a complete explanation of RADIUS server states, if you are using StarOS 12.3 or an earlier release, refer to the RADIUS Server State Behavior appendix in the AAA and GTPP Interface Administration and Reference. If you are using StarOS 14.0 or a later release, refer to the AAA Interface Administration and Reference.

**detect-dead-server**

```plaintext
detect-dead-server { consecutive-failures consecutive_failures_count | keepalive | response-timeout response_timeout_duration } ```

**Important:** For a complete explanation of RADIUS server states, if you are using StarOS 12.3 or an earlier release, refer to the RADIUS Server State Behavior appendix in the AAA and GTPP Interface Administration and Reference. If you are using StarOS 14.0 or a later release, refer to the AAA Interface Administration and Reference.
**keepalive**: Enables the AAA server alive-dead detect mechanism based on sending keepalive authentication messages to all authentication servers. Default is disabled.

**response-timeout** *response_timeout_duration*: Specifies the number of seconds, for any AAA Manager, to wait for a response to any message before a server’s state is changed from “Active” to “Down”. *response_timeout_duration* must be an integer from 1 through 65535.

**Important**: If both consecutive-failures and response-timeout are configured, then both parameters must be met before a server’s state is changed to “Down”.

**Important**: The “Active” or “Down” state of a RADIUS server as defined by the system, is based on accessibility and connectivity. For example, if the server is functional but the system has placed it into a “Down” state, it could be the result of a connectivity problem. When a RADIUS server’s state is changed to “Down”, a trap is sent to the management station and the deadtime timer is started.

**max-outstanding** *max_messages*

Specifies the maximum number of outstanding messages a single AAA Manager instance will queue. *max_messages* must be an integer from 1 through 4000.

Default: 256

**max-retries** *max_retries*

Specifies the maximum number of times communication with a AAA server will be attempted before it is marked as “Not Responding”, and the detect dead server’s consecutive failures count is incremented. *max_retries* must be an integer from 0 through 65535.

Default: 5

**max-transmissions** *max_transmissions*

Sets the maximum number of re-transmissions for RADIUS authentication requests. This limit is used in conjunction with max-retries parameter for each server. When failing to communicate with a RADIUS server, the subscriber is failed once all of the configured RADIUS servers have been exhausted, or once the configured number of maximum transmissions is reached. For example, if three servers are configured and if the configured max-retries is 3 and max-transmissions is 12, then the primary server is tried four times (once plus three retries), the secondary server is tried four times, and then a third server is tried four times. If there is a fourth server, it is not tried because the maximum number of transmissions (12) has been reached.

*max_transmissions* must be an integer from 1 through 65535.

Default: Disabled

**probe-message** local-service-address *ipv4/ipv6_address*

**radius** probe-message: Configures AVPs to be sent in RADIUS authentication probe messages. 
**local-service-address**: Configures the service ip-address to be sent as an AVP in RADIUS authentication probe messages. 
*ipv4/ipv6_address*: Specifies the IP address of the server. 
*ip_address* must be specified in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation. A maximum of 128 RADIUS servers can be configured per context. This limit includes accounting and authentication servers.
**radius**

**strip-domain { authentication-only | accounting-only }**

Specifies that the domain must be stripped from the user name prior to authentication or accounting. By default, strip-domain configuration will be applied to both authentication and accounting messages, if configured. When the argument `authentication-only` or `accounting-only` is present, `strip-domain` is applied only to the specified RADIUS message types.

**timeout idle_seconds**

Specifies the number of seconds to wait for a response from the RADIUS server before re-sending the messages. `idle_seconds` must be an integer from 1 through 65535. Default: 3

**Usage**

Use this command to configure the basic RADIUS parameters according to the RADIUS server used for the context.

**Example**

The following command configures the RADIUS timeout parameter to 300 seconds.

```
radius timeout 300
```
radius accounting

This command configures the current context’s RADIUS accounting parameters.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > AAA Server Group Configuration
configure > context context_name > aaa group group_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-aaa-group)#

Syntax

radius accounting { archive [ stop-only ] | deadtime minutes | detect-dead-server { consecutive-failures consecutive_failures_count | keepalive | response-timeout response_timeout_duration } | fire-and-forget | interim interval interim_interval | max-outstanding max_messages | max-pdu-size octets | max-retries max_retries | max-transmissions max_transmissions | timeout idle_seconds }

default radius accounting { deadtime | detect-dead-server | fire-and-forget | interim interval | max-transmissions } | max-outstanding | max-pdu-size | max-retries | max-transmissions | timeout }

no radius accounting { archive | detect-dead-server | fire-and-forget | interim interval | max-transmissions }

---

no
Removes the specified configuration.

default
Configures the default setting for the specified keyword.

archive [ stop-only ]
Enables archiving of RADIUS accounting messages in the system after the accounting message has exhausted retries to all available RADIUS accounting servers. All RADIUS accounting messages generated by a session are serially delivered to the RADIUS accounting server. That is, previous RADIUS accounting messages from the same call must be delivered and acknowledged by the RADIUS accounting server before the next RADIUS accounting message is sent to the RADIUS accounting server. stop-only specifies archiving of only STOP accounting messages. Default: enabled

deadtime minutes
Specifies the number of minutes to wait before changing the state of a RADIUS server from “Down” to “Active”. minutes must be an integer from 0 through 65535.
Default: 10 minutes

**Important:** This parameter should be set to allow enough time to remedy the issue that originally caused the server’s state to be changed to “Down”. After the deadtime timer expires, the system returns the server’s state to “Active” regardless of whether or not the issue has been fixed.

**Important:** For a complete explanation of RADIUS server states, if you are using StarOS 12.3 or an earlier release, refer to the *RADIUS Server State Behavior* appendix in the *AAA and GTPP Interface Administration and Reference*. If you are using StarOS 14.0 or a later release, refer to the *AAA Interface Administration and Reference*.

```
detect-dead-server { consecutive-failures consecutive_failures_count | keepalive | response-timeout response_timeout_duration }
```

- **consecutive-failures** *consecutive_failures_count*: Specifies the number of consecutive failures, for any AAA Manager, before a server’s state is changed from “Active” to “Down”.
  - *consecutive_failures_count* must be an integer from 1 through 1000. Default: 4
- **keepalive**: Enables the AAA server alive-dead detect mechanism based on sending keepalive authentication messages to all authentication servers. Default: disabled
- **response-timeout** *response_timeout_duration*: Specifies the number of seconds, for any AAA Manager, to wait for a response to any message before a server’s state is changed from “Active” to “Down”.
  - *response_timeout_duration* must be an integer from 1 through 65535.

**Important:** If both **consecutive-failures** and **response-timeout** are configured, then both parameters must be met before a server’s state is changed to “Down”.

**Important:** The “Active” or “Down” state of a RADIUS server as defined by the system, is based on accessibility and connectivity. For example, if the server is functional but the system has placed it into a “Down” state, it could be the result of a connectivity problem. When a RADIUS server’s state is changed to “Down”, a trap is sent to the management station and the deadtime timer is started.

**Important:** For a complete explanation of RADIUS server states, if you are using StarOS 12.3 or an earlier release, refer to the *RADIUS Server State Behavior* appendix in the *AAA and GTPP Interface Administration and Reference*. If you are using StarOS 14.0 or a later release, refer to the *AAA Interface Administration and Reference*.

```
fire-and-forget
```

Enables RADIUS Fire-and-Forget accounting for the AAA group.

- Default: Disabled
- The request sent to the RADIUS accounting server configured under the AAA group with this keyword configured will not expect a response from the server. If the request must be sent to more than one such type of server, the acct-algorithm first-n configuration in the AAA group can be used.

**Important:** The Fire-and-Forget feature is supported on GGSN, HA, PDSN and P-GW.

Keepalive feature for server state detection is supported in conjunction since there is no waiting for responses. Archiving in such a AAA group is not supported. If the server is down, the request is sent to the next server in the group. If all the servers in the group are down, the request is deleted.
This CLI is independent of the APN or subscriber profile configuration `aaa secondary-group aaa_group_name`.

```
interim interval interim_interval
```

Specifies the time interval, in seconds, for sending accounting INTERIM-UPDATE records.
`interim_interval` must be an integer from 50 through 4000000.
Default: Disabled

**Important:** If RADIUS is used as the accounting protocol for the GGSN product, other commands are used to trigger periodic accounting updates. However, these commands would cause RADIUS STOP/START packets to be sent as opposed to INTERIM-UPDATE packets. Also, note that accounting interim interval settings received from a RADIUS server take precedence over those configured on the system.

```
max-outstanding max_messages
```

Specifies the maximum number of outstanding messages a single AAA Manager instance will queue.
`max_messages` must be an integer from 1 through 4000.
Default: 256

```
max-pdu-size octets
```

Specifies the maximum sized packet data unit which can be accepted/generated, in bytes (octets).
`octets` must be an integer from 512 through 2048.
Default: 2048

```
max-retries max_retries
```

Specifies the maximum number of times communication with a AAA server will be attempted before it is marked as “Not Responding” and the detect dead server consecutive failures count is incremented.
`max_retries` must be an integer from 0 through 65535.
Default: 5

Once the maximum number of retries is reached this is considered a single failure for the consecutive failures count for detecting dead servers.

```
max-transmissions max_transmissions
```

Sets the maximum number of transmissions for a RADIUS accounting message before the message is declared as failed.
`max_transmissions` must be an integer from 1 through 65535.
Default: Disabled

```
timeout timeout_duration
```

Specifies the duration to wait for a response from a RADIUS server before retransmitting a request.
`timeout_duration` must be an integer from 1 through 65535.
Default: 3

### Usage

Use this command to configure RADIUS accounting options according to the RADIUS server used for the context.

### Example

The following command configures the accounting timeout parameter to 16 seconds.

```
The following command configures the accounting timeout parameter to 16 seconds.
```
radius accounting timeout 16
radius accounting apn-to-be-included

This command specifies the APN name inclusion for RADIUS accounting.

Product

GGSN

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > Context Configuration > AAA Server Group Configuration
configure > context context_name > aaa group group_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-aaa-group)#

Syntax

radius accounting apn-to-be-included { gi | gn }

default radius accounting apn-to-be-included

<table>
<thead>
<tr>
<th>Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>default</strong></td>
</tr>
<tr>
<td>Configures the default setting.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>gi</strong></td>
</tr>
<tr>
<td>Specifies the use of Gi APN name in RADIUS accounting request. Gi APN represents the APN received in the Create PDP context request message from SGSN.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>gn</strong></td>
</tr>
<tr>
<td>Specifies the use of Gn APN name in RADIUS accounting request. Gn APN represents the APN selected by the GGSN.</td>
</tr>
</tbody>
</table>

Usage

Use this command to specify the APN name to be included for RADIUS accounting.

Example

The following command configures the gn APN name to be included for RADIUS accounting:

    radius accounting apn-to-be-included gn
radius accounting algorithm

This command specifies the fail-over/load-balancing algorithm to select the RADIUS accounting server(s) to which accounting data must be sent.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > AAA Server Group Configuration

configure > context context_name > aaa group group_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-aaa-group)#

Syntax

radius accounting algorithm { first-n n | first-server | round-robin }

default radius accounting algorithm

default
Configures the default setting.
Default: first-server

first-n n
Default: 1 (Disabled)
Specifies that the AGW must send accounting data to n (more than one) AAA accounting servers based on their priority. The full set of accounting data is sent to each of the n AAA servers. Response from any one of the servers would suffice to proceed with the call. On receiving an ACK from any one of the servers, all retries are stopped.
n is the number of AAA servers to which accounting data will be sent, and must be an integer from 2 through 128.

first-server
Specifies that the context must send accounting data to the RADIUS accounting server with the highest configured priority. In the event that this server becomes unreachable, accounting data is sent to the server with the next-highest configured priority. This is the default algorithm.

round-robin
Specifies that the context must load balance sending accounting data among all of the defined RADIUS accounting servers. Accounting data is sent in a circular queue fashion on a per Session Manager task basis, where data is sent to the next available server and restarts at the beginning of the list of configured servers. The order of the list is based upon the configured relative priority of the servers.
In releases to prior to 17, for subscribers with IMSI containing hexadecimal characters the round robin algorithm fails causing the messages to be forwarded to a single RADIUS server all the time. This algorithm works only for decimal based IMSI addresses.
Usage

Use this command to specify the algorithm to select the RADIUS accounting server(s) to which accounting data must be sent.

Example

The following command configures to use the round-robin algorithm for RADIUS accounting server selection:

```
radius accounting algorithm round-robin
```
radius accounting billing-version

This command configures billing-system version of RADIUS accounting servers.

Product  
All

Privilege  
Security Administrator, Administrator

Mode  
Exec > Global Configuration > Context Configuration > AAA Server Group Configuration
configure > context context_name > aaa group group_name

Entering the above command sequence results in the following prompt:

[context_name] host_name(config-aaa-group)#

Syntax

radius accounting billing-version version

default radius accounting billing-version

default

Configures the default setting.
Default: 0

version

Specifies the billing-system version, and must be an integer from 0 through 4294967295.

Usage

Use this command to configure the billing-system version of RADIUS accounting servers.

Example

The following command configures the billing-system version of RADIUS accounting servers as 10:

radius accounting billing-version 10
radius accounting gtp trigger-policy

This command configures the RADIUS accounting trigger policy for GTP messages.

Product
GGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > AAA Server Group Configuration

configure > context context_name > aaa group group_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-aaa-group)#

Syntax

radius accounting gtp trigger-policy [ standard | ggsn-preservation-mode ]

default radius accounting gtp trigger-policy

default
Resets the RADIUS accounting trigger policy to standard behavior for GTP session.

standard
This keyword sets the RADIUS accounting trigger policy to standard behavior which is configured for GTP session for GGSN service.

ggsn-preservation-mode
This keyword sends RADIUS Accounting Start when the GTP message with private extension of preservation mode is received from SGSN.

Important: This is a customer-specific keyword and needs customer-specific license to use this feature. For more information on GGSN preservation mode, refer to the GGSN Service Configuration Mode Commands chapter.

Usage

Use this command to set the trigger policy for the AAA accounting for a GTP session.

Example

The following command sets the RADIUS accounting trigger policy for GTP session to standard:

default radius accounting gtp trigger-policy
radius accounting ha policy

This command configures the RADIUS accounting policy for Home Agent (HA) sessions.

**Product**
HA

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > AAA Server Group Configuration

```yaml
configure > context context_name > aaa group group_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-aaa-group)#
```

**Syntax**

```yaml
radius accounting ha policy { custom1-aaa-res-mgmt | session-start-stop }
```

```yaml
default radius accounting ha policy
```

**default**

Configures the default setting.

```yaml
session-start-stop
```

Specifies sending Accounting Start when the Session is connected, and sending Accounting Stop when the session is disconnected. This is the default behavior.

```yaml
custom1-aaa-res-mgmt
```

Accounting Start/Stop messages are generated to assist special resource management done by AAA servers. It is similar to the session-start-stop accounting policy, except for the following differences:

- Accounting Start is also generated during MIP session handoffs.
- No Accounting stop is generated when an existing session is overwritten and the new session continues to use the IP address assigned for the old session.
- Accounting Start is generated when a new call overwrites an existing session.

**Usage**

Use this command to configure the AAA accounting behavior for an HA session.

**Example**

The following command configures the HA accounting policy to `custom1-aaa-res-mgmt`:

```
radius accounting ha policy custom1-aaa-res-mgmt
```
radius accounting interim

This command configures the volume of uplink and downlink volume octet counts that trigger RADIUS interim accounting, and configures the time period between the sending of interim accounting records.

**Product**
- GGSN
- PDSN
- HA
- HSGW

**Privilege**
Security Administrator, Administrator

**Mode**
- Exec > Global Configuration > Context Configuration > AAA Server Group Configuration
- configure > context context_name > aaa group group_name

Entering the above command sequence results in the following prompt:
```
[context_name]host_name(config-aaa-group)#
```

**Syntax**
```
radius accounting interim { interval interim_interval | volume { downlink bytes uplink bytes | total bytes | uplink bytes downlink bytes } }
```

```
o radius accounting interim volume
```

- **no**
  Disables RADIUS interim accounting.

- **interval interim_interval**
  Specifies the time interval, in seconds, between sending interim accounting records. The `interim_interval` must be an integer from 50 through 40000000.

- **volume { downlink bytes uplink bytes | total bytes | uplink bytes downlink bytes }**
  - `downlink bytes uplink bytes`: Specifies the downlink to uplink volume limit, in bytes, for RADIUS Interim accounting. The `bytes` must be an integer from 100000 through 4000000000.
  - `total bytes`: Specifies the total volume limit, in bytes, for RADIUS interim accounting. The `bytes` must be an integer from 100000 through 4000000000.
  - `uplink bytes downlink bytes`: Specifies the uplink to downlink volume limit, in bytes, for RADIUS interim accounting. The `bytes` must be an integer from 100000 through 4000000000.

**Usage**
Use this command to trigger RADIUS interim accounting based on the volume of uplink and downlink bytes and/or to configure the time interval between the sending of interim accounting records.

**Example**

---

Cisco ASR 5x00 Command Line Interface Reference  169
The following command triggers RADIUS interim accounting when the total volume of uplink and downlink bytes reaches 110000:

```
radius accounting interim volume total 110000
```

The following command sets the interval between sending interim accounting records to 3 minutes (180 seconds):

```
radius accounting interim interval 180
```
radius accounting ip remote-address

This command configures IP remote address-based RADIUS accounting parameters.

Product
- PDSN
- HA

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > AAA Server Group Configuration
configure > context context_name > aaa group group_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-aaa-group)#

Syntax

[ no ] radius accounting ip remote-address { collection | list list_id }

no
Removes the specified configuration.

collection
Enables collecting and reporting Remote-Address-Based accounting in RADIUS Accounting. This should be enabled in the AAA Context. It is disabled by default.

list list_id
Enters the Remote Address List Configuration mode. This mode configures a list of remote addresses that can be referenced by the subscriber's profile. 
list_id must be an integer from 1 through 65535.

Usage
This command is used as part of the Remote Address-based Accounting feature to both configure remote IP address lists and enable the collection of accounting data for the addresses in those lists on a per-subscriber basis.

Individual subscriber can be associated to remote IP address lists through the configuration/specification of an attribute in their local or RADIUS profile. (Refer to the radius accounting command in the Subscriber Configuration mode.) When configured/specifed, accounting data is collected pertaining to the subscriber’s communication with any of the remote addresses specified in the list.

Once this functionality is configured on the system and in the subscriber profiles, it must be enabled by executing this command with the collection keyword.

Example
The following command enables collecting and reporting Remote-Address-Based accounting in RADIUS Accounting:

radius accounting ip remote-address collection
radius accounting keepalive

This command configures the keepalive authentication parameters for the RADIUS accounting server.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > AAA Server Group Configuration

```
configure > context context_name > aaa group group_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-aaa-group)#
```

**Syntax**

```
radius accounting keepalive { calling-station-id id | consecutive-response consecutive_responses | framed-ip-address ip_address | interval seconds | retries number | timeout seconds | username user_name }

default radius accounting keepalive { calling-station-id | consecutive-response | interval | retries | timeout | username }

no radius accounting keepalive framed-ip-address
```

---

**no**

Removes the specified configuration.

**default**

Configures the default setting for the specified keyword.

**calling-station-id id**

Configures the Calling-Station-Id to be used for the keepalive authentication.

`id` must be an alphanumeric string of size 1 to 15 characters.

Default: 000000000000000

**consecutive-response consecutive_responses**

Configures the number of consecutive authentication response after which the server is marked as reachable.

`consecutive_responses` must be an integer from 1 through 10.

Default: 1

**framed-ip-address ip_address**

Configures the framed-ip-address to be used for the keepalive accounting.

`ip_address` must be specified using IPv4 dotted-decimal notation.
AAA Server Group Configuration Mode Commands

```
radius accounting keepalive
```

### interval seconds
Configures the time interval between the two keepalive access requests.
Default: 30 seconds

### retries number
Configures the number of times the keepalive access request to be sent before marking the server as unreachable.
`number` must be an integer from 3 through 10.
Default: 3

### timeout timeout_duration
Configures the time interval between each keepalive access request retries.
`timeout_duration` must be an integer from 1 through 30.
Default: 3 seconds

### username user_name
Configures the user name to be used for authentication.
`user_name` must be an alphanumeric string of 1 through 127 characters.
Default: Test-Username

---

**Usage**

Use this command to configure the keepalive authentication parameters for the RADIUS accounting server.

**Example**

The following command sets the user name for RADIUS keepalive access requests to `Test-Username2`:

```
radius accounting keepalive username Test-Username2
```

The following command sets the number of RADIUS accounting keepalive retries to 4.

```
radius accounting keepalive retries 4
```
radius accounting pdif trigger-policy

This command configures the policy for generating START/STOP pairs in overflow condition.

**Product**
PDIF

**Privilege**
Administrator, Security Administrator

**Mode**
Exec > Global Configuration > Context Configuration > AAA Server Group Configuration

```
configure > context context_name > aaa group group_name
```

Entering the above command sequence results in the following prompt:

```
[context_name] host_name(config-aaa-group) #
```

**Syntax**

```
radius accounting pdif trigger-policy { standard | counter-rollover }
```

**default radius accounting pdif trigger-policy**

```
default
```

The default option configures the “standard” policy.

```
standard
```

Applies a policy as defined by the standards.

```
counter-rollover
```

If the counter-rollover option is enabled, the system generates a STOP/START pair before input/output data octet counts (or input/output data packet counts) become larger than \((2^{32} - 1)\) in value. This setting is used to guarantee that a 32-bit octet count in any STOP message has not wrapped to larger than \(2^{32}\) thus ensuring the accuracy of the count. The system may, at its discretion, send the STOP/START pair at any time, so long as it does so before the 32-bit counter has wrapped.

**Usage**

Used to define the policy for dealing with overflow packet counts.

**Example**

Use the following example to set the default policy to *standard*.

```
default radius accounting pdif trigger-policy
```

default radius accounting pdif trigger-policy
radius accounting rp

This command configures the RADIUS accounting R-P originated call options.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > AAA Server Group Configuration

configure > context context_name > aaa group group_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-aaa-group)#
```

**Syntax**

```
radius accounting rp { handoff-stop { immediate | wait-active-stop } | tod minute hour | trigger-event { active-handoff | active-start-param-change | active-stop } | trigger-policy { airlink-usage { counter-rollover } | custom { active-handoff | active-start-param-change | active-stop } | standard } | trigger-stop-start }

no radius accounting rp { tod minute hour | trigger-event { active-handoff | active-start-param-change | active-stop } | trigger-stop-start }

default radius accounting rp { handoff-stop { immediate | wait-active-stop } | trigger-policy }
```

**no**
Removes the specified configuration.

**default**
Sets the default configuration for the specified keyword.

**handoff-stop { immediate | wait-active-stop }**
Specifies the behavior of generating accounting STOP when handoff occurs.
- **immediate**: Indicates that accounting STOP should be generated immediately on handoff, i.e. not to wait active-stop from the old PCF.
- **wait-active-stop**: Indicates that accounting STOP is generated only when active-stop received from the old PCF when handoff occurs.

Default: **wait-active-stop**

**tod minute hour**
Specifies the time of day a RADIUS event is to be generated for accounting. Up to four different times of the day may be specified through individual commands.

- **minute** must be an integer from 0 through 59.
- **hour** must be an integer from 0 through 23.
AAA Server Group Configuration Mode Commands

```
trigger-event { active-handoff | active-start-param-change | active-stop }
```

**active-start-param-change**: Enabled
**active-stop**: Disabled

Configures the events for which a RADIUS event is generated for accounting as one of the following:

- **active-handoff**: Enables a single R-P event (and therefore a RADIUS accounting event) when an Active PCF-to-PFC Handoff occurs. Normally two R-P events will occur (one for the Connection Setup, and the second for the Active-Start)
- **active-start-param-change**: Enables an R-P event (and therefore a RADIUS accounting event) when an Active-Start is received from the PCF and there has been a parameter change.
- **active-stop**: Enables an R-P event (and therefore a RADIUS accounting event) when an Active-Stop is received from the PCF.

Default: **active-handoff**: Disabled

**Important**: This keyword has been obsoleted by the **trigger-policy** keyword. Note that if this command is used, if the context configuration is displayed, radius accounting rp configuration is represented in terms of the trigger-policy.

```
trigger-policy { airlink-usage [ counter-rollover ] | custom [ active-handoff | active-start-param-change | active-stop ] | standard }
```

Default: **airlink-usage**: Disabled

**custom**:
- **active-handoff** = Disabled
- **active-start-param-change** = Disabled
- **active-stop** = Disabled

**standard**: Enabled

Configures the overall accounting policy for R-P sessions as one of the following:

- **airlink-usage [ counter-rollover ]**: Specifies the use of Airlink-Usage RADIUS accounting policy for R-P, which generates a start on Active-Starts, and a stop on Active-Stops.
- **counter-rollover**: If the **counter-rollover** option is enabled, the system generates a STOP/START pair before input/output data octet counts (or input/output data packet counts) become larger than $2^{32} - 1$ in value. This setting is used to guarantee that a 32-bit octet count in any STOP message has not wrapped to larger than $2^{32}$ thus ensuring the accuracy of the count. The system, may, at its discretion, send the STOP/START pair at any time, so long as it does so before the 32-bit counter has wrapped. Note that a STOP/START pair is never generated unless the subscriber RP session is in the Active state, since octet/packet counts are not accumulated when in the Dormant state.

- **custom**: Specifies the use of custom RADIUS accounting policy for R-P. The custom policy can consist of the following:
  - **active-handoff**: Enables a single R-P event (and therefore a RADIUS accounting event) when an Active PCF-to-PFC Handoff occurs. Normally two R-P events will occur (one for the Connection Setup, and the second for the Active-Start)
  - **active-start-param-change**: Enables an R-P event (and therefore a RADIUS accounting event) when an Active-Start is received from the PCF and there has been a parameter change.

**Important**: Note that a custom trigger policy with only **active-start-param-change** enabled is identical to the **standard** trigger-policy.
**active-stop**: Enables an R-P event (and therefore a RADIUS accounting event) when an Active-Stop is received from the PCF.

**Important**: If the `radius accounting rp trigger-policy custom` command is executed without any of the optional keywords, all custom options are disabled.

**standard**: Specifies the use of Standard RADIUS accounting policy for R-P in accordance with IS-835B.

**trigger-stop-start**

Specifies that a stop/start RADIUS accounting pair should be sent to the RADIUS server when an applicable R-P event occurs.

**Usage**

Use this command to configure the events for which a RADIUS event is sent to the server when the accounting procedures vary between servers.

**Example**

The following command enables an R-P event (and therefore a RADIUS accounting event) when an Active-Stop is received from the PCF:

```
radius accounting rp trigger-event active-stop
```

The following command generates the STOP only when active-stop received from the old PCF when handoff occurs:

```
default radius accounting rp handoff-stop
```
radius accounting server

For accounting, this command configures the RADIUS accounting server(s) in the current context.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > AAA Server Group Configuration
configure > context context_name > aaa group group_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-aaa-group)#

Syntax

radius [ mediation-device ] accounting server ip_address [ encrypted ] key value [ acct-on { disable | enable } ] [ acct-off { disable | enable } ] [ admin-status { disable | enable } ] [ max max_messages ] [ max-rate max_value ] [ oldports ] [ port port_number ] [ priority priority ] [ type { mediation-device | standard } ] [ -noconfirm ]

no radius [ mediation-device ] accounting server ip_address [ oldports | port port_number ]

no
Removes the server or server port(s) specified from the list of configured servers.

mediation-device

Enables mediation-device specific AAA transactions used to communicate with this RADIUS server.

Important: If this option is not used, by default the system enables standard AAA transactions.

ip_address [ port port_number ]

Specifies the IP address of the accounting server. ip_address must be specified using IPv4 dotted-decimal notation. A maximum of 1600 RADIUS servers per context/system and 128 servers per server group can be configured. This limit includes accounting and authentication servers.

port port_number specifies the port number to use for communications. port_number must be an integer from 0 through 65535. Default is 1813.

Important: The same RADIUS server IP address and port can be configured in multiple RADIUS server groups within a context.

[ encrypted ] key value

Specifies the shared secret key used to authenticate the client to the servers. The encrypted keyword indicates the key specified is encrypted.
In 12.1 and earlier releases, the key value must be an alphanumeric string of 1 through 127 characters without encryption, and 1 through 256 characters with encryption.

In StarOS 12.2 and later releases, the key value must be an alphanumeric string of 1 through 127 characters without encryption, and 1 through 236 characters with encryption enabled.

The encrypted keyword is intended only for use by the chassis while saving configuration scripts. The system displays the encrypted keyword in the configuration file as a flag that the variable following the key keyword is the encrypted version of the plain text key. Only the encrypted key is saved as part of the configuration file.

```
acct-on { disable | enable }
```

This keyword enables/disables sending of the Accounting-On message when a new RADIUS server is added to the configuration. By default, this keyword will be disabled.

When enabled, the Accounting-On message is sent when a new RADIUS server is added in the configuration. However, if for some reason the Accounting-On message cannot be sent at the time of server configuration (for example, if the interface is down), then the message is sent as soon as possible. Once the Accounting-On message is sent, if it is not responded to after the configured RADIUS accounting timeout, the message is retried the configured number of RADIUS accounting retries. Once all retries have been exhausted, the system no longer attempts to send the Accounting-On message for this server.

```
acct-off { disable | enable }
```

Disables and enables the sending of the Accounting-Off message when a RADIUS server is removed from the configuration.

The Accounting-Off message is sent when a RADIUS server is removed from the configuration, or when there is an orderly shutdown. However, if for some reason the Accounting-On message cannot be sent at this time, it is never sent. The Accounting-Off message is sent only once, regardless of how many accounting retries are enabled.

Default: enable

```
max max_messages
```

Specifies the maximum number of outstanding messages that may be allowed to the server.

`max_messages` must be an integer from 0 through 4000.

Default: 0

```
max-rate max_value
```

Specifies the rate at which the accounting messages should be sent to the RADIUS server by a single AAA manager task.

`max_value` must be an integer from 0 through 1000.

Default: 0 (disabled)

```
oldports
```

Sets the UDP communication port to the out of date standardized default for RADIUS communications to 1646.

```
priority priority
```

Specifies the relative priority of this accounting server. The priority is used in server selection for determining which server to send accounting data to.

`priority` must be an integer from 1 through 1000, where 1 is the highest priority. When configuring two or more servers with the same priority you will be asked to confirm that you want to do this. If you use the –
**Noconfirm** option, you are not asked for confirmation and multiple servers could be assigned the same priority.
Default: 1000

**Type** { mediation-device | standard }

**Mediation-device**: Obsolete keyword.
Specifies the type of AAA transactions to use to communicate with this RADIUS server.
**Standard**: Use standard AAA transactions.
Default: **standard**

**Admin-status** { disable | enable }
Configures the admin-status for the RADIUS accounting server.
**Enable**: Enables the RADIUS accounting server.
**Disable**: Disables the RADIUS accounting server.

**Usage**
Use this command to configure the RADIUS accounting servers with which the system must communicate for accounting.
You can configure up to 1600 RADIUS servers per context/system and 128 servers per server group. The servers can be configured as Accounting, Authentication, Charging servers, or any combination thereof.

**Example**
The following command sets the accounting server with mediation device transaction for AAA server 10.2.3.4:

```
radius mediation-device accounting server 10.2.3.4 key sharedKey port 1024 max 127
```
radius algorithm

This command configures the RADIUS authentication server selection algorithm for the current context.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > AAA Server Group Configuration

```
configure > context context_name > aaa group group_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-aaa-group)#
```

**Syntax**

```
radius algorithm { first-server | round-robin }
```

**default radius algorithm**

```
default
```

- Configures the default setting.
- Default: **first-server**

```
first-server
```

- Authentication data is sent to the first available authentication server based upon the relative priority of each configured server.

```
round-robin
```

- Authentication data is sent in a circular queue fashion on a per Session Manager task basis where data is sent to the next available authentication server and restarts at the beginning of the list of configured servers. The order of the list is based upon the configured relative priority of the servers.

**Usage**

Use this command to configure the context’s RADIUS authentication server selection algorithm to ensure proper load distribution amongst the available authentication servers.

**Example**

The following command configures to use the round-robin algorithm for RADIUS authentication server selection:

```
radius algorithm round-robin
```
radius allow

This command configures the system behavior for allowing subscriber sessions when RADIUS accounting and/or authentication is unavailable.

Product
All products used in CDMA deployments

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > AAA Server Group Configuration

configure > context context_name > aaa group group_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-aaa-group)#

Syntax

[ no ] radius allow { authentication-down | accounting-down }

- no
  Specifies that the specified option is to be disabled.

- authentication-down
  Allows sessions while authentication is not available (down).
  Default: Disabled

- accounting-down
  Allows sessions while accounting is unavailable (down).
  Default: Enabled

Usage

Allow sessions during system troubles when the risk of IP address and/or subscriber spoofing is minimal. The denial of sessions may cause dissatisfaction with subscribers at the cost/expense of verification and/or accounting data.

Important: Please note that this command is applicable ONLY to CDMA products. To configure this functionality in UMTS/LTE products (GGSN/P-GW/SAEGW), use the command mediation-device delay-GTP-response in APN Configuration mode.

Example

The following command configures the RADIUS server to allow the sessions while accounting is unavailable.

radius allow accounting-down
radius attribute

This command configures the system’s RADIUS identification parameters.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > AAA Server Group Configuration

`configure > context context_name > aaa group group_name`

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-aaa-group)#`

Syntax

```plaintext
radius attribute { accounting accounting_attribute | authentication authentication_attribute | nas-identifier nas_id | nas-ip-address address primary_address [ backup secondary_address ] [ nexthop-forwarding-address nexthop_address ] [ mpls-label input in_label_value | output out_label_value1 [ out_label_value2 ] [ vlan vlan_id ] ] }

no radius attribute { accounting accounting_attribute | authentication authentication_attribute | nas-identifier | nas-ip-address }

default radius attribute { accounting | authentication | nas-identifier }
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Removes or disables the specified configuration.</td>
</tr>
<tr>
<td><code>default</code></td>
<td>Configures the default setting(s).</td>
</tr>
<tr>
<td><code>accounting accounting_attribute</code></td>
<td>Enables RADIUS accounting attributes for the following options, provided they are supported in the configured RADIUS dictionary:</td>
</tr>
<tr>
<td></td>
<td><em>3gpp-cg-address</em></td>
</tr>
<tr>
<td></td>
<td><em>3gpp-charging-characteristics</em></td>
</tr>
<tr>
<td></td>
<td><em>3gpp-charging-id</em></td>
</tr>
<tr>
<td></td>
<td><em>3gpp-ggsn-address</em></td>
</tr>
<tr>
<td></td>
<td><em>3gpp-ggsn-mcc-mnc</em></td>
</tr>
<tr>
<td></td>
<td><em>3gpp-gprs-qos-negotiated-profile</em></td>
</tr>
<tr>
<td></td>
<td><em>3gpp-imeisv</em></td>
</tr>
<tr>
<td></td>
<td><em>3gpp-imsi-mcc-mnc</em></td>
</tr>
</tbody>
</table>
• 3gpp-ms-timezone
• 3gpp-nsapi
• 3gpp-pdp-type
• 3gpp-rat-type
• 3gpp-select-mode
• 3gpp-session-stopindicator
• 3gpp-sgsn-address
• 3gpp-sgsn-mcc-mnc
• 3gpp-user-location-info
• acct-authentic
• acct-delay-time
• acct-input-octets
• acct-input-packets
• acct-output-octets
• acct-output-packets
• acct-session-id
• acct-session-time
• acct-statustype
• called-station-id
• calling-station-id
• class
• event-timestamp
• framed-ip-address
• framed-ipv6-prefix
• imsi
• nas-identifier
• nas-ip-address
• nas-port-type
• service-type
• username

By default, all of the attributes are enabled.

**authentication authentication_attribute**

Enables RADIUS authentication attributes for the following options, provided they are supported in the configured RADIUS dictionary:

• 3gpp-cg-address
• 3gpp-charging-characteristics
• 3gpp-ggsn-address
AAA Server Group Configuration Mode Commands

radius attribute

Cisco ASR 5x00 Command Line Interface Reference

By default, all of the attributes are enabled.

- 3gpp-ggsn-mcc-mnc
- 3gpp-gprs-qos-negotiated-profile
- 3gpp-imeisv
- 3gpp-imsi-mcc-mnc
- 3gpp-ms-timezone
- 3gpp-nsapi
- 3gpp-pdp-type
- 3gpp-rat-type
- 3gpp-select-mode
- 3gpp-sgsn-address
- 3gpp-sgsn-mcc-mnc
- 3gpp-user-location-info
- called-station-id
- calling-station-id
- chap-challenge
- framed-ipaddress
- framed-ipv6-prefix
- imsi
- nas-identifier
- nas-ip-address
- nas-port-type
- service-type
- username

By default, all of the attributes are enabled.

**nas-identifier nas_id**

Specifies the attribute name by which the system will be identified in Access-Request messages. *nas_id* must be a case-sensitive alphanumeric string of 1 through 32 characters.

**nas-ip-address address primary_address**

Specifies the AAA interface IP address(es) used to identify the system. Up to two addresses can be configured.

*primary_address*: The IP address of the primary interface to use in the current context. This must be specified using the IPv4 dotted-decimal notation.

**Important**: In 12.0 and earlier releases, the configuration of NAS IP address with IPv6 prefix is currently not supported.
backup secondary_address

backup: The IP address of the secondary interface to use in the current context. This must be specified using IPv4 dotted-decimal notation.

next-hop-forwarding-address next-hop_address

Configures next hop IP address for this NAS IP address. It optionally sets the RADIUS client to provide VLAN ID and nexthop forwarding address to system when running in single nexthop gateway mode. next-hop_address must be specified using IPv4 dotted-decimal notation.

Important: To define more than one NAS IP address per context, in Global Configuration Mode use the aaa large-configuration command. If enabled, for a PDSN a maximum of 400 and for a GGSN a maximum of 800 NAS IP addresses/NAS identifiers (1 primary and 1 secondary per server group) can be configured per context.

mpls-label input in_label_value | output out_label_value1 [ out_label_value2 ]

Configures the traffic from the specified RADIUS client NAS IP address to use the specified MPLS labels.

- in_label_value is the MPLS label that will identify inbound traffic destined for the configured NAS IP address.
- out_label_value1 and out_label_value2 identify the MPLS labels to be added to packets sent from the specified NAS IP address.
- out_label_value1 is the inner output label.
- out_label_value2 is the outer output label.

MPLS label values must be an integer from 16 to 1048575.

vlan vlan_id

This optional keyword sets the RADIUS client to provide VLAN ID with nexthop forwarding address to system when running in single nexthop gateway mode.

vlan_id must be a pre-configured VLAN ID, and must be an integer from 1 through 4096. It is the VLAN ID to be provided to the system in RADIUS attributes.

This option is available only when nexthop-forwarding gateway is also configured with nexthop-forwarding-address next-hop_address keyword and aaa-large configuration is enabled at Global Configuration level.

Usage

This is necessary for NetWare Access Server usage such as the system must be identified to the NAS. The system supports the concept of the active nas-ip-address. The active nas-ip-address is defined as the current source ip address for RADIUS messages being used by the system. This is the content of the nas-ip-address attribute in each RADIUS message.

The system will always have exactly one active nas-ip-address. The active nas-ip-address will start as the primary nas-ip-address. However, the active nas-ip-address may switch from the primary to the backup, or the backup to the primary. The following events will occur when the active nas-ip-address is switched:

- All current in-process RADIUS accounting messages from the entire system are cancelled. The accounting message is re-sent, with retries preserved, using the new active nas-ip-address. Acct-Delay-Time, however, is updated to reflect the time that has occurred since the accounting event. The value of Event-Timestamp is preserved.
• All current in-process RADIUS authentication messages from the entire system are cancelled. The authentication message is re-sent, with retries preserved, using the new active nas-ip-address. The value of Event-Timestamp is preserved.

• All subsequent in-process RADIUS requests uses the new active nas-ip-address.

The system uses a revertive algorithm when transitioning active NAS IP addresses as described below:

• If the configured primary nas-ip-address transitions from UP to DOWN, and the backup nas-ip-address is UP, then the active nas-ip-address switches from the primary to the backup nas-ip-address.

• If the backup nas-ip-address is active, and the primary nas-ip-address transitions from DOWN to UP, then the active nas-ip-address switches from the backup to the primary nas-ip-address.

Example

The following command configures the RADIUS identification parameter, NAS IP address to 10.2.3.4.

```
radius attribute nas-ip-address 10.2.3.4
```
radius authenticate

This command configures RADIUS authentication related parameters.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > AAA Server Group Configuration

configure > context context_name > aaa group group_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-aaa-group)#

Syntax

radius authenticate { apn-to-be-included { gi | gn } | null-username }

default radius authenticate { apn-to-be-included | null-username }

no radius authenticate null-username

default
Configures the default setting.

no radius authenticate null-username
Disables sending an Access-Request message to the AAA server for user names (NAI) that are blank.

apn-to-be-included
Specifies the APN name to be included for RADIUS authentication.

gi: Specifies the usage of Gi APN name in RADIUS authentication request. Gi APN represents the APN received in the Create PDP Context request message from SGSN.

gn: Specifies the usage of Gn APN name in RADIUS authentication request. Gn APN represents the APN selected by the GGSN.

null-username
Specifies attempting RADIUS authentication even if the provided user name is NULL (empty).
Default: Enables authenticating, sending Access-Request messages to the AAA server, all user names, including NULL user names.

Usage
Use this command to disable, or re-enable, sending Access-Request messages to the AAA server for user names (NAI) that are blank (NULL).

Example
The following command disables sending of Access-Request messages for user names (NAI) that are blank:
no radius authenticate null-username

The following command re-enables sending of Access-Request messages for user names (NAI) that are blank:

radius authenticate null-username
radius authenticator-validation

This command enables/disables the MD5 authentication of RADIUS user. MD5 authentication is enabled by default.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > AAA Server Group Configuration

configure > context context_name > aaa group group_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-aaa-group)#

Syntax

[ default | no ] radius authenticator-validation

no

Disables MD5 authentication validation for an Access-Request message to the AAA server.

Usage

Use this command to disable or re-enable, sending Access-Request messages to the AAA server for MD5 validation.

Example

The following command disables MD5 authentication validation for Access-Request messages for user names (NAI):

    no radius authenticator-validation

The following command enables MD5 authentication validation for Access-Request messages for user names (NAI):

    radius authenticator-validation
radius charging

This command configures basic RADIUS options for Active Charging Service (ACS).

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > AAA Server Group Configuration
configure > context context_name > aaa group group_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-aaa-group)#

Syntax

radius charging { deadtime dead_time | detect-dead-server { consecutive-failures consecutive_failures_count | response-timeout response_timeout_duration } | max-outstanding max_messages | max-retries max_retries | max-transmissions max_transmissions | timeout idle_seconds }

default radius charging { deadtime | detect-dead-server | max-outstanding | max-retries | max-transmissions | timeout }

no radius charging { detect-dead-server | max-transmissions | timeout }

no

Removes the specified configuration.

default

Configures the default setting for the specified keyword.

deadtime dead_time

Specifies the number of minutes to wait before attempting to communicate with a server that has been marked as unreachable.

dead_time must be an integer from 0 through 65535.
Default: 10

detect-dead-server { consecutive-failures consecutive_failures_count | response-timeout response_timeout_duration }

consecutive-failures consecutive_failures_count: Specifies the number of consecutive failures, for each AAA Manager, before a server is marked as unreachable.

consecutive_failures_count must be an integer from 1 through 1000.
Default: 4

response-timeout response_timeout_duration: Specifies the number of seconds for each AAA Manager to wait for a response to any message before a server is detected as failed, or in a down state.

response_timeout_duration must be an integer from 1 through 65535.
max-outstanding max_messages
Specifies the maximum number of outstanding messages a single AAA Manager instance will queue.
max_messages must be an integer from 1 through 4000.
Default: 256

max-retries max_retries
Specifies the maximum number of times communication with a AAA server will be attempted before it is marked as unreachable, and the detect dead servers consecutive failures count is incremented.
max_retries must be an integer from 0 through 65535.
Default: 5

max-transmissions max_transmissions
Sets the maximum number of re-transmissions for RADIUS authentication requests. This limit is used in conjunction with the max-retries parameter for each server.
When failing to communicate with a RADIUS server, the subscriber is failed once all of the configured RADIUS servers have been exhausted or once the configured number of maximum transmissions is reached. For example, if three servers are configured and if the configured max-retries is 3 and max-transmissions is 12, then the primary server is tried four times (once plus three retries), the secondary server is tried four times, and then a third server is tried four times. If there is a fourth server, it is not tried because the maximum number of transmissions (12) has been reached.
max_transmissions must be an integer from 1 through 65535.
Default: Disabled

timeout idle_seconds
Specifies the number of seconds to wait for a response from the RADIUS server before re-sending the messages.
idle_seconds must be an integer from 1 through 65535.
Default: 3

Usage
Use this command to manage the basic Charging Service RADIUS options according to the RADIUS server used for the context.

Example
The following command configures the AAA server to be marked as unreachable when the consecutive failure count exceeds 6:

```
radius charging detect-dead-server consecutive-failures 6
```

The following command sets the timeout value to 300 seconds to wait for a response from RADIUS server before resending the messages:

```
radius charging timeout 300
```
radius charging accounting algorithm

This command specifies the fail-over/load-balancing algorithm to be used for selecting RADIUS servers for charging services.

Product
- PDSN
- GGSN

Privilege
- Security Administrator, Administrator

Mode
- Exec > Global Configuration > Context Configuration > AAA Server Group Configuration
- configure > context context_name > aaa group group_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-aaa-group)#

Syntax

```
radius charging accounting algorithm { first-n \n | first-server | round-robin }\n```

```
first-n \n
Specifies that the AGW must send accounting data to n (more than one) AAA servers based on their priority. Response from any one of the n AAA servers would suffice to proceed with the call. The full set of accounting data is sent to each of the n AAA servers. 
\n n is the number of AAA servers to which accounting data will be sent, and must be an integer from 2 through 128. 
\n Default: 1 (Disabled)
```

```
first-server

Specifies that the context must send accounting data to the RADIUS server with the highest configured priority. In the event that this server becomes unreachable, accounting data is sent to the server with the next-highest configured priority. This is the default algorithm.
```

```
round-robin

Specifies that the context must load balance sending accounting data among all of the defined RADIUS servers. Accounting data is sent in a circular queue fashion on a per Session Manager task basis, where data is sent to the next available server and restarts at the beginning of the list of configured servers. The order of the list is based upon the configured relative priority of the servers.
```

Usage

Use this command to specify the accounting algorithm to use to select RADIUS servers for charging services configured in the current context.

Example

The following command configures to use the round-robin algorithm for RADIUS server selection:

```
radius charging accounting algorithm round-robin
```
radius charging accounting server

This command configures RADIUS charging accounting servers in the current context for ACS Prepaid Accounting.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > AAA Server Group Configuration

```bash
configure > context context_name > aaa group group_name
```

Entering the above command sequence results in the following prompt:

```bash
[context_name]host_name(config-aaa-group)#
```

**Syntax**

```bash
radius charging accounting server ip_address [ encrypted ] key value [ max max_messages ] [ oldports ] [ port port_number ] [ priority priority ] [ admin-status { enable | disable } ] [ -noconfirm ]
```

```bash
no radius charging accounting server ip_address [ oldports | port port_number ]
```

**ip_address**

Specifies the IP address of the accounting server. `ip_address` must be specified using IPv4 dotted-decimal notation. A maximum of 128 RADIUS servers can be configured per context. This limit includes accounting and authentication servers.

```bash
[ encrypted ] key value
```

Specifies the shared secret key used to authenticate the client to the servers. The `encrypted` keyword indicates the key specified is encrypted.

In 12.1 and earlier releases, the `key value` must be an alphanumeric string of 1 through 127 characters without encryption, and 1 through 256 characters with encryption.

In StarOS 12.2 and later releases, the `key value` must be an alphanumeric string of 1 through 127 characters without encryption, and 1 through 236 characters with encryption enabled.

The `encrypted` keyword is intended only for use by the system while saving configuration scripts. The system displays the `encrypted` keyword in the configuration file as a flag that the variable following the `key` keyword is the encrypted version of the plain text key. Only the encrypted key is saved as part of the configuration file.

**max max_messages**

Specifies the maximum number of outstanding messages that may be allowed to the server. `max_messages` must be an integer from 0 through 4000.

Default: 0
oldports
Sets the UDP communication port to the out of date standardized default for RADIUS communications to 1646.

port port_number
Specifies the port number to use for communication. 
port_number must be an integer from 0 through 65535. 
Default: 1813

priority priority
Specifies the relative priority of this accounting server. The priority is used in server selection for determining which server to send accounting data to. priority must be an integer from 1 through 1000, where 1 is the highest priority. 
Default: 1000

admin-status { enable | disable }
Enables or disables the RADIUS authentication/accounting/charging server functionality and saves the status setting in the configuration file to re-establish the set status at reboot.

-noconfirm
Specifies that the command must execute without any prompts and confirmation from the user.

Usage
This command is used to configure the RADIUS charging accounting server(s) with which the system is to communicate for ACS Prepaid Accounting requests. 
Up to 128 AAA servers can be configured per context when the system is functioning as a PDSN and/or HA. 
Up to 16 servers are supported per context when the system is functioning as a GGSN.

Example
The following commands configure RADIUS charging accounting server with the IP address set to 10.1.2.3, port to 1024, priority to 10:

```
radius charging accounting server 10.1.2.3 key sharedKey212 port 1024 max 127
radius charging accounting server 10.1.2.3 encrypted key scrambledKey234 oldports priority 10
```
radius charging algorithm

This command specifies the RADIUS authentication server selection algorithm for ACS for the current context.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > AAA Server Group Configuration

```
configure > context context_name > aaa group group_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-aaa-group)#
```

**Syntax**

```
radius charging algorithm { first-server | round-robin }
```

**default radius charging algorithm**

```
default
```

Configures the default setting.
Default: first-server

```
first-server
```

Accounting data is sent to the first available server based upon the relative priority of each configured server.

```
round-robin
```

Accounting data is sent in a circular queue fashion on a per Session Manager task basis where data is sent to the next available server and restarts at the beginning of the list of configured servers. The order of the list is based upon the configured relative priority of the servers.

**Usage**

Use this command to configure the context’s RADIUS server selection algorithm for ACS to ensure proper load distribution amongst the available servers.

**Example**

The following command configures to use the round-robin algorithm for RADIUS server selection:

```
radius algorithm round-robin
```
radius charging server

This command configures the RADIUS charging server(s) in the current context for ACS Prepaid Authentication.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > AAA Server Group Configuration

configure > context context_name > aaa group group_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-aaa-group)#

Syntax

radius charging server ip_address [ encrypted ] key value [ max max_messages ] [ oldports ] [ port port_number ] [ priority priority ] [ admin-status { enable | disable } ] [ -noconfirm ]

no radius charging server ip_address [ oldports | port port_number ]

no

Removes the server or server port(s) specified from the list of configured servers.

ip_address

Specifies the IP address of the server. ip_address must be specified using IPv4 dotted-decimal notation. A maximum of 128 RADIUS servers can be configured per context. This limit includes accounting and authentication servers.

[ encrypted ] key value

Specifies the shared secret key used to authenticate the client to the servers. The encrypted keyword indicates the key specified is encrypted. In 12.1 and earlier releases, the key value must be an alphanumeric string of 1 through 127 characters without encryption, and 1 through 256 characters with encryption. In StarOS 12.2 and later releases, the key value must be an alphanumeric string of 1 through 127 characters without encryption, and 1 through 236 characters with encryption enabled. The encrypted keyword is intended only for use by the system while saving configuration scripts. The system displays the encrypted keyword in the configuration file as a flag that the variable following the key keyword is the encrypted version of the plain text key. Only the encrypted key is saved as part of the configuration file.

max max_messages

Specifies the maximum number of outstanding messages that may be allowed to the server. max_messages must be an integer from 0 through 4000. Default: 256
oldports
Sets the UDP communication port to the old default for RADIUS communications to 1645.

port port_number
Specifies the port number to use for communications.
port_number must be an integer from 1 through 65535.
Default: 1812

priority priority
Specifies the relative priority of this accounting server. The priority is used in server selection for determining which server to send accounting data to.
priority must be an integer from 1 through 1000, where 1 is the highest priority.
Default: 1000

admin-status { enable | disable }
Enables or disables the RADIUS authentication, accounting, or charging server functionality and saves the status setting in the configuration file to re-establish the set status at reboot.

-noconfirm
Specifies that the command must execute without any prompts and confirmation from the user.

Usage
This command is used to configure the RADIUS charging server(s) with which the system is to communicate for ACS Prepaid Authentication requests.
Up to 128 AAA servers can be configured per context when the system is functioning as a PDSN and/or HA.
Up to 16 servers are supported per context when the system is functioning as a GGSN.

Example
The following commands configure RADIUS charging server with the IP address set to 10.2.3.4, port to 1024, priority to 10:

    radius charging server 10.2.3.4 key sharedKey212 port 1024 max 127
    radius charging server 10.2.3.4 encrypted key scrambledKey234 oldports priority 10
radius ip vrf

This command associates the specific AAA group (NAS-IP) with a Virtual Routing and Forwarding (VRF) Context instance for BGP/MPLS, GRE, and IPSec Tunnel functionality which needs VRF support for RADIUS communication. By default the VRF is NULL, which means that AAA group is associated with global routing table.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > AAA Server Group Configuration
configure > context context_name > aaa group group_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-aaa-group)#

Syntax

radius ip vrf vrf_name

no radius ip vrf

no

Disables the configured IP Virtual Routing and Forwarding (VRF) context instance and removes the association between the VRF context instance and the AAA group instance (NAS-IP).
By default this command is disabled, which means the NAS-IP being used is assumed a non-VRF IP and specific AAA group does not have any VRF association.

vrf_name

Specifies the name of a pre-configured VRF context instance.

vrf_name is the name of a pre-configured virtual routing and forwarding (VRF) context configured in Context configuration mode through ip vrf command.

⚠️ Caution: Any incorrect configuration, such as associating AAA group with wrong VRF instance or removing a VRF instance, will fail the RADIUS communication.

Usage

Use this command to associate/disassociate a pre-configured VRF context for a feature such as BGP/MPLS VPN or GRE, and IPSec tunneling which needs VRF support for RADIUS communication.
By default the VRF is NULL, which means that AAA group (NAS-IP) is associated with global routing table and NAS-IP being used is assumed a non-VRF IP.
This IP VRF feature can be applied to RADIUS communication, which associates the VRF with the AAA group. This command must be configured whenever a VRF IP is used as a NAS-IP in the AAA group or at the Context level for the “default” AAA group.
This is a required configuration as VRF IPs may be overlapping hence AAA needs to know which VRF the configured NAS-IP belongs to. By this support different VRF-based subscribers can communicate with...
different RADIUS servers using the same, overlapping NAS-IP address, if required across different AAA groups.

Example

The following command associates VRF context instance `ip_vrf1` with specific AAA group (NAS-IP):

```
radius ip vrf ip_vrf1
```
radius keepalive

This command configures the RADIUS keepalive authentication parameters.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > AAA Server Group Configuration

configure > context context_name > aaa group group_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-aaa-group)#

Syntax

radius keepalive { calling-station-id id | consecutive-response number | encrypted | interval seconds | password | retries number | timeout seconds | username user_name | valid-response access-accept [ access-reject ] }

default radius keepalive { calling-station-id | consecutive-response | interval | password | retries | timeout | username | valid-response }

default

Configures the default setting for the specified keyword.

calling-station-id id

Specifies the Calling-Station-Id to be used for the keepalive authentication.
$id$ must be an alphanumeric string of size 1 to 15 characters.
Default: 000000000000000

consecutive-response number

Specifies the number of consecutive authentication responses after which the server is marked as reachable.
$number$ must be an integer from 1 through 10.
Default: 1

encrypted password

Specifies encrypting the password.
In 12.1 and earlier releases, the $password$ must be an alphanumeric string of 1 through 63 characters.
In StarOS 12.2 and later releases, $password$ must be an alphanumeric string of 1 through 132 characters.
Default password: Test-Password

interval seconds

Specifies the time interval, in seconds, between two keepalive access requests.
Default: 30 seconds
** AAA Server Group Configuration Mode Commands **

---

**radius keepalive**

---

**password**

Specifies the password to be used for authentication.

`password` must be an alphanumeric string of 1 through 63 characters.

Default password: Test-Password

---

**retries number**

Specifies the number of times the keepalive access request to be sent before marking the server as unreachable.

`number` must be an integer from 3 through 10.

Default: 3

---

**timeout timeout_duration**

Specifies the time interval between keepalive access request retries.

`timeout_duration` must be an integer from 1 through 30.

Default: 3 seconds

---

**username user_name**

Specifies the user name to be used for authentication.

`user_name` must be an alphanumeric string of 1 through 127 characters.

Default: Test-Username

---

**valid-response access-accept [ access-reject ]**

Specifies the valid response for the authentication request.

- If `access-reject` is configured, then both access-accept and access-reject are considered as success for the keepalive authentication request.
- If `access-reject` is not configured, then only access-accept is considered as success for the keepalive access request.

Default: `keepalive valid-response access-accept`

---

**Usage**

Use this command to configure the keepalive authentication parameters for the RADIUS server.

---

**Example**

The following command configures the user name for RADIUS keepalive access requests to `Test-Username2`:

```
radius keepalive username Test-Username2
```

The following command configures the number of RADIUS keepalive retries to 4:

```
radius keepalive retries 4
```
radius mediation-device

See the radius accounting server command.
## radius probe-interval

This command configures the time interval between two RADIUS authentication probes.

### Product

All

### Privilege

Security Administrator, Administrator

### Mode

Exec > Global Configuration > Context Configuration > AAA Server Group Configuration

```
configure > context context_name > aaa group group_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-aaa-group)#
```

### Syntax

```
radius probe-interval seconds
```

```
default radius probe-interval
```

```
default
```

Configures the default setting.

```
default
```

```
seconds
```

Specifies the number of seconds to wait before sending another probe authentication request to a RADIUS server.

- `seconds` must be an integer from 1 through 65535.
- Default: 60

### Usage

Use this command for Interchassis Session Recovery (ICSR) support to set the duration between two authentication probes to the RADIUS server.

### Example

The following command sets the RADIUS authentication probe interval to 30 seconds.

```
radius probe-interval 30
```
radius probe-max-retries

This command configures the number of retries for RADIUS authentication probe response.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > AAA Server Group Configuration

configure > context context_name > aaa group group_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-aaa-group)#

Syntax

radius probe-max-retries retries

default radius probe-max-retries

default

Configures the default setting.

retries

Specifies the number of retries for RADIUS authentication probe response before the authentication is declared as failed.

retries must be an integer from 0 through 65535.

Default: 5

Usage

Use this command with Interchassis Session Recovery (ICSR) to set the number of attempts to send RADIUS authentication probe without a response before the authentication is declared as failed.

Example

The following command configures the maximum number of retries to 6 seconds.

radius probe-max-retries 6
radius probe-timeout

This command configures the timeout duration for Interchassis Session Recovery (ICSR) to wait for a response for RADIUS authentication probes.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > AAA Server Group Configuration

```configure > context  context_name > aaa group  group_name```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-aaa-group)\#```

**Syntax**

```radius probe-timeout  idle_seconds```

**default radius probe-timeout**

```default```

Configures the default setting.

```idle_seconds```

Specifies the number of seconds to wait for a response from the RADIUS server before re-sending the authentication probe. 

`idle_seconds` must be an integer from 0 through 65535. 

Default: 3

**Usage**

Use this command to set the time duration for ICSR, to wait for a response before re-sending the RADIUS authentication probe to the RADIUS server.

**Example**

The following command sets the authentication probe timeout to 120 seconds:

```radius probe-timeout 120```
radius server

This command configures RADIUS authentication server(s) in the current context for authentication.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > AAA Server Group Configuration

`configure > context context_name > aaa group group_name`

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-aaa-group)#`

**Syntax**

```plaintext
radius server ip_address [ encrypted ] key value [ admin-status { disable | enable } ] [ max max_messages ] [ max-rate max_value ] [ oldports ] [ port port_number ] [ priority priority ] [ probe | no-probe ] [ probe-username user_name ] [ probe-password [ encrypted ] password password ] [ type { mediation-device | standard } ] [ -noconfirm ]
```

```plaintext
no radius server ip_address [ oldports | port port_number ]
```

- no

Removes the server or server port(s) specified from the list of configured servers.

```plaintext
ip_address port port_number
```

Specifies the IP address and port number of the server.

- `ip_address`: Must be specified using IPv4 dotted-decimal notation. A maximum of 1600 RADIUS servers per context/system and 128 servers per Server group can be configured. This limit includes accounting and authentication servers.
- `port port_number`: Specifies the port number to use for communications. `port_number` must be an integer from 1 through 65535. Default: 1812.

**Important:** The same RADIUS server IP address and port can be configured in multiple RADIUS server groups within a context.

```plaintext
[ encrypted ] key value
```

Specifies the shared secret key used to authenticate the client to the servers. The `encrypted` keyword indicates the key specified is encrypted.

- In 12.1 and earlier releases, the key `value` must be an alphanumeric string of 1 through 127 characters without encryption, and 1 through 256 characters with encryption.
- In StarOS 12.2 and later releases, the key `value` must be an alphanumeric string of 1 through 127 characters without encryption, and 1 through 236 characters with encryption enabled.
The **encrypted** keyword is intended only for use by the chassis while saving configuration scripts. The system displays the **encrypted** keyword in the configuration file as a flag that the variable following the **key** keyword is the encrypted version of the plain text key. Only the encrypted key is saved as part of the configuration file.

```
admin-status { disable | enable }
```

Enables or disables the RADIUS authentication, accounting, or charging server functionality and saves the status setting in the configuration file to re-establish the set status at reboot.

```
max max_messages
```

Specifies the maximum number of outstanding messages that may be allowed to the server. 

*max_messages* must be an integer from 0 through 4000.

Default: 256

```
max-rate max_value
```

Specifies the rate at which the authentication messages should be sent to the RADIUS server by a single AAA manager task.

*max_value* must be an integer from 0 through 1000.

Default: 0 (disabled)

```
oldports
```

Sets the UDP communication port to the old default for RADIUS communications to 1645.

```
priority priority
```

Specifies the relative priority of this accounting server. The priority is used in server selection for determining which server to send accounting data to.

*priority* must be an integer from 1 through 1000, where 1 is the highest priority. When configuring two or more servers with the same priority you will be asked to confirm that you want to do this. If you use the **-noconfirm** option, you are not asked for confirmation and multiple servers could be assigned the same priority.

Default: 1000

```
probe
```

Enable probe messages to be sent to the specified RADIUS server.

```
no-probe
```

Disable probe messages from being sent to the specified RADIUS server. This is the default behavior.

```
probe-username user_name
```

The user name sent to the RADIUS server to authenticate probe messages. *user_name* must be an alphanumeric string of 1 through 127 characters.

```
probe-password [ encrypted ] password
```

The password sent to the RADIUS server to authenticate probe messages.

*encrypted*: This keyword is intended only for use by the chassis while saving configuration scripts. The system displays the **encrypted** keyword in the configuration file as a flag that the variable following the
password keyword is the encrypted version of the plain text password. Only the encrypted password is saved as part of the configuration file.

**password** *password*: Specifies the probe-user password for authentication. *password* must be an alphanumeric string of 1 through 63 characters.

### type { mediation-device | standard }

Specifies the type of transactions the RADIUS server accepts.

- **mediation-device**: Specifies mediation-device specific AAA transactions. This device is available if you purchased a transaction control services license. Contact your local Cisco representative for licensing information.
- **standard**: Specifies standard AAA transactions. (Default)

---

**-noconfirm**

Specifies that the command must execute without any prompts and confirmation from the user.

---

**Usage**

This command is used to configure the RADIUS authentication server(s) with which the system is to communicate for authentication.

You can configure up to 1600 RADIUS servers per context/system and 128 servers per Server group. The servers can be configured as accounting, authentication, charging servers, or any combination thereof.

**Example**

The following commands configure RADIUS server with the IP address set to 10.2.3.4, port to 1024, priority to 10:

```
radius server 10.2.3.4 key sharedKey212 port 1024 max 127
radius server 10.2.3.4 encrypted key scrambledKey234 oldports priority 10
```
radius trigger

This command enables specific RADIUS triggers.

Product

GGSN
P-GW
SAEGW

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > Context Configuration > AAA Server Group Configuration

configure > context context_name > aaa group group_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-aaa-group)#

Syntax

[ no ] radius trigger { ms-timezone-change | qos-change | rai-change | rat-change | serving-node-change | uli-change }

default radius trigger

no
Disables specified RADIUS trigger.

default
Configures the default setting.
Default: All RADIUS triggers are enabled.

ms-timezone-change
Specifies to enable RADIUS trigger for MS time zone change.

qos-change
Specifies to enable RADIUS trigger for Quality of Service change.

rae-change
Specifies to enable RADIUS trigger for Routing Area Information change.

rat-change
Specifies to enable RADIUS trigger for Radio Access Technology change.

serving-node-change
Specifies to enable RADIUS trigger for Serving Node change.
**uli-change**

Specifies to enable RADIUS trigger for User Location Information change.

---

### Usage

Use this command to enable RADIUS triggers.

### Example

The following command enables RADIUS trigger for RAT change:

```
radius trigger rat-change
```
Chapter 3
AAL2 Node Configuration Mode Commands

The AAL2 Node Configuration Mode is used to configure the ATM Adaptation Layer 2 nodes to manage the Access Link Control Application Part (ALCAP) on HNB-GW for IuCS-over-ATM support towards CS core network.

Exec > Global Configuration > Context Configuration > ALCAP Service Configuration > AAL2 Node Configuration
configure > context context_name > alcap-service service_name > aal2-node node_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-aal2-node-node_name)#

**Important:** The AAL2 Node configured here will be used to bind with ATM port in PVC configuration sub-mode of ATM configuration mode for IuCS-over-ATM functionality.

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
**aal2-path-id**

This command sets the AAL2 path identifier with AAL2 node and also used to block a particular AAL2 path.

**Product**
HNB-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > ALCAP Service Configuration > AAL2 Node Configuration

```
configure > context context_name > alcap-service service_name > aal2-node node_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-aal2-node-node_name)#
```

**Syntax**

```
[no] aal2-path-id aal2_path_id [block]
```

- **no**
  Removes the configured AAL2 path identifier from this AAL2 node configuration.

- **aal2_path_id**
  Specifies the AAL2 path identifier configured with adjacent AAL2 node(s). The AAL2 path id must be unique within an AAL2 node configuration. This value is used to identify a particular path towards an adjacent AAL2 node and is sent in ALCAP protocol messages to peer where path identification is required. The `aal2_path_id` must be an integer between 1 through 4294967295.

**Important:** This AAL2 path id `aal2_path_id` will be used to bind with ATM port in PVC configuration mode of ATM configuration mode.

- **block**
  This keyword block the AAL2 path configured with specific path identifier. When this keyword is executed ALCAP-BLO-REQUEST shall be sent to the adjacent AAL2 node.
  To unblock an AAL2 path, the no keyword will be used for a locally blocked path by sending ALCAP-UNBLOCK-REQUEST to the adjacent AAL2 node.

**Usage**

Use this command to configure an AAL2 path between a pair of adjacent nodes, which is identified by a unique number called AAL2 path identifier. An AAL2 path provides 248 AAL2 channels wherein each AAL2 channel is used for one circuit switched call. The AAL2 channel range defined is 8 to 255.
This command can be used for blocking or unblocking an AAL2 path towards an adjacent AAL2 node.

**Important:** The AAL2 path id configured here will be used to bind with ATM port in PVC configuration sub-mode of ATM configuration mode for IuCS-over-ATM functionality.
Example

Following command sets the AAL2 path identifier 2 in an AAL2 node configuration.

```
al2-path-id 2
```

Following command unblocks the AAL2 path identifier 6 which was earlier blocked in an AAL2 node configuration.

```
no al2-path-id 6 block
```
end

Exits the current mode and returns to the Exec Mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**
Change the mode back to the Exec mode.
exit

Exits the current mode and returns to the previous mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Return to the previous mode.
point-code

This command configure the point code of adjacent AAL2 node in SS7 format address. This point code shall be filled in the destination point-code (dpc) field of MTP3 routing label. This is required if signaling transport network is based on MTP3-broadband (MTP3B).

Product
HNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > ALCAP Service Configuration > AAL2 Node Configuration

configure > context context_name > alcap-service service_name > aal2-node node_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-aal2-node-node_name)#

Syntax
[no] point-code point_code

no
Removes the configured point code from this AAL2 node configuration.

point_code
Defines the point code to assign to adjacent AAL2 node in SS7 format.

point_code: value entered must adhere to the point code variant selected when the AAL2 node was defined:

- ITU Range 0.0.1 to 7.255.7
- ANSI Range 0.0.1 to 255.255.255
- TTC Range 0.0.1 to 15.31.255
- a string of 1 to 11 combined digits ad period.

Usage
Use this command to configure configure the point code of adjacent AAL2 node in SS7 format address. This point code shall be filled in the destination point-code (dpc) field of MTP3 routing label. This is required if signaling transport network is based on MTP3-broadband (MTP3B).

A maximum of 16 point codes for adjacent AAL2 nodes can be configured in one ALCAP service.

Example
The following command configures the point code 4.121.5 for adjacent AAL2 node.

point-code 4.121.5

The following command removes the point code 4.121.15 from AAL2 node configuration.

no point-code 4.121.15
Chapter 4
Accounting Policy Configuration Mode Commands

The Accounting Policy Configuration Mode is used to define the accounting method, mode, and event trigger responses for the accounting policy supporting the Rf (off-line charging) interface.

**Mode**

Exec > Global Configuration > Context Configuration > Accounting Policy Configuration

`configure > context context_name > policy accounting policy_name`

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-accounting-policy)#`

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
accounting-event-trigger

Configures the response to specific event triggers for this policy. Multiple event instances can be configured.

Product
HSGW
P-GW
S-GW
SAEGW

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > Accounting Policy Configuration

configure > context context_name > policy accounting policy_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-accounting-policy)#

Syntax

accounting-event-trigger { cgi-sai-change | ecgi-change | flow-information-change | interim-timeout | location-change | rai-change | tai-change } action { interim | stop-start }

[ default | no ] accounting-event-trigger { cgi-sai-change | ecgi-change | flow-information-change | interim-timeout | location-change | rai-change | tai-change }

Default
Returns the command to its default setting of interim for the action keyword (for all events).

No
Removes the specified event trigger configuration from this policy.

cgi-sai-change
Specifies that the action is initiated upon indication of a Cell Global Identification-Service Area Identification (CGI-SAI) change.

ecgi-change
Specifies that the action is initiated upon indication of an E-UTRAN Cell Global Identifier (ECGI) change.

flow-information-change
Specifies that the action is initiated upon indication of a change in the flow information.

interim-timeout
Specifies that the action is initiated upon expiration of the interim interval.
location-change
Specifies that the action is initiated upon indication of a location change.

rai-change
Specifies that the action is initiated upon indication of an Routing Area Identifier (RAI) change.

tai-change
Specifies that the action is initiated upon indication of a Tracking Area Identity (TAI) change.

action { interim | stop-start }
Default: interim
Specifies the action initiated upon the occurrence of an event.
interim: Specifies that an interim ACR (Accounting Request) is sent.
stop-start: Specifies that a Stop-Start ACR is sent.

Usage
Use the is command to configure that action taken upon the occurrence on an accounting event trigger.

Example
The following command configures the policy to send a Stop-Start ACR upon indication of an interim timeout:

    accounting-event-trigger interim-timeout action stop-start
accounting-keys

Aggregates the accounting information, using the configurable keys (QCI) along with default keys.

Product
HSGW
P-GW
S-GW
SAEGW

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > Accounting Policy Configuration

configure > context context_name > policy accounting policy_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-accounting-policy)#

Syntax

accounting-keys qci

default accounting-keys

default
Aggregate the accounting information, using QoS Class Identifier (QCI) as the additional key.

qci
Aggregate the accounting information, using QCI as the additional key.

Usage
Use this command to aggregate the accounting information, using the configurable keys (QCI) along with default keys.
In service data flow (SDF) level accounting, buckets are created and maintained using the Reporting-Level AVP value present in Gx message. The following are the accounting keys currently supported:
• Rating-group
• Rating-group and Service-Identifier
• Rating-group and QCI
• Rating-group, Service-Identifier, and QCI

Example

The following command aggregates the accounting information, using QCI as the additional key:

accounting-keys qci
accounting-level

Configures the type of accounting performed by this profile.

Product

- HSGW
- P-GW
- S-GW
- SAEGW

Privilege

Administrator

Mode

Exec > Global Configuration > Context Configuration > Accounting Policy Configuration

configure > context context_name > policy accounting policy_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-accounting-policy)#

Syntax

accounting-level { flow | pdn | pdn-qci | qci | sdf | subscriber }

default accounting-level

default

Returns the command to the default setting of subscriber-based accounting.

flow

Specifies that flow-based accounting is to be used for this accounting profile. Accounting Request (ACR) Start messages include an AVP with the following Evolved Packet System (EPS) information:

- PDN identifier
- QCI for which accounting is done
- Charging rule name for which accounting is being done
- AF charging identifier (included if PCRF has provided a charging identifier to correlate AF generated information)
- Flow description for the flows
- User Equipment information if available (ESN/MEID)
- Address of HSGW/S-GW
- Address of the P-GW (if available), one or more instances

pdn

Specifies that PDN-based accounting is to be used for this accounting profile. ACR Start messages include an AVP with the following EPS information:

- Addresses allocated to the UE in this PDN
• PDN identifier
• User Equipment information if available (ESN/MEID)
• Address of HSGW/S-GW
• Address of the P-GW (if available), one or more instances

`pdn-qci`

Specifies that PDN-QCI accounting is to be used for this accounting profile. ACR Start messages include an AVP with the following EPS information:
• Addresses allocated to the UE in this PDN
• PDN identifier
• QCI for which accounting is done
• User Equipment information if available (ESN/MEID)
• Address of HSGW/S-GW
• Address of the P-GW (if available), one or more instances

`qci`

Specifies that QCI-based accounting is to be used for this accounting profile. ACR Start messages include an AVP with the following EPS information:
• QCI for which accounting is done
• User Equipment information if available (ESN/MEID)
• Address of HSGW/S-GW
• Address of the P-GW (if available), one or more instances

`sdf`

Specifies that service data flow accounting is to be used for this accounting profile. ACR Start messages include an AVP with the following EPS information:

`subscriber`

Specifies that subscriber-based accounting is to be used for this accounting profile. ACR Start messages include an AVP with the following EPS information:
• User Equipment information if available (ESN/MEID)
• Address of HSGW/S-GW
• Address of the P-GW (if available), one or more instances

**Usage**

Use this command to specify the type of accounting performed by this profile.

**Example**

The following command sets the accounting type for this profile to flow-based:

```
accounting-level flow
```
accounting-mode

Configures the accounting mode for this profile.

**Product**
- HSGW
- P-GW
- S-GW
- SAEGW

**Privilege**
Administrator

**Mode**
- Exec > Global Configuration > Context Configuration > Accounting Policy Configuration
  - configure > context context_name > policy accounting policy_name
  - Entering the above command sequence results in the following prompt:
    
    `[context_name]host_name(config-accounting-policy)#`

**Syntax**

```
accounting-mode normal
default accounting-mode
```

```
<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>accounting-mode normal</code></td>
<td>Specifies that “normal” (start/interim/stop) accounting will be performed for this profile.</td>
</tr>
<tr>
<td><code>default accounting-mode</code></td>
<td>Returns the accounting mode for this profile to its default setting of “normal”.</td>
</tr>
</tbody>
</table>
```

**Usage**

Use this command to set the accounting mode for this profile.
apn-name-to-be-included

This command configures whether the virtual or real Access Point Name (APN) is sent in Rf accounting message.

Product
GGSN
P-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Accounting Policy Configuration
configure > context context_name > policy accounting policy_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-accounting-policy)#

Syntax

apn-name-to-be-included { gn | virtual }
default apn-name-to-be-included

default

Configures this command with the default setting.
Default: gn

gn
Sends the Gn APN name in the Rf accounting messages.

virtual

Sends the virtual APN name, if configured in the APN Configuration Mode, in the Rf accounting messages.

Usage

Use this command to configure the APN name to be included in Rf accounting messages. Virtual APN name can be set to be sent in Rf accounting messages if it is configured in the APN Configuration Mode.

Example

The following command sets the virtual APN name to be sent in Rf accounting message:

apn-name-to-be-included virtual
attribute

This command configures the attributes to be reported in Rf accounting.

Product
P-GW

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > Accounting Policy Configuration

configure > context context_name > policy accounting policy_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-accounting-policy)#

Syntax

[ default | no ] attribute csg

[ default | no ]
Specifies to disable reporting of attributes in Rf accounting.

csg
Specifies to enable reporting of Closed Subscriber Group (CSG) related IEs received during the initial attach (Create Session Request) for Rf accounting purpose.

Usage

Use this command to enable or disable the reporting of attributes received during the initial attach (Create Session Request) for Rf billing purpose.
CC

Configures a charging characteristics (CC) profile, within the accounting profile configuration, for CDR generation.

**Product**
- GGSN
- HSGW
- P-GW
- S-GW
- SAEGW

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Accounting Policy Configuration

`configure > context context_name > policy accounting policy_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-accounting-policy)#
```

**Syntax**

```
cc profile index { buckets num | interval seconds | sdf-interval seconds | sdf-volume { downlink octets { uplink octets } | total octets | uplink octets { downlink octets } } | serving-nodes num | tariff time1 min hrs [ time2 min hrs...time4 min hrs ] | volume { downlink octets { uplink octets } | total octets | uplink octets { downlink octets } } }

default cc profile index

no cc profile index { buckets | interval | sdf-interval | sdf-volume | serving-nodes | tariff | volume }

default
Returns all profile features, for the specified profile index, to their default settings.

no
Returns the specified feature to its default setting.

profile index
Specifies a billing type to be applied to this profile. `index` must be one of the following:
1: Hot billing
2: Flat billing
4: Prepaid billing
8: Normal billing
cyber

Cisco ASR 5x00 Command Line Interface Reference

231

Accounting Policy Configuration Mode Commands

`buckets num`
Default: 4
Specifies the number of container changes in the S-GW CDR due to QoS changes or tariff times. If an accounting policy is not configured, this value is 4. GTPP accounting will use the default value if the configured value is beyond 4.
In 12.1 and earlier releases, `num` must be an integer value from 1 through 4.
In release 12.2, `num` must be an integer value from 1 through 10.
In 12.3 and later releases, `num` must be an integer value from 1 through 20.

⚠️ Important: Please note that the maximum value for the CC profile buckets is extended to support up to 10 for Diameter Rf accounting only. However, in the case of GTPP accounting, this CLI command allows configuring only up to 4 buckets.

`interval seconds`
Default: disabled
Specifies a time interval for closing the charging record if the minimum volume thresholds are satisfied. `seconds` must be an integer value from 60 through 40000000.

`sdf-interval seconds`
Default: disabled
Specifies a time interval for closing the charging record for a specific flow if the minimum volume thresholds are satisfied. `seconds` must be an integer value from 60 through 40000000.

`sdf-volume { downlink octets { uplink octets } | total octets | uplink octets { downlink octets } }

Specifies octet volume thresholds for the generation of interim CDRs for a specific flow.
`downlink octets`: Sets the threshold limit for the number of downlink octets that must be reached before the charging record for a specific flow is closed. `octets` must be an integer value from 100000 through 4000000000.
`total octets`: Sets the threshold limit for the total number of octets that must be reached before the charging record for a specific flow is closed. `octets` must be an integer value from 100000 through 4000000000.
`uplink octets`: Sets the threshold limit for the number of uplink octets that must be reached before the charging record for a specific flow is closed. `octets` must be an integer value from 100000 through 4000000000.

`serving-nodes num`
Default: 4
Specifies the number of serving node changes (inter-serving node switchovers) after which the interim CDR is generated. In P-GW and S-GW, a partial record needs to be generated whenever there is a serving node address list overflow. Serving node is added to the CDR list during handover scenarios. `num` must be an integer value from 1 through 4. If an accounting policy is not configured, this value is 4.

`tariff time1 min hrs [ time2 min hrs...time4 min hrs ]`
Specifies time-of-day values used to determine when a container is closed in the charging records.
`time1 min hrs`: Specifies the first time-of-day value used to close the current container in the charging record. `min` must be an integer value from 0 through 59. `hrs` must be an integer value from 0 through 23.
time2 min hrs...time4 minutes hours: Specifies the second, third and fourth time-of-day values used to close containers in the charging record. min must be an integer value from 0 through 59. hrs must be an integer value from 0 through 23.

volume { downlink octets { uplink octets } | total octets | uplink octets { downlink octets } }

Specifies octet volume thresholds for the generation of interim CDRs.

downlink octets: Sets the threshold limit for the number of downlink octets that must be reached before the charging record is closed.
In 12.1 and earlier releases, the downlink octets must be an integer value from 100000 to 1345294336.
In 12.2 and later releases, the downlink octets must be an integer value from 100000 to 4000000000.

total octets: Sets the threshold limit for the total number of octets that must be reached before the charging record is closed.
In 12.1 and earlier releases, the total octets must be an integer value from 100000 to 4000000000.
In 12.2 and later releases, the total octets must be an integer value from 100000 to 4000000000.

uplink octets: Sets the threshold limit for the number of uplink octets that must be reached before the charging record is closed.
In 12.1 and earlier releases, the uplink octets must be an integer value from 100000 to 4000000000.
In 12.2 and later releases, the uplink octets must be an integer value from 100000 to 4000000000.

Usage
Use this command to set charging characteristics that directly affect the CDR generation on the HSGW, P-GW, or S-GW.

Example
The following command creates a hot billing profile with a total octet volume threshold set to 500000:

```
cc profile 1 volume total 500000
```
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
```
exit
```

**Usage**
Use this command to return to the parent configuration mode.
max-containers

Control the number of containers in an ACR message.

Product

- GGSN
- HSGW
- P-GW
- S-GW
- SAEGW

Privilege

- Administrator

Mode

Exec > Global Configuration > Context Configuration > Accounting Policy Configuration

configure > context context_name > policy accounting policy_name

Example

The following command sets a maximum of 20 containers in an ACR message:

```
max-containers 20
```
operator-string

Configures a text string to be included with accounting messages sent by this policy.

Product

HSGW
P-GW
S-GW
SAEGW

Privilege

Administrator

Mode

Exec > Global Configuration > Context Configuration > Accounting Policy Configuration

\texttt{configure > context \textit{context\_name} > policy \textit{accounting \_policy\_name}}

Entering the above command sequence results in the following prompt:

\texttt{[context\_name]\textit{host\_name}(config\_accounting\_policy)#}

Syntax

\texttt{operator-string \textit{string}}

\texttt{no operator-string}

\texttt{no}

Removes the operator string from this policy.

\texttt{string}

Specifies a text string that is included with accounting messages originating from this policy. \texttt{string} must be from 1 to 63 alphanumeric characters.

Usage

Use this command to create a text string to be included with accounting messages originating from this policy.

Example

The following command creates the text string \texttt{pgw\_local} to be included with accounting messages originating from this policy:

\texttt{operator-string \textit{pgw\_local}}
service-context-id

Configures the value to be sent in the Service-Context-Id AVP, which defines the context in which Rf is used.

Product
GGSN
HSGW
P-GW
S-GW
SAEGW

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > Accounting Policy Configuration

configure > context context_name > policy accounting policy_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-accounting-policy)#

Syntax

service-context-id service_context_id

default service-context-id

default

Configures this command with the default setting. Currently, the default value is encoded based on the dictionary wherever applicable; when not applicable, it is not encoded.

service_context_id

Specifies the service context as an alphanumeric string of 1 through 63 characters that can contain punctuation characters.

Usage

If Service-Context-Id is applicable and configured using this command, it will be sent in the AVP Service-Context-Id in the Rf ACR message.

Example

The following command specifies the value version@customer.com to be sent in the Service-Context-Id AVP in the Rf ACR message:

service-context-id version@customer.com
Chapter 5
ACL Configuration Mode Commands

The Access Control List Configuration Mode is used to create and manage IP-based, user access privileges.

Mode
Exec > Global Configuration > Context Configuration > ACL Configuration
`configure > context context_name > ip access-list acl_name`

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-acl)#`

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
deny/permit (by source IP address masking)

Filters subscriber sessions based on the IP address mask sent by the source to the mobile node or the network.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > ACL Configuration

configure > context context_name > ip access-list acl_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-acl)#

**Syntax**

```plaintext
{ deny | permit } [ log ] source_address source_wildcard
after { deny | permit } [ log ] source_address source_wildcard
before { deny | permit } [ log ] source_address source_wildcard
no { deny | permit } [ log ] source_address source_wildcard
```

*after*

Indicates that all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed. This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

*before*

Indicates that all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed. This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

*no*

Removes the rule which exactly matches the options specified.

*deny | permit*

Specifies the rule is either block (deny) or an allow (permit) filter.
ACL Configuration Mode Commands

deny/permit (by source IP address masking)

- **deny**: Indicates the rule, when matched, drops the corresponding packets.
- **permit**: Indicates the rule, when matched, allows the corresponding packets.

**log**
Default: packets are not logged.
Indicates all packets which match the filter are to be logged.

**Important**: The logging option is not supported for ACLs applied on SPIO or local contexts.

**source_address**
The IP address(es) from which the packet originated. IP addresses must be entered in IPv4 dotted-decimal format.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the **source_wildcard** parameter.

**source_wildcard**
This option is used in conjunction with the **source_address** option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:
- Zero-bits in this parameter mean that the corresponding bits configured for the **source_address** parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the **source_address** parameter must be ignored.

**Important**: The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.

**Usage**
Define a rule when any packet from the IP addresses which fall into the group of addresses matching the IP address masking. This allows the reduction of filtering rules as it does not require a rule for each source and destination pair.

**Important**: The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the Engineering Rules appendix in the System Administration Guide.

**Example**

The following command defines two rules with the second logging filtered packets:

```
permit 1.2.3.0 0.0.0.31
deny log 1.2.4.0 0.0.0.15
```

The following sets the insertion point before the first rule defined above:
deny/permit (by source IP address masking)

before permit 1.2.3.0 0.0.0.31

The following command sets the insertion point after the second rule defined above:

after deny log 1.2.4.0 0.0.0.15

The following deletes the first rule defined above:

no permit 1.2.3.0 0.0.0.31
deny/permit (any)

Filters subscriber sessions based on any packet received. This command is also sets the access control list insertion point.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > ACL Configuration
configure > context context_name > ip access-list acl_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-acl)#

Syntax

{ deny | permit } [ log ] any

after { deny | permit } [ log ] any

before { deny | permit } [ log ] any

no { deny | permit } [ log ] any

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

after
Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

before
Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

no
 Removes the rule which exactly matches the options specified.
deny | permit

Specifies the rule is either block (deny) or an allow (permit) filter.

- **deny**: Indicates the rule, when matched, drops the corresponding packets.
- **permit**: Indicates the rule, when matched, allows the corresponding packets.

log

Default: Packets are not logged.
Indicates all packets which match the filter are to be logged.

**Important**: The logging option is not supported for ACLs applied on SPIO or local contexts.

any

Indicates all packets will match the filter regardless of source and/or destination.

**Usage**

Define a catch all rule to place at the end of the list of rules.

**Important**: It is suggested that any rule which is added to be a catch all should also have the log option specified. The logged packets may be used to determine if the current list of rules is adequate or needs modification to ensure proper security. The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the Engineering Rules appendix in the System Administration Guide.

**Example**

The following commands define two rules with the second logging filtered packets:

```plaintext
permit any
deny log any
```

The following sets the insertion point before the first rule defined above:

```plaintext
before permit any
```

The following command sets the insertion point after the second rule defined above:

```plaintext
after deny log any
```

The following deletes the first rule defined above:

```plaintext
no permit any
```
deny/permit (by host IP address)

Filters subscriber sessions based on the targeted host IP address sent by the source to the mobile node or the network.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > ACL Configuration

```bash
configure > context context_name > ip access-list acl_name
```

Entering the above command sequence results in the following prompt:

```bash
[context_name]host_name(config-acl)#
```

**Syntax**

```bash
{ deny | permit } [ log ] host source_host_address
after { deny | permit } [ log ] host source_host_address
before { deny | permit } [ log ] host source_host_address
no { deny | permit } [ log ] host source_host_address
```

- **after**
  Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.
  This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

- **before**
  Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.
  This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

- **Important**: If the options specified do not exactly match an existing rule, the insertion point does not change.

- **no**
  Removes the rule which exactly matches the options specified.

- **deny | permit**
  Specifies the rule is either block (deny) or an allow (permit) filter.
deny/permit (by host IP address)

- **deny**: Indicates the rule, when matched, drops the corresponding packets.
- **permit**: Indicates the rule, when matched, allows the corresponding packets.

**log**

Default: Packets are not logged.
Indicates that all packets which match the filter are to be logged.

**Important**: The logging option is not supported for ACLs applied on SPI0 or local contexts.

**source_host_address**

The IP address of the source host to filter against expressed in IPv4 dotted-decimal notation.

**Usage**

Define a rule when a very specific remote host is to be blocked. In simplified networks where the access controls need only block a few hosts, this command allows the rules to be very clear and concise.

**Important**: The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*.

**Example**

The following commands define two rules with the second logging filtered packets:

- `permit host 10.2.3.4`
- `deny log host 10.2.3.5`

The following sets the insertion point before the first rule defined above:

- `before permit host 10.2.3.4`

The following command sets the insertion point after the second rule defined above:

- `after deny log host 10.2.3.5`

The following deletes the first rule defined above:

- `no permit host 10.2.3.4`
deny/permit (by source ICMP packets)

Filters subscriber sessions based on the internet control message protocol (ICMP) packets sent by the source to the mobile node or the network.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > ACL Configuration

```bash
configure > context context_name > ip access-list acl_name
```

Entering the above command sequence results in the following prompt:

```bash
[context_name]host_name(config-acl)#
```

**Syntax**

```bash
{ deny | permit } [ log ] icmp { source_address source_wildcard | any | host source_host_address } { dest_address dest_wildcard | any | host dest_host_address } [ icmp_type [ icmp_code ] ]
```

```bash
after { deny | permit } [ log ] icmp { source_address source_wildcard | any | host source_host_address } { dest_address dest_wildcard | any | host dest_host_address } [ icmp_type [ icmp_code ] ]
```

```bash
before { deny | permit } [ log ] icmp { source_address source_wildcard | any | host source_host_address } { dest_address dest_wildcard | any | host dest_host_address } [ icmp_type [ icmp_code ] ]
```

```bash
no { deny | permit } [ log ] icmp { source_address source_wildcard | any | host source_host_address } { dest_address dest_wildcard | any | host dest_host_address } [ icmp_type [ icmp_code ] ]
```

**Important:**
If the options specified do not exactly match an existing rule, the insertion point does not change.

**after**
Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

**before**
Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.
**deny/permit** (by source ICMP packets)

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

**no**
Removes the rule which exactly matches the options specified.

**deny | permit**
Specifies the rule is either block (deny) or an allow (permit) filter.
  - **deny**: Indicates the rule, when matched, drops the corresponding packets.
  - **permit**: Indicates the rule, when matched, allows the corresponding packets.

**log**
Default: packets are not logged.
Indicates all packets which match the filter are to be logged.

**Important:** The logging option is not supported for ACLs applied on SPI0 or local contexts.

**source_address**
The IP address(es) from which the packet originated. IP addresses must be entered in IPv4 dotted-decimal format.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the **source_wildcard** parameter.

**source_wildcard**
This option is used in conjunction with the **source_address** option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:
  - Zero-bits in this parameter mean that the corresponding bits configured for the **source_address** parameter must be identical.
  - One-bits in this parameter mean that the corresponding bits configured for the **source_address** parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

**any**
Specifies that the rule applies to all packets.

**host**
Specifies that the rule applies to a specific host as determined by its IP address.
### ACL Configuration Mode Commands

deny/permit (by source ICMP packets)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>source_host_address</strong></td>
<td>The IP address of the source host to filter against expressed in IPv4 dotted-decimal notation.</td>
</tr>
<tr>
<td><strong>dest_host_address</strong></td>
<td>The IP address of the destination host to filter against expressed in IPv4 dotted-decimal notation.</td>
</tr>
<tr>
<td><strong>dest_address</strong></td>
<td>The IP address(es) to which the packet is to be sent. This option is used to filter all packets to a specific IP address or a group of IP addresses. When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the <strong>dest_wildcard</strong> parameter.</td>
</tr>
</tbody>
</table>
| **dest_wildcard**  | This option is used in conjunction with the **dest_address** option to specify a group of addresses for which packets are to be filtered. The mask must be entered as a complement:  
  - Zero-bits in this parameter mean that the corresponding bits configured for the **dest_address** parameter must be identical.  
  - One-bits in this parameter mean that the corresponding bits configured for the **dest_address** parameter must be ignored.  

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>icmp_type</strong></td>
<td>Specifies that all ICMP packets of a particular type are to be filtered. The type can be an integer value between 0 and 255.</td>
</tr>
<tr>
<td><strong>icmp_code</strong></td>
<td>Specifies that all ICMP packets of a particular code are to be filtered. The type can be an integer value between 0 and 255.</td>
</tr>
</tbody>
</table>

**Usage**

Define a rule to block ICMP packets which can be used for address resolution and possible be a security risk. The IP filtering allows flexible controls for pairs of individual hosts or groups by IP masking which allows the filtering of entire subnets if necessary.

**Important:** The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the Engineering Rules appendix in the System Administration Guide.

**Example**

The following commands define two rules with the second logging filtered packets:

```
permit icmp host 10.2.3.4 any 168
```
deny log icmp 10.2.3.0 0.0.0.31 host 10.2.4.16 168 11

The following sets the insertion point before the first rule defined above:

before permit icmp host 10.2.3.4 any 168

The following command sets the insertion point after the second rule defined above:

after deny log icmp 10.2.3.0 0.0.0.31 host 10.2.4.16 168 11

The following deletes the first rule defined above:

no permit icmp host 10.2.3.4 any 168
deny/permit (by IP packets)

Filters subscriber sessions based on the internet protocol packets sent by the source to the mobile node or the network.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > ACL Configuration

```
configure > context context_name > ip access-list acl_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-acl)#
```

**Syntax**

```
{ deny | permit } [ log ] ip { ( source_address source_wildcard | any | host source_host_address ) ( dest_address dest_wildcard | any | host dest_host_address ) [ fragment ] [ protocol num ]

after { deny | permit } [ log ] ip { ( source_address source_wildcard | any | host source_host_address ) ( dest_address dest_wildcard | any | host dest_host_address ) [ fragment ] [ protocol num ]

before { deny | permit } [ log ] ip { ( source_address source_wildcard | any | host source_host_address ) ( dest_address dest_wildcard | any | host dest_host_address ) [ fragment ] [ protocol num ]

no { deny | permit } [ log ] ip { ( source_address source_wildcard | any | host source_host_address ) ( dest_address dest_wildcard | any | host dest_host_address ) [ fragment ] [ protocol num ]
```

---

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

---

**after**
Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

---

**before**
Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.
**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

<table>
<thead>
<tr>
<th><strong>no</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Removes the rule which exactly matches the options specified.</td>
</tr>
</tbody>
</table>

| **deny | permit** |
|--------|
| Specifies the rule is either block (deny) or an allow (permit) filter. |
| - **deny:** Indicates the rule, when matched, drops the corresponding packets. |
| - **permit:** Indicates the rule, when matched, allows the corresponding packets. |

<table>
<thead>
<tr>
<th><strong>log</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Default: Packets are not logged.</td>
</tr>
<tr>
<td>Indicates all packets which match the filter are to be logged.</td>
</tr>
</tbody>
</table>

**Important:** The logging option is not supported for ACLs applied on SPIO or local contexts.

<table>
<thead>
<tr>
<th><strong>source_address</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>The IP address(es) from which the packet originated.</td>
</tr>
<tr>
<td>This option is used to filter all packets from a specific IP address or a group of IP addresses.</td>
</tr>
<tr>
<td>When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the <code>source_wildcard</code> parameter.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>source_wildcard</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>This option is used in conjunction with the <code>source_address</code> option to specify a group of addresses for which packets are to be filtered.</td>
</tr>
<tr>
<td>The mask must be entered as a complement:</td>
</tr>
<tr>
<td>- Zero-bits in this parameter mean that the corresponding bits configured for the <code>source_address</code> parameter must be identical.</td>
</tr>
<tr>
<td>- One-bits in this parameter mean that the corresponding bits configured for the <code>source_address</code> parameter must be ignored.</td>
</tr>
</tbody>
</table>

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

<table>
<thead>
<tr>
<th><strong>any</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies that the rule applies to all packets.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>host</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies that the rule applies to a specific host as determined by its IP address.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>source_host_address</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>The IP address of the source host to filter against expressed in IPv4 dotted-decimal notation.</td>
</tr>
</tbody>
</table>
**ACL Configuration Mode Commands**

**deny/permit (by IP packets)**

---

**dest_host_address**

The IP address of the destination host to filter against expressed in IPv4 dotted-decimal notation.

---

**dest_address**

The IP address(es) to which the packet is to be sent.

This option is used to filter all packets to a specific IP address or a group of IP addresses. When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the **dest_wildcard** parameter.

---

**dest_wildcard**

This option is used in conjunction with the **dest_address** option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the **dest_address** parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the **dest_address** parameter must be ignored.

**Important**: The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.

---

**fragment**

Indicates packet filtering is to be applied to IP packet fragments only.

---

**protocol num**

Indicates that the packet filtering is to be applied to a specific protocol number. **num** can be an integer ranging from 0 to 255.

**Important**: This keyword is not applicable to a SPIO interface. Instead, you must specify the type of protocol packets for which you want to deny/permit processing on a SPIO. For example, **deny icmp**, **deny tcp**, or **deny udp**.

---

**Usage**

Block IP packets when the source and destination are of interest.

**Important**: The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the Engineering Rules appendix in the System Administration Guide.

---

**Example**

The following commands define two rules with the second logging filtered packets:

```
permit ip host 10.2.3.4 any fragment

deny log ip 10.2.3.0 0.0.0.31 host 10.2.4.16
```
The following sets the insertion point before the first rule defined above:

```plaintext
before permit ip host 10.2.3.4 any fragment
```

The following command sets the insertion point after the second rule defined above:

```plaintext
after deny log ip 10.2.3.0 0.0.0.31 host 10.2.4.16
```

The following deletes the first rule defined above:

```plaintext
no permit ip host 10.2.3.4 any fragment
```
deny/permit (by TCP/UDP packets)

Filters subscriber sessions based on the transmission control protocol/user datagram protocol packets sent by the source to the mobile node or the network.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > ACL Configuration
configure > context context_name > ip access-list acl_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-acl)#

Syntax

{ deny | permit } [ log ] { tcp | udp } { { source_address source_wildcard | any | host source_host_address } [ eq source_port | gt source_port | lt source_port | neq source_port ] } { { dest_address dest_wildcard | any | host dest_host_address } [ eq dest_port | gt dest_port | lt dest_port | neq dest_port | range start_port end_port ] }

after { deny | permit } [ log ] { tcp | udp } { { source_address source_wildcard | any | host source_host_address } [ eq source_port | gt source_port | lt source_port | neq source_port ] } { { dest_address dest_wildcard | any | host dest_host_address } [ eq dest_port | gt dest_port | lt dest_port | neq dest_port | range start_port end_port ] }

before { deny | permit } [ log ] { tcp | udp } { { source_address source_wildcard | any | host source_host_address } [ eq source_port | gt source_port | lt source_port | neq source_port ] } { { dest_address dest_wildcard | any | host dest_host_address } [ eq dest_port | gt dest_port | lt dest_port | neq dest_port | range start_port end_port ] }

no { deny | permit } [ log ] { tcp | udp } { { source_address source_wildcard | any | host source_host_address } [ eq source_port | gt source_port | lt source_port | neq source_port ] } { { dest_address dest_wildcard | any | host dest_host_address } [ eq dest_port | gt dest_port | lt dest_port | neq dest_port | range start_port end_port ] }

Important: If the options specified do not exactly match an existing rule, the insertion point does not change.
before
Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed. This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

no
Removes the rule which exactly matches the options specified.

deny/permit
Specifies the rule is either block (deny) or an allow (permit) filter.
- **deny**: Indicates the rule, when matched, drops the corresponding packets.
- **permit**: Indicates the rule, when matched, allows the corresponding packets.

log
Default: Packets are not logged. Indicates all packets which match the filter are to be logged.

**Important:** The logging option is not supported for ACLs applied on SPIO or local contexts.

tcp/udp
Specifies the filter is to be applied to IP based transmission control protocol or the user datagram protocol.
- **tcp**: Filter applies to TPC packets.
- **udp**: Filter applies to UDP packets.

source_address
The IP address(es) from which the packet originated. IP addresses must be entered in IPv4 dotted-decimal format. This option is used to filter all packets from a specific IP address or a group of IP addresses. When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the source wildcard parameter.

source wildcard
This option is used in conjunction with the source_address option to specify a group of addresses for which packets are to be filtered. The mask must be entered as a complement:
- Zero-bits in this parameter mean that the corresponding bits configured for the source_address parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the source_address parameter must be ignored.
**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

<table>
<thead>
<tr>
<th>any</th>
<th>Specifies that the rule applies to all packets.</th>
</tr>
</thead>
<tbody>
<tr>
<td>host</td>
<td>Specifies that the rule applies to a specific host as determined by its IP address.</td>
</tr>
<tr>
<td>source_host_address</td>
<td>The IP address of the source host to filter against expressed in IPv4 dotted-decimal notation.</td>
</tr>
<tr>
<td>dest_host_address</td>
<td>The IP address of the destination host to filter against expressed in IPv4 dotted-decimal notation.</td>
</tr>
<tr>
<td>eq source_port</td>
<td>Specifies a single, specific source TCP port number to be filtered. source_port must be an integer from 0 through 65535.</td>
</tr>
<tr>
<td>gt source_port</td>
<td>Specifies that all source TCP port numbers greater than the one specified are to be filtered. source_port must be an integer from 0 through 65535.</td>
</tr>
<tr>
<td>lt source_port</td>
<td>Specifies that all source TCP port numbers less than the one specified are to be filtered. source_port must be an integer from 0 through 65535.</td>
</tr>
<tr>
<td>neq source_port</td>
<td>Specifies that all source TCP port numbers not equal to the one specified are to be filtered. source_port must be an integer from 0 through 65535.</td>
</tr>
<tr>
<td>dest_address</td>
<td>The IP address(es) to which the packet is to be sent. This option is used to filter all packets to a specific IP address or a group of IP addresses. When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the dest_wildcard parameter.</td>
</tr>
<tr>
<td>dest_wildcard</td>
<td>This option is used in conjunction with the dest_address option to specify a group of addresses for which packets are to be filtered. The mask must be entered as a complement:</td>
</tr>
<tr>
<td></td>
<td>• Zero-bits in this parameter mean that the corresponding bits configured for the dest_address parameter must be identical.</td>
</tr>
</tbody>
</table>
ACL Configuration Mode Commands

- One-bits in this parameter mean that the corresponding bits configured for the dest_address parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.

---

eq dest_port

Specifies a single, specific destination TCP port number to be filtered. dest_port must be an integer from 0 through 65535.

---

gt dest_port

Specifies that all destination TCP port numbers greater than the one specified are to be filtered. dest_port must be an integer from 0 through 65535.

---

lt dest_port

Specifies that all destination TCP port numbers less than the one specified are to be filtered. dest_port must be an integer from 0 through 65535.

---

neq dest_port

Specifies that all destination TCP port numbers not equal to the one specified are to be filtered. dest_port must be an integer from 0 through 65535.

---

range start_port end_port

Specifies a range of ports to be matched. start_port must be an integer from 0 through 65535, and must be less than the end_port value. end_port must be an integer from 0 through 65535, and must be greater than the start_port value.

**Important:** This option is supported in PDIF Release 8.3.

---

Usage

Block IP packets when the source and destination are of interest but for only a limited set of ports.

**Important:** The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the Engineering Rules appendix in the System Administration Guide.

---

Example

The following commands define four rules with the second and fourth rules logging filtered packets:

```plaintext
permit tcp host 10.2.3.4 any
deny log udp 10.2.3.0 0.0.0.31 host 10.2.4.16
permit tcp host 10.2.3.64 gt 1023 any
deny log udp 10.2.3.0 0.0.0.31 10.2.4.127 0.0.0.127
```
The following sets the insertion point before the first rule defined above:

```
before permit tcp host 10.2.3.4 any
```

The following command sets the insertion point after the second rule defined above:

```
after deny log udp 10.2.3.0 0.0.0.31 host 10.2.4.16
```

The following deletes the third rule defined above:

```
no permit tcp host 10.2.3.64 gt 1023 any
```
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**
Use this command to return to the parent configuration mode.
**readdress server**

Alters the destination address and port number in TCP or UDP packet headers to redirect packets to a different server.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > ACL Configuration

```
configure > context context_name > ip access-list acl_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-acl)#
```

**Syntax**

```
readdress server redirect_address [ port port_no ] { tcp | udp } { { source_address source_wildcard | any | host source_host_address } [ eq source_port | gt source_port | lt source_port | neq source_port ] } { { dest_address dest_wildcard | any | host dest_host_address } [ eq ] dest_port | gt dest_port | lt dest_port | neq dest_port ] }

after readdress server redirect_address [ port port_no ] { tcp | udp } { { source_address source_wildcard | any | host source_host_address } [ eq source_port | gt source_port | lt source_port | neq source_port ] } { { dest_address dest_wildcard | any | host dest_host_address } [ eq ] dest_port | gt dest_port | lt dest_port | neq dest_port ] }

before readdress server redirect_address [ port port_no ] { tcp | udp } { { source_address source_wildcard | any | host source_host_address } [ eq source_port | gt source_port | lt source_port | neq source_port ] } { { dest_address dest_wildcard | any | host dest_host_address } [ eq ] dest_port | gt dest_port | lt dest_port | neq dest_port ] }

no readdress server redirect_address [ port port_no ] { tcp | udp } { { source_address source_wildcard | any | host source_host_address } [ eq source_port | gt source_port | lt source_port | neq source_port ] } { { dest_address dest_wildcard | any | host dest_host_address } [ eq ] dest_port | gt dest_port | lt dest_port | neq dest_port ] }
```

**after**
Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

---

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.
before
Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

no
Removes the rule which exactly matches the options specified.

redirect_address
The IP address to which the IP packets are redirected. TCP or UDP packet headers are rewritten to contain the new destination address. This must be an IPv4 address specified in dotted-decimal notation.

port  port_no
The number of the port at the redirect address where the packets are sent. TCP or UDP packet headers are rewritten to contain the new destination port number.

tcp | udp
Specifies the redirect is to be applied to the IP based transmission control protocol or the user datagram protocol.
  - tcp: Redirect applies to TCP packets.
  - udp: Redirect applies to UDP packets.

source_address
The IP address(es) from which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the source_wildcard parameter.

source_wildcard
This option is used in conjunction with the source_address option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:
  - Zero-bits in this parameter mean that the corresponding bits configured for the source_address parameter must be identical.
  - One-bits in this parameter mean that the corresponding bits configured for the source_address parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.
any
Specifies that the rule applies to all packets.

host
Specifies that the rule applies to a specific host as determined by its IP address.

source_host_address
The IP address of the source host to filter against expressed in IPv4 dotted-decimal notation.

dest_host_address
The IP address of the destination host to filter against expressed in IPv4 dotted-decimal notation.

eq source_port
Specifies a single, specific source TCP port number to be filtered.
source_port must be an integer from 0 through 65535.

gt source_port
Specifies that all source TCP port numbers greater than the one specified are to be filtered.
source_port must be an integer from 0 through 65535.

lt source_port
Specifies that all source TCP port numbers less than the one specified are to be filtered.
source_port must be an integer from 0 through 65535.

neq source_port
Specifies that all source TCP port numbers not equal to the one specified are to be filtered.
source_port must be an integer from 0 through 65535.

dest_address
The IP address(es) to which the packet is to be sent.
This option is used to filter all packets to a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the dest_wildcard parameter.

dest_wildcard
This option is used in conjunction with the dest_address option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:
  • Zero-bits in this parameter mean that the corresponding bits configured for the dest_address parameter must be identical.
  • One-bits in this parameter mean that the corresponding bits configured for the dest_address parameter must be ignored.
**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

- **eq dest_port**
  Specifies a single, specific destination TCP port number to be filtered.
  *dest_port* must be an integer from 0 through 65535.

- **gt dest_port**
  Specifies that all destination TCP port numbers greater than the one specified are to be filtered.
  *dest_port* must be an integer from 0 through 65535.

- **lt dest_port**
  Specifies that all destination TCP port numbers less than the one specified are to be filtered.
  *dest_port* must be an integer 0 through 65535.

- **neq dest_port**
  Specifies that all destination TCP port numbers not equal to the one specified are to be filtered.
  *dest_port* must be an integer 0 through 65535.

**Usage**

Use this command to define a rule that redirects packets to a different destination address. The TCP and UDP packet headers are modified with the new destination address and destination port.

**Important:** The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*.

**Important:** Prior to Release 8.3, for packets received from the packet data network destined for a subscriber's UE, the system applied logic to reset the source address of a packet to the original destination address of the input packet before applying the outbound access control list (ACL). In Release 8.3 and higher, the system reverses the order and applies the outbound ACL before resetting the source address. This change impacts all current readdress server rules in inbound IPv4 ACLs.

**Important:** After Release 8.3, for every readdress server rule in an inbound IPv4 ACL, you must add a permit rule to an outbound ACL that explicitly permits packets from the readdress rule's redirect address and port number. If the permit rule is omitted, the system will reject all packets destined for the subscriber’s UE from the readdress rule's redirect address and port number.

**Example**

The following command defines a rule that redirects packets to the server at 192.168.10.4, UDP packets coming from any host with a destination of any host are matched:

```
readdress server 192.168.10.4 udp any any
```

The following sets the insertion point before the rule defined above:
before readdress server 192.168.10.4 udp any any

The following command sets the insertion point after the first rule defined above:

after readdress server 192.168.10.4 udp any any

The following deletes the rule defined above:

no readdress server 192.168.10.4 udp any any
redirect context (by IP address masking)

Redirects subscriber sessions based on the IP address mask sent by the source to the mobile node or the network.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > ACL Configuration

configure > context context_name > ip access-list acl_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-acl)#

Syntax

redirect context context_id [ log ] source_address source_wildcard
after redirect context context_id [ log ] source_address source_wildcard
before redirect context context_id [ log ] source_address source_wildcard
no redirect context context_id [ log ] source_address source_wildcard

after
Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed. This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

Important: If the options specified do not exactly match an existing rule, the insertion point does not change.

before
Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed. This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

Important: If the options specified do not exactly match an existing rule, the insertion point does not change.

no
Removes the rule which exactly matches the options specified.
**context context_id**

The context identification number of the context to which packets are redirected. At the executive mode prompt, use the `show context all` command to display context names and context IDs.

**log**

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

**source_address**

The IP address(es) from which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the `source_wildcard` parameter.

**source_wildcard**

This option is used in conjunction with the `source_address` option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:
- Zero-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.

**Usage**

Define a rule when any packet from the IP addresses which fall into the group of addresses matching the IP address masking. This allows the reduction of redirect rules as it does not require a rule for each source and destination pair.

**Important:** The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the Engineering Rules appendix in the System Administration Guide.

**Important:** Also note that “redirect” rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

**Example**

The following command defines a rule that redirects packets to the context with the context ID of 23 and the source IP and wildcard of 192.168.22.0 and 0.0.0.31:

```
redirect context 23 198.162.22.0 0.0.0.31
```

The following sets the insertion point before the rule defined above:
before redirect context 23 198.162.22.0 0.0.0.31

The following command sets the insertion point after the first rule defined above:

after redirect context 23 198.162.22.0 0.0.0.31

The following deletes the first rule defined above:

no redirect context 23 198.162.22.0 0.0.0.31
redirect context (any)

Redirects subscriber sessions based on any packet received. This command is also used to set the access control list insertion point.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > ACL Configuration

```
configure > context context_name > ip access-list acl_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-acl)#
```

**Syntax**

```
redirect context context_id [ log ] any
after redirect context context_id [ log ] any
before redirect context context_id [ log ] any
no redirect context context_id [ log ] any
```

**after**
Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed. This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

**before**
Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed. This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

**no**
Removes the rule which exactly matches the options specified.
**context context_id**

The context identification number of the context to which packets are redirected. At the executive mode prompt, use the `show context all` command to display context names and context IDs.

**log**

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

**any**

Indicates all packets will match the redirect regardless of source and/or destination.

---

**Usage**

Define a catch all rule to place at the end of the list of rules to provide explicit handling of rules which do not fit any other criteria.

---

**Important:** Any rule which is added as a catch all should also have the log option specified. The logged packets may be used to determine if the current list of rules is adequate or needs modification to ensure proper security.

**Important:** The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the Engineering Rules appendix in the System Administration Guide.

**Important:** Also note that “redirect” rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

---

**Example**

The following command defines a rule that redirects packets to the context with the context ID of 23 and any source IP:

```
redirect context 23 any
```

The following sets the insertion point before the rule defined above:

```
before redirect context 23 any
```

The following command sets the insertion point after the first rule defined above:

```
after redirect context 23 any
```

The following deletes the first rule defined above:

```
no redirect context 23 any
```
redirect context (by host IP address)

Redirects subscriber sessions based on the targeted host IP address sent by the source to the mobile node or the network.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > ACL Configuration

configure > context context_name > ip access-list acl_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-acl)#

Syntax

redirect context context_id [ log ] host source_ipv4_address
after redirect context context_id [ log ] host source_ipv4_address
before redirect context context_id [ log ] host source_ipv4_address
no redirect context context_id [ log ] host source_ipv4_address

after
Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

Important: If the options specified do not exactly match an existing rule, the insertion point does not change.

before
Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

Important: If the options specified do not exactly match an existing rule, the insertion point does not change.

no
Removes the rule which exactly matches the options specified.
redirect context (by host IP address)

**context context_id**

The context identification number of the context to which packets are redirected. At the executive mode prompt, use the `show context all` command to display context names and context IDs.

**log**

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

**host**

Specifies that the rule applies to a specific host as determined by its IP address.

**source_ipv4_address**

The IP address of the source host to filter against expressed in IPv4 dotted-decimal notation.

**Usage**

Define a rule when a very specific remote host is to be blocked. In simplified networks where the access controls need only block a few hosts, this command allows the rules to be very clear and concise.

**Important:** The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the Engineering Rules appendix in the System Administration Guide.

**Important:** Also note that “redirect” rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

**Example**

The following command defines a rule that redirects packets to the context with the context ID of 23 and a host IP address of 192.168.200.11:

```
redirect context 23 host 192.168.200.11
```

The following sets the insertion point before the rule defined above:

```
before redirect context 23 host 192.168.200.11
```

The following command sets the insertion point after first the rule defined above:

```
after redirect context 23 host 192.168.200.11
```

The following deletes the first rule defined above:

```
no redirect context 23 host 192.168.200.11
```
redirect context (by source ICMP packets)

Redirects subscriber sessions based on the internet control message protocol packets sent by the source to the mobile node or the network.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > ACL Configuration
configure > context context_name > ip access-list acl_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-acl)#
```

**Syntax**

```
redirect context context_id [ log ] icmp { source_address source_wildcard | any | host source_host_address } { dest_address dest_wildcard | any | host dest_host_address } [ icmp_type [ icmp_code ] ]
```

```
before redirect context context_id [ log ] icmp { source_address source_wildcard | any | host source_host_address } { dest_address dest_wildcard | any | host dest_host_address } [ icmp_type [ icmp_code ] ]
```

```
o redirect context context_id [ log ] icmp { source_address source_wildcard | any | host source_host_address } { dest_address dest_wildcard | any | host dest_host_address } [ icmp_type [ icmp_code ] ]
```

```
after
```

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

---

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

```
before
```

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.
**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

**no**
Removes the rule which exactly matches the options specified.

**context context_id**
The context identification number of the context to which packets are redirected. At the executive mode prompt, use the `show context all` command to display context names and context IDs.

**log**
Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

**source_address**
The IP address(es) from which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the `source_wildcard` parameter.

**source_wildcard**
This option is used in conjunction with the `source_address` option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:
- Zero-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.

**any**
Specifies that the rule applies to all packets.

**host**
Specifies that the rule applies to a specific host as determined by its IP address.

**source_host_address**
The IP address of the source host to filter against expressed in IPv4 dotted-decimal notation.

**dest_host_address**
The IP address of the destination host to filter against expressed in IPv4 dotted-decimal notation.
**redirect context (by source ICMP packets)**

```
dest_address
```

The IP address(es) to which the packet is to be sent.

This option is used to filter all packets to a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the `dest_wildcard` parameter.

```
dest_wildcard
```

This option is used in conjunction with the `dest_address` option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the `dest_address` parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the `dest_address` parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.

```
icmp_type
```

Specifies that all ICMP packets of a particular type are to be filtered. The type can be an integer value between 0 and 255.

```
icmp_code
```

Specifies that all ICMP packets of a particular code are to be filtered. The type can be an integer value between 0 and 255.

**Usage**

Define a rule to block ICMP packets which can be used for address resolution and possibly be a security risk.

The IP redirecting allows flexible controls for pairs of individual hosts or groups by IP masking which allows the redirecting of entire subnets if necessary.

**Important:** The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*.

**Important:** Also note that “redirect” rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

**Example**

The following command defines a rule that redirects packets to the context with the context ID of 23, and ICMP packets coming from the host with the IP address 198.162.100.25:

```
redirect context 23 icmp host 192.168.100.25
```

The following sets the insertion point before the rule defined above:
before redirect context 23 icmp host 192.168.100.25

The following command sets the insertion point after the first rule defined above:

after redirect context 23 icmp host 192.168.100.25

The following deletes the first rule defined above:

no redirect context 23 icmp host 192.168.100.25
redirect context (by IP packets)

Redirects subscriber sessions based on the internet protocol packets sent by the source to the mobile node or the network.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > ACL Configuration

configure > context context_name > ip access-list acl_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-acl)#

Syntax

redirect context context_id [ log ] ip { source_address source_wildcard | any | host source_host_address } { dest_address dest_wildcard | any | host dest_host_address } [ fragment ] [ protocol num ]

after redirect context context_id [ log ] ip { source_address source_wildcard | any | host source_host_address } { dest_address dest_wildcard | any | host dest_host_address } [ fragment ] [ protocol num ]

before redirect context context_id [ log ] ip { source_address source_wildcard | any | host source_host_address } { dest_address dest_wildcard | any | host dest_host_address } [ fragment ] [ protocol num ]

no redirect context context_id [ log ] ip { source_address source_wildcard | any | host source_host_address } { dest_address dest_wildcard | any | host dest_host_address } [ fragment ] [ protocol num ]

after

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

Important: If the options specified do not exactly match an existing rule, the insertion point does not change.

before

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.
**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

```markdown
no
```

Removes the rule which exactly matches the options specified.

```markdown
context context_id
```

The context identification number of the context to which packets are redirected. At the executive mode prompt, use the `show context all` command to display context names and context IDs.

```markdown
log
```

Default: packets are not logged. Indicates all packets which match the redirect are to be logged.

```markdown
source_address
```

The IP address(es) from which the packet originated. This option is used to filter all packets from a specific IP address or a group of IP addresses. When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the `sourceWildcard` parameter.

```markdown
sourceWildcard
```

This option is used in conjunction with the `source_address` option to specify a group of addresses for which packets are to be filtered. The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.

```markdown
any
```

Specifies that the rule applies to all packets.

```markdown
host
```

Specifies that the rule applies to a specific host as determined by its IP address.

```markdown
source_host_address
```

The IP address of the source host to filter against expressed in IPv4 dotted-decimal notation.

```markdown
dest_host_address
```

The IP address of the destination host to filter against expressed in IPv4 dotted-decimal notation.
**dest_address**

The IP address(es) to which the packet is to be sent. This option is used to filter all packets to a specific IP address or a group of IP addresses. When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the `dest_wildcard` parameter.

**dest_wildcard**

This option is used in conjunction with the `dest_address` option to specify a group of addresses for which packets are to be filtered. The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the `dest_address` parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the `dest_address` parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

**fragment**

Indicates packet redirection is to be applied to IP packet fragments only.

**protocol num**

Indicates that the packet filtering is to be applied to a specific protocol number. `num` can be an integer ranging from 0 to 255.

**Usage**

Block IP packets when the source and destination are of interest.

**Important:** The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*.

**Important:** Also note that “redirect” rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

**Example**

The following command defines a rule that redirects packets to the context with the context ID of 23, and IP packets coming from the host with the IP address 198.162.100.25, and fragmented packets for any destination are matched:

```
redirect context 23 ip host 198.162.100.25 any fragment
```

The following sets the insertion point before the rule defined above:

```
before redirect context 23 ip host 198.162.100.25 any fragment
```
The following command sets the insertion point after the first rule defined above:

```
after redirect context 23 ip host 198.162.100.25 any fragment
```

The following deletes the first rule defined above:

```
no redirect context 23 ip host 198.162.100.25 any fragment
```
redirect context (by TCP/UDP packets)

Redirects subscriber sessions based on the transmission control protocol/user datagram protocol packets sent by the source to the mobile node or the network.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > ACL Configuration

```
configure > context context_name > ip access-list acl_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-acl)#
```

**Syntax**

```
redirect context context_id [ log ] { tcp | udp } { { source_address source_wildcard | any | host source_host_address } [ eq source_port | gt source_port | lt source_port | neq source_port ] } { { dest_address dest_wildcard | any | host dest_host_address } [ eq dest_port | gt dest_port | lt dest_port | neq dest_port ] }

after redirect context context_id [ log ] { tcp | udp } { { source_address source_wildcard | any | host source_host_address } [ eq source_port | gt source_port | lt source_port | neq source_port ] } { { dest_address dest_wildcard | any | host dest_host_address } [ eq dest_port | gt dest_port | lt dest_port | neq dest_port ] }

before redirect context context_id [ log ] { tcp | udp } { { source_address source_wildcard | any | host source_host_address } [ eq source_port | gt source_port | lt source_port | neq source_port ] } { { dest_address dest_wildcard | any | host dest_host_address } [ eq dest_port | gt dest_port | lt dest_port | neq dest_port ] }

no redirect context context_id [ log ] { tcp | udp } { { source_address source_wildcard | any | host source_host_address } [ eq source_port | gt source_port | lt source_port | neq source_port ] } { { dest_address dest_wildcard | any | host dest_host_address } [ eq dest_port | gt dest_port | lt dest_port | neq dest_port ] }
```

**after**
Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.
before
Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed. This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

Important: If the options specified do not exactly match an existing rule, the insertion point does not change.

no
Removes the rule which exactly matches the options specified.

custom context_id
The context identification number of the context to which packets are redirected. At the executive mode prompt, use the show context all command to display context names and context IDs.

log
Default: packets are not logged. Indicates all packets which match the redirect are to be logged.

tcp | udp
Specifies the redirect is to be applied to IP based transmission control protocol or the user datagram protocol.
  • tcp: Redirect applies to TPC packets.
  • udp: Redirect applies to UDP packets.

source_address
The IP address(es) from which the packet originated. This option is used to filter all packets from a specific IP address or a group of IP addresses. When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the source wildcard parameter.

source wildcard
This option is used in conjunction with the source_address option to specify a group of addresses for which packets are to be filtered. The mask must be entered as a complement:
  • Zero-bits in this parameter mean that the corresponding bits configured for the source_address parameter must be identical.
  • One-bits in this parameter mean that the corresponding bits configured for the source_address parameter must be ignored.

Important: The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.

any
Specifies that the rule applies to all packets.
**host**
Specifies that the rule applies to a specific host as determined by its IP address.

**source_host_address**
The IP address of the source host to filter against expressed in IPv4 dotted-decimal notation.

**dest_host_address**
The IP address of the destination host to filter against expressed in IPv4 dotted-decimal notation.

**eq source_port**
Specifies a single, specific source TCP port number to be filtered.
*source_port* must be configured to an integer value from 0 to 65535.

**gt source_port**
Specifies that all source TCP port numbers greater than the one specified are to be filtered.
*source_port* must be an integer from 0 through 65535.

**lt source_port**
Specifies that all source TCP port numbers less than the one specified are to be filtered.
*source_port* must be an integer from 0 through 65535.

**neq source_port**
Specifies that all source TCP port numbers not equal to the one specified are to be filtered.
*source_port* must be an integer from 0 through 65535.

**dest_address**
The IP address(es) to which the packet is to be sent.
This option is used to filter all packets to a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the *dest_wildcard* parameter.

**dest_wildcard**
This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:
- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.
eq dest_port
Specifies a single, specific destination TCP port number to be filtered. 
dest_port must be an integer from 0 through 65535.

gt dest_port
Specifies that all destination TCP port numbers greater than the one specified are to be filtered. 
dest_port must be an integer from 0 through 65535.

lt dest_port
Specifies that all destination TCP port numbers less than the one specified are to be filtered. 
dest_port must be an integer from 0 through 65535.

neq dest_port
Specifies that all destination TCP port numbers not equal to the one specified are to be filtered. 
dest_port must be an integer from 0 through 65535.

Usage
Block IP packets when the source and destination are of interest but for only a limited set of ports.

**Important:** The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the Engineering Rules appendix in the System Administration Guide.

**Important:** Also note that “redirect” rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example
The following command defines a rule that redirects packets to the context with the context ID of 23, and UDP packets coming from any host are matched:

    redirect context 23 udp any

The following sets the insertion point before the rule defined above:

    before redirect context 23 udp any

The following command sets the insertion point after the first rule defined above:

    after redirect context 23 udp any

The following deletes the rule defined above:

    no redirect context 23 udp any
redirect css delivery-sequence

This is a restricted command. In 9.0 and later releases, this command is obsoleted.
redirect css service (any)

Redirects subscriber sessions based on any packet received (Content Service Steering). This command is also used to set the access control list insertion point.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > ACL Configuration

configure > context context_name > ip access-list acl_name

Entering the above command sequence results in the following prompt:

\[context_name]host_name(config-acl)#

**Syntax**

redirect css service service_name [ log ] any
after redirect css service service_name [ log ] any
before redirect css service service_name [ log ] any
no redirect css service service_name [ log ] any

**after**
Indicates all rule definitions defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

**before**
Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule definitions which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

**no**
Removes the rule definition which exactly matches the options specified.
**css service service_name**

The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the `show active-charging all` command to display the names of all configured charging services. `service_name` must be an alphanumeric string from 1 through 15 characters.

**log**

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

**any**

Indicates all packets will match the redirect regardless of source and/or destination.

**Usage**

Define a catch all rule definitions to place at the end of the list of rule definitions to provide explicit handling of rule definitions which do not fit any other criteria.

**Important:** Any rule definition which is added to be a catch all should also have the `log` option specified. The logged packets may be used to determine if the current list of rule definitions is adequate or needs modification to ensure proper security.

**Important:** The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*.

**Important:** Also note that “redirect” rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

**Example**

The following command defines a rule definition that redirects packets to the charging service with the name `chgsvc1` and any source IP:

```
redirect css service chgsvc1 any
```

The following sets the insertion point before the rule definition above:

```
before redirect service chgsvc1 any
```

The following command sets the insertion point after the first rule definitions above:

```
after redirect service chgsvc1 any
```

The following deletes the first rule definition above:

```
no redirect service chgsvc1 any
```
redirect css service (by host IP address)

Redirect subscriber sessions based on the targeted host IP address sent by the source to the mobile node or the network (Content Service Steering).

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > ACL Configuration

`configure > context context_name > ip access-list acl_name`

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-acl)#`

**Syntax**

```
redirect css service service_name [ log ] host source_host_address
after redirect css service service_name [ log ] host source_host_address
before redirect css service service_name [ log ] host source_host_address
no redirect css service service_name [ log ] host source_host_address
```

**after**

Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

**before**

Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

**no**

Removes the rule definition which exactly matches the options specified.
**css service service_name**

The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the `show active-charging service all` command to display the names of all configured charging services. 

`service_name` must be an alphanumeric string from 1 through 15 characters.

**log**

Default: packets are not logged. Indicates all packets which match the redirect are to be logged.

**host**

Specifies that the rule definition applies to a specific host as determined by its IP address.

`source_host_address`

The IP address of the source host to filter against expressed in IPv4 dotted-decimal notation.

**Usage**

Define a rule definition when a very specific remote host is to be blocked. In simplified networks where the access controls need only block a few hosts, this command allows the rule definitions to be very clear and concise.

**Important:** The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the Engineering Rules appendix in the System Administration Guide.

**Important:** Also note that “redirect” rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

**Example**

The following command defines a rule definition that redirects packets to the charging service with the name `chgsvc1` and a host IP address of `192.168.200.11`:

```
redirect css service chgsvc1 host 192.168.200.11
```

The following sets the insertion point before the rule definition above:

```
before redirect css service chgsvc1 host 192.168.200.11
```

The following command sets the insertion point after the first rule definition above:

```
after redirect css service chgsvc1 host 192.168.200.11
```

The following deletes the first rule definition above:

```
no redirect css service chgsvc1 host 192.168.200.11
```
redirect css service (by ICMP packets)

Redirects subscriber sessions based on the internet control message protocol packets sent by the source to the mobile node or the network (Content Service Steering).

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > ACL Configuration
configure > context context_name > ip access-list acl_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-acl)#

**Syntax**

redirect css service service_name [ log ] icmp { any | host source_host_address | source_address source_wildcard } { any | host dest_host_address | dest_address dest_wildcard } [ icmp_type [ icmp_code ]]

before redirect css service service_name [ log ] icmp { any | host source_host_address | source_address source_wildcard } { any | host dest_host_address | dest_address dest_wildcard } [ icmp_type [ icmp_code ]]

after redirect css service service_name [ log ] icmp { any | host source_host_address | source_address source_wildcard } { any | host dest_host_address | dest_address dest_wildcard } [ icmp_type [ icmp_code ]]

no redirect css service service_name [ log ] icmp { any | host source_host_address | source_address source_wildcard } { any | host dest_host_address | dest_address dest_wildcard } [ icmp_type [ icmp_code ]]

**Important:**

If the options specified do not exactly match an existing rule definition, the insertion point does not change.

**before**

Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

**after**

Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.
### Important: If the options specified do not exactly match an existing rule definition, the insertion point does not change.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Removes the rule definition which exactly matches the options specified.</td>
</tr>
<tr>
<td>css service service_name</td>
<td>The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the <code>show active-charging service all</code> command to display the names of all configured charging services. <code>service_name</code> must be an alphanumeric string from 1 through 15 characters.</td>
</tr>
<tr>
<td>log</td>
<td>Default: packets are not logged. Indicates all packets which match the redirect are to be logged.</td>
</tr>
<tr>
<td>source_address</td>
<td>The IP address(es) from which the packet originated. This option is used to filter all packets from a specific IP address or a group of IP addresses. When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the <code>source_wildcard</code> parameter.</td>
</tr>
</tbody>
</table>
| source_wildcard          | This option is used in conjunction with the `source_address` option to specify a group of addresses for which packets are to be filtered. The mask must be entered as a complement:  
  - Zero-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be identical.  
  - One-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be ignored.  

#### Important: The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous. |
| any                      | Specifies that the rule definition applies to all packets.                   |
| host                     | Specifies that the rule definition applies to a specific host as determined by its IP address. |
| source_host_address      | The IP address of the source host to filter against expressed in IPv4 dotted-decimal notation. |
**destination host address**

The IP address of the destination host to filter against expressed in IPv4 dotted-decimal notation.

**destination address**

The IP address(es) to which the packet is to be sent.

This option is used to filter all packets to a specific IP address or a group of IP addresses.

When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the `dest_wildcard` parameter.

**destination wildcard**

This option is used in conjunction with the `destination address` option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the `destination address` parameter must be identical.

- One-bits in this parameter mean that the corresponding bits configured for the `destination address` parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

**icmp type**

Specifies that all ICMP packets of a particular type are to be filtered. The type can be an integer value between 0 and 255.

**icmp code**

Specifies that all ICMP packets of a particular code are to be filtered. The type can be an integer value between 0 and 255.

**Usage**

Define a rule definition to block ICMP packets which can be used for address resolution and possibly be a security risk.

The IP redirecting allows flexible controls for pairs of individual hosts or groups by IP masking which allows the redirecting of entire subnets if necessary.

**Important:** The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the Engineering Rules appendix in the System Administration Guide.

**Important:** Also note that “redirect” rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

**Example**

The following command defines a rule definition that redirects packets to the charging service named chgsvcl, and ICMP packets coming from the host with the IP address 198.162.100.25:
redirect css service chgsvcl icmp host 192.168.200.11

The following sets the insertion point before the rule definition above:

before redirect css service chgsvcl icmp host 192.168.200.11

The following command sets the insertion point after the first rule definition above:

after redirect css service chgsvcl icmp host 192.168.200.11

The following deletes the first rule definition above:

no redirect css service chgsvcl icmp host 192.168.200.11
redirect css service (by IP packets)

Redirects subscriber sessions based on the internet protocol packets sent by the source to the mobile node or the network (Content Service Steering).

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > ACL Configuration

```
configure > context context_name > ip access-list acl_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-acl)#
```

**Syntax**

```
redirect css service service_name [ log ] ip { any | host source_host_address | source_address source_wildcard } { any | host dest_host_address | dest_address dest_wildcard } [ fragment ]
```

```
after redirect css service service_name [ log ] ip { any | host source_host_address | source_address source_wildcard } { any | host dest_host_address | dest_address dest_wildcard } [ fragment ]
```

```
before redirect css service service_name [ log ] ip { any | host source_host_address | source_address source_wildcard } { any | host dest_host_address | dest_address dest_wildcard } [ fragment ]
```

```
no redirect css service service_name [ log ] ip { any | host source_host_address | source_address source_wildcard } { any | host dest_host_address | dest_address dest_wildcard } [ fragment ]
```

**Important:**
- After
  Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.
  This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

- **Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

- Before
  Indicates all rule definitions defined subsequent to this command are to be inserted before the command identified by the exact options listed.
  This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.
**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

**no**
Removes the rule definition that exactly matches the options specified.

**css service service_name**
The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the `show active-charging service all` command to display the names of all configured charging services.

`service_name` must be an alphanumeric string from 1 through 15 characters.

**log**
Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

**source_address**
The IP address(es) from which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the `source_wildcard` parameter.

**source_wildcard**
This option is used in conjunction with the `source_address` option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:
- Zero-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

**any**
Specifies that the rule definition applies to all packets.

**host**
Specifies that the rule definition applies to a specific host as determined by its IP address.

**source_host_address**
The IP address of the source host to filter against expressed in IPv4 dotted-decimal notation.
**dest_host_address**
The IP address of the destination host to filter against expressed in IPv4 dotted-decimal notation.

**dest_address**
The IP address(es) to which the packet is to be sent.
This option is used to filter all packets to a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the **dest_wildcard** parameter.

**dest_wildcard**
This option is used in conjunction with the **dest_address** option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:
- Zero-bits in this parameter mean that the corresponding bits configured for the **dest_address** parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the **dest_address** parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

**fragment**
Indicates packet redirection is to be applied to IP packet fragments only.

**Usage**
Block IP packets when the source and destination are of interest.

**Important:** The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*.

**Important:** Also note that “redirect” rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

**Example**
The following command defines a rule definition that redirects packets to the charging service named *chgsvc1*, and IP packets coming from the host with the IP address 198.162.100.25, and fragmented packets for any destination are matched:

```
redirect css service chgsvc1 ip host 192.168.100.25 any fragment
```

The following sets the insertion point before the rule definition above:

```
before redirect css service chgsvc1 ip host 192.168.100.25 any fragment
```

The following command sets the insertion point after the first rule definition above:
after redirect css service chgsvcl ip host 192.168.100.25 any fragment

The following deletes the first rule definition above:

no redirect css service chgsvcl ip host 192.168.100.25 any fragment
redirect css service (by source IP address masking)

Redirects subscriber sessions based on the IP address mask sent by the source to the mobile node or the network (Content Service Steering).

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > ACL Configuration

configure > context context_name > ip access-list acl_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-acl)#

Syntax

redirect css service service_name [ log ] source_address source_wildcard

after redirect css service service_name [ log ] source_address source_wildcard

before redirect css service service_name [ log ] source_address source_wildcard

no redirect css service service_name [ log ] source_address source_wildcard

after

Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

Important: If the options specified do not exactly match an existing rule definition, the insertion point does not change.

before

Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

Important: If the options specified do not exactly match an existing rule definition, the insertion point does not change.

no

Removes the rule definition which exactly matches the options specified.
**css service service_name**

The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the `show active-charging service all` command to display the names of all configured charging services. `service_name` must be an alphanumeric string from 1 through 15 characters.

**log**

Default: packets are not logged.
Indicates all packets which match the filter are to be logged.

**source_address**

The IP address(es) from which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the `source_wildcard` parameter.

**source_wildcard**

This option is used in conjunction with the `source_address` option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:
- Zero-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.

**Usage**

Define a rule definition when any packet from the IP addresses which fall into the group of addresses matching the IP address masking. This allows the reduction of filtering rule definitions as it does not require a rule definition for each source and destination pair.

**Important:** The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the Engineering Rules appendix in the System Administration Guide.

**Example**

The following command defines a rule definition to redirect packets to a charging service named `chgsvc1`:

```
redirect css service chgsvc1 10.2.3.0 0.0.0.31
```
redirect css service (by TCP/UDP packets)

Redirects subscriber sessions based on the transmission control protocol/user datagram protocol packets sent by the source to the mobile node or the network (Content Service Steering).

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > ACL Configuration

```
configure > context context_name > ip access-list acl_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-acl)#
```

**Syntax**

```
redirect css service service_name [ log ] { tcp | udp } { { source_address source_wildcard | any | host source_host_address } [ eq source_port | gt source_port | lt source_port | neq source_port | range start_source_port end_source_port ] } { { dest_address dest_wildcard | any | host dest_host_address } [ eq dest_port | gt dest_port | lt dest_port | neq dest_port | range start_dest_port end_dest_port ] }
```

```
after redirect css service service_name [ log ] { tcp | udp } { { source_address source_wildcard | any | host source_host_address } [ eq source_port | gt source_port | lt source_port | neq source_port | range start_source_port end_source_port ] } { { dest_address dest_wildcard | any | host dest_host_address } [ eq dest_port | gt dest_port | lt dest_port | neq dest_port | range start_dest_port end_dest_port ] }
```

```
before redirect css service service_name [ log ] { tcp | udp } { { source_address source_wildcard | any | host source_host_address } [ eq source_port | gt source_port | lt source_port | neq source_port | range start_source_port end_source_port ] } { { dest_address dest_wildcard | any | host dest_host_address } [ eq dest_port | gt dest_port | lt dest_port | neq dest_port | range start_dest_port end_dest_port ] }
```

```
no redirect css service service_name [ log ] { tcp | udp } { { source_address source_wildcard | any | host source_host_address } [ eq source_port | gt source_port | lt source_port | neq source_port | range start_source_port end_source_port ] } { { dest_address dest_wildcard | any | host dest_host_address } [ eq dest_port | gt dest_port | lt dest_port | neq dest_port | range start_dest_port end_dest_port ] }
```

---

**after**

Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.
**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

**before**
Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

**no**
Removes the rule definition which exactly matches the options specified.

**css service service_name**
The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the `show active-charging service all` command to display the names of all configured charging services.
`service_name` must be an alphanumeric string from 1 through 15 characters.

**log**
Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

**tcp | udp**
Specifies the redirect is to be applied to IP-based transmission control protocol or the user datagram protocol.
  • `tcp`: Redirect applies to TCP packets.
  • `udp`: Redirect applies to UDP packets.

**source_address**
The IP address(es) from which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the `source_wildcard` parameter.

**source_wildcard**
This option is used in conjunction with the `source_address` option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:
  • Zero-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be identical.
  • One-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be ignored.
**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.

- **any**
  Specifies that the rule definition applies to all packets.

- **host**
  Specifies that the rule definition applies to a specific host as determined by its IP address.

- **source_host_address**
  The IP address of the source host to filter against expressed in IPv4 dotted-decimal notation.

- **dest_host_address**
  The IP address of the destination host to filter against expressed in IPv4 dotted-decimal notation.

- **eq source_port**
  Specifies a single, specific source TCP port number to be filtered.
  `source_port` must be configured to an integer value from 0 to 65535.

- **gt source_port**
  Specifies that all source TCP port numbers greater than the one specified are to be filtered.
  `source_port` must be configured to an integer value from 0 to 65535.

- **lt source_port**
  Specifies that all source TCP port numbers less than the one specified are to be filtered.
  `source_port` must be configured to an integer value from 0 to 65535.

- **neq source_port**
  Specifies that all source TCP port numbers not equal to the one specified are to be filtered.
  `source_port` must be configured to an integer value from 0 to 65535.

- **range start_source_port end_source_port**
  Specifies that all source TCP ports within a specific range are to be filtered.
  `start_source_port` is the initial port in the range and `end_source_port` is the final port in the range.
  Both `start_source_port` and `end_source_port` can be configured to an integer value from 0 to 65535.

- **dest_address**
  The IP address(es) to which the packet is to be sent.
  This option is used to filter all packets to a specific IP address or a group of IP addresses.
  When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the `dest_wildcard` parameter.
**dest_wildcard**

This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered. The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.

**eq dest_port**

Specifies a single, specific destination TCP port number to be filtered. *dest_port* must be configured to an integer value from 0 to 65535.

**gt dest_port**

Specifies that all destination TCP port numbers greater than the one specified are to be filtered. *dest_port* must be configured to an integer value from 0 to 65535.

**lt dest_port**

Specifies that all destination TCP port numbers less than the one specified are to be filtered. *dest_port* must be configured to an integer value from 0 to 65535.

**neq dest_port**

Specifies that all destination TCP port numbers not equal to the one specified are to be filtered. *dest_port* must be configured to an integer value from 0 to 65535.

**range start_dest_port end_dest_port**

Specifies that all destination TCP ports within a specific range are to be filtered. *start_dest_port* is the initial port in the range and *end_dest_port* is the final port in the range. Both *start_dest_port* and *end_dest_port* can be configured to an integer value from 0 to 65535.

**Usage**

Field: Block IP packets when the source and destination are of interest but for only a limited set of ports.

**Important:** The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the Engineering Rules appendix in the System Administration Guide.

**Important:** Also note that “redirect” rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

**Example**
The following command defines a rule definition that redirects packets to the charging service named chgsvcl, and UDP packets coming from any host are matched:

```
redirect css service chgsvcl udp any
```

The following sets the insertion point before the rule definition above:

```
before redirect css service chgsvcl udp any
```

The following command sets the insertion point after the first rule definition above:

```
after redirect css service chgsvcl udp any
```

The following command deletes the rule definition above:

```
no redirect css service chgsvcl udp any
```
redirect css service (for downlink, any)

Redirects subscriber sessions based on any packet received in the downlink (from the Mobile Node) direction (Content Service Steering). This command is also used to set the access control list insertion point.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > ACL Configuration

configure > context context_name > ip access-list acl_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-acl)#

Syntax

redirect css service service_name [ log ] downlink any

after redirect css service service_name [ log ] downlink any

before redirect css service service_name [ log ] downlink any

no redirect css service service_name [ log ] downlink any

after
Indicates all rule definitions defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

Important: If the options specified do not exactly match an existing rule definition, the insertion point does not change.

before
Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

Important: If the options specified do not exactly match an existing rule definition, the insertion point does not change.

no
Removes the rule definition which exactly matches the options specified.
**css service service_name**

The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the `show active-charging service all` command to display the names of all configured charging services. `service_name` must be an alphanumeric string from 1 through 15 characters.

**downlink**

Apply this rule definition only to packets in the downlink (from the Mobile Node) direction.

**log**

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

**any**

Indicates all packets will match the redirect regardless of source and/or destination.

**Usage**

Define a catch all rule definition to place at the end of the list of rule definitions to provide explicit handling of rule definitions which do not fit any other criteria.

**Important:** Any rule definition which is added to be a catch all should also have the `log` option specified. The logged packets may be used to determine if the current list of rule definitions is adequate or needs modification to ensure proper security.

**Important:** The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the Engineering Rules appendix in the System Administration Guide.

**Important:** Also note that “redirect” rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

**Example**

The following command defines a rule definition that redirects packets to the charging service with the name `chgsvc1` and any source IP:

```
redirect css service chgsvc1 downlink any
```

The following sets the insertion point before the rule definition above:

```
before redirect css service chgsvc1 downlink any
```

The following command sets the insertion point after the first rule definition above:

```
after redirect css service chgsvc1 downlink any
```

The following deletes the first rule definition above:

```
no redirect css service chgsvc1 downlink any
```
redirect css service (for downlink, by host IP address)

Redirects subscriber sessions based on the targeted host IP address in the downlink (from the Mobile Node) direction (Content Service Steering).

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > ACL Configuration
```
configure > context context_name > ip access-list acl_name
```
Entering the above command sequence results in the following prompt:
```
[context_name]host_name(config-acl)#
```

**Syntax**

```
redirect css service service_name [ log ] downlink host source_host_address

before redirect css service service_name [ log ] downlink host source_host_address

after redirect css service service_name [ log ] downlink host source_host_address

no redirect css service service_name [ log ] downlink host source_host_address
```

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

```
before
```

Indicates all rule definitions defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

```
Important: 
```

If the options specified do not exactly match an existing rule definition, the insertion point does not change.

```
no
```

Removes the rule definition which exactly matches the options specified.
**css service service_name**

The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the `show active-charging service all` command to display the names of all configured charging services. `service_name` must be an alphanumeric string from 1 through 15 characters.

**downlink**

Apply this rule definition only to packets in the downlink (from the Mobile Node) direction.

**log**

Default: packets are not logged. Indicates all packets which match the redirect are to be logged.

**host**

Specifies that the rule definition applies to a specific host as determined by its IP address.

**source_host_address**

The IP address of the source host to filter against expressed in IPv4 dotted-decimal notation.

**Usage**

Define a rule definition when a very specific remote host is to be blocked. In simplified networks where the access controls need only block a few hosts, this command allows the rule definitions to be very clear and concise.

**Important:** The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the Engineering Rules appendix in the System Administration Guide.

**Important:** Also note that “redirect” rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

**Example**

The following command defines a rule definition that redirects packets to the charging service with the name `chgsvcl` and a host IP address of `192.168.200.11`:

```
redirect css service chgsvcl downlink host 192.168.200.11
```

The following sets the insertion point before the rule definition above:

```
before redirect css service chgsvcl downlink host 192.168.200.11
```

The following command sets the insertion point after the first rule definition above:

```
after redirect css service chgsvcl downlink host 192.168.200.11
```

The following deletes the first rule definition above:

```
no redirect css service chgsvcl downlink host 192.168.200.11
```
redirect css service (for downlink, by ICMP packets)

Redirects subscriber sessions based on the internet control message protocol packets in the downlink (from the Mobile Node) direction (Content Service Steering).

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > ACL Configuration

```
configure > context context_name > ip access-list acl_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-acl)#
```

**Syntax**

```
redirect css service service_name [ log ] downlink icmp { any | host source_host_address | source_address source_wildcard } { any | host dest_host_address | dest_address dest_wildcard } [ icmp_type [ icmp_code ] ]

after redirect css service service_name [ log ] downlink icmp { any | host source_host_address | source_address source_wildcard } { any | host dest_host_address | dest_address dest_wildcard } [ icmp_type [ icmp_code ] ]

before redirect css service service_name [ log ] downlink icmp { any | host source_host_address | source_address source_wildcard } { any | host dest_host_address | dest_address dest_wildcard } [ icmp_type [ icmp_code ] ]

no redirect css service service_name [ log ] downlink icmp { any | host source_host_address | source_address source_wildcard } { any | host dest_host_address | dest_address dest_wildcard } [ icmp_type [ icmp_code ] ]
```

**Important:**
If the options specified do not exactly match an existing rule definition, the insertion point does not change.

**after**
Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

---

**before**
Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.
redirect css service (for downlink, by ICMP packets)

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

```no
```

Removes the rule definition which exactly matches the options specified.

```css service service_name```

The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the `show active-charging service all` command to display the names of all configured charging services.

*service_name* must be an alphanumeric string from 1 through 15 characters.

```downlink```

Apply this rule definition only to packets in the downlink (from the Mobile Node) direction.

```log```

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

```source_address```

The IP address(es) from which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the `source_wildcard` parameter.

```source_wildcard```

This option is used in conjunction with the `source_address` option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:
- Zero-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.

```any```

Specifies that the rule definition applies to all packets.

```host```

Specifies that the rule definition applies to a specific host as determined by its IP address.
source_host_address
The IP address of the source host to filter against expressed in IPv4 dotted-decimal notation.

dest_host_address
The IP address of the destination host to filter against expressed in IPv4 dotted-decimal notation.

dest_address
The IP address(es) to which the packet is to be sent.
This option is used to filter all packets to a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the dest_wildcard parameter.

dest_wildcard
This option is used in conjunction with the dest_address option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:
- Zero-bits in this parameter mean that the corresponding bits configured for the dest_address parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the dest_address parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.

icmp_type
Specifies that all ICMP packets of a particular type are to be filtered. The type can be an integer value between 0 and 255.

icmp_code
Specifies that all ICMP packets of a particular code are to be filtered. The type can be an integer value between 0 and 255.

**Usage**
Define a rule definition to block ICMP packets which can be used for address resolution and possibly be a security risk.
The IP redirecting allows flexible controls for pairs of individual hosts or groups by IP masking which allows the redirecting of entire subnets if necessary.

**Important:** The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the Engineering Rules appendix in the System Administration Guide.

**Important:** Also note that “redirect” rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.
Example

The following command defines a rule definition that redirects packets to the charging service named `chgsvc1`, and ICMP packets coming in the downlink (from the Mobile Node) direction from the host with the IP address 192.168.100.25:

```
redirect css service chgsvc1 downlink icmp host 192.168.100.25
```

The following sets the insertion point before the rule definition above:

```
before redirect css service chgsvc1 downlink icmp host 192.168.100.25
```

The following command sets the insertion point after the first rule definition above:

```
after redirect css service chgsvc1 downlink icmp host 192.168.100.25
```

The following deletes the first rule definition above:

```
no redirect css service chgsvc1 downlink icmp host 192.168.100.25
```
redirect css service (for downlink, by IP packets)

Redirects subscriber sessions based on the internet protocol packets in the downlink (from the Mobile Node) direction (Content Service Steering).

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > ACL Configuration

configure > context context_name > ip access-list acl_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-acl)#

Syntax

redirect css service service_name [ log ] downlink ip { any | host source_host_address | source_address source_wildcard } { any | host dest_host_address | dest_address dest_wildcard } [ fragment ]

after redirect css service service_name [ log ] downlink ip { any | host source_host_address | source_address source_wildcard } { any | host dest_host_address | dest_address dest_wildcard } [ fragment ]

before redirect css service service_name [ log ] downlink ip { any | host source_host_address | source_address source_wildcard } { any | host dest_host_address | dest_address dest_wildcard } [ fragment ]

no redirect css service service_name [ log ] downlink ip { any | host source_host_address | source_address source_wildcard } { any | host dest_host_address | dest_address dest_wildcard } [ fragment ]

after
Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

Important: If the options specified do not exactly match an existing rule definition, the insertion point does not change.

before
Indicates all rule definitions defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.
**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

---

no

Removes the rule definition which exactly matches the options specified.

---

css service service_name

The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the `show active-charging service all` command to display the names of all configured charging services. *service_name* must be an alphanumeric string from 1 through 15 characters.

---

downlink

Apply this rule definition only to packets in the downlink (from the Mobile Node) direction.

---

log

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

---

source_address

The IP address(es) from which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the `source_wildcard` parameter.

---

source_wildcard

This option is used in conjunction with the `source_address` option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:
- Zero-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.

---

any

Specifies that the rule definition applies to all packets.

---

host

Specifies that the rule definition applies to a specific host as determined by its IP address.
source_host_address
The IP address of the source host to filter against expressed in IPv4 dotted-decimal notation.

dest_host_address
The IP address of the destination host to filter against expressed in IPv4 dotted-decimal notation.

dest_address
The IP address(es) to which the packet is to be sent. This option is used to filter all packets to a specific IP address or a group of IP addresses. When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the dest_wildcard parameter.

dest_wildcard
This option is used in conjunction with the dest_address option to specify a group of addresses for which packets are to be filtered. The mask must be entered as a complement:
- Zero-bits in this parameter mean that the corresponding bits configured for the dest_address parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the dest_address parameter must be ignored.

Important: The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.

fragment
Indicates packet redirection is to be applied to IP packet fragments only.

Usage
Block IP packets when the source and destination are of interest.

Important: The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the Engineering Rules appendix in the System Administration Guide.

Important: Also note that “redirect” rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example
The following command defines a rule definition that redirects packets to the charging service named chgsvcl, and downlink IP packets coming from the host with the IP address 198.162.100.25, and fragmented packets for any destination are matched:

**redirect css service chgsvcl downlink ip host 198.162.100.25 any fragment**

The following sets the insertion point before the rule definition above:
before redirect css service chgsvcl downlink ip host 198.162.100.25 any fragment

The following command sets the insertion point after the first rule definition above:

after redirect css service chgsvcl downlink ip host 198.162.100.25 any fragment

The following deletes the first rule definition above:

no redirect css service chgsvcl downlink ip host 198.162.100.25 any fragment
redirect css service (for downlink, by source IP address masking)

Redirects subscriber sessions based on the IP address mask sent by the source in the downlink (from the Mobile Node) direction (Content Service Steering).

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > ACL Configuration

configure > context context_name > ip access-list acl_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-acl)#

**Syntax**

```
redirect css service service_name [ log ] downlink source_address source_wildcard
after redirect css service service_name [ log ] downlink source_address source_wildcard
before redirect css service service_name [ log ] downlink source_address source_wildcard
no redirect css service service_name [ log ] downlink source_address source_wildcard
```

**after**

Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

**before**

Indicates all rule definitions defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.
no

Removes the rule definition which exactly matches the options specified.

css service service_name

The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the show active-charging service all command to display the names of all configured charging services. service_name must be an alphanumeric string from 1 through 15 characters.

downlink

Apply this rule definition only to packets in the downlink (from the Mobile Node) direction.

log

Default: packets are not logged.
Indicates all packets which match the filter are to be logged.

source_address

The IP address(es) from which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the source_wildcard parameter.

source_wildcard

This option is used in conjunction with the source_address option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:
  ● Zero-bits in this parameter mean that the corresponding bits configured for the source_address parameter must be identical.
  ● One-bits in this parameter mean that the corresponding bits configured for the source_address parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.

**Usage**

Define a rule definition when any packet from the IP addresses which fall into the group of addresses matching the IP address masking. This allows the reduction of filtering rule definitions as it does not require a rule definition for each source and destination pair.

**Important:** The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the Engineering Rules appendix in the System Administration Guide.

**Example**

The following command defines a rule definition to redirect packets to a charging service named chgsvc1:
redirect css service chgsvcl downlink 10.2.3.0 0.0.0.31
redirect css service (for downlink, by TCP/UDP packets)

Redirects subscriber sessions to a charging service based on the transmission control protocol/user datagram protocol packets in the downlink (from the Mobile Node) direction (Content Service Steering).

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > ACL Configuration
configure > context context_name > ip access-list acl_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-acl)#

Syntax

redirect css service service_name [ log ] downlink { tcp | udp } { { source_address source_wildcard | any | host source_host_address } [ eq source_port | gt source_port | lt source_port | neq source_port | range start_source_port end_source_port ] } { { dest_address dest_wildcard | any | host dest_host_address } [ eq dest_port | gt dest_port | lt dest_port | neq dest_port | range start_dest_port end_dest_port ] }

after redirect css service service_name [ log ] downlink { tcp | udp } { { source_address source_wildcard | any | host source_host_address } [ eq source_port | gt source_port | lt source_port | neq source_port | range start_source_port end_source_port ] } { { dest_address dest_wildcard | any | host dest_host_address } [ eq dest_port | gt dest_port | lt dest_port | neq dest_port | range start_dest_port end_dest_port ] }

before redirect css service service_name [ log ] downlink { tcp | udp } { { source_address source_wildcard | any | host source_host_address } [ eq source_port | gt source_port | lt source_port | neq source_port | range start_source_port end_source_port ] } { { dest_address dest_wildcard | any | host dest_host_address } [ eq dest_port | gt dest_port | lt dest_port | neq dest_port | range start_dest_port end_dest_port ] }

no redirect css service service_name [ log ] downlink { tcp | udp } { { source_address source_wildcard | any | host source_host_address } [ eq source_port | gt source_port | lt source_port | neq source_port | range start_source_port end_source_port ] } { { dest_address dest_wildcard | any | host dest_host_address } [ eq dest_port | gt dest_port | lt dest_port | neq dest_port | range start_dest_port end_dest_port ] }

after

 Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.
**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

**before**
Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed. This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

**no**
Removes the rule definition which exactly matches the options specified.

**css service service_name**
The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the `show active-charging service all` command to display the names of all configured charging services.

*service_name* must be an alphanumeric string from 1 through 15 characters.

**downlink**
Apply this rule definition only to packets in the downlink (from the Mobile Node) direction.

**log**
Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

**tcp | udp**
Specifies the redirect is to be applied to IP based transmission control protocol or the user datagram protocol.
- **tcp**: Redirect applies to TCP packets.
- **udp**: Redirect applies to UDP packets.

**source_address**
The IP address(es) from which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the `source wildcard` parameter.

**source wildcard**
This option is used in conjunction with the `source_address` option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:
- Zero-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be identical.
ACL Configuration Mode Commands

- One-bits in this parameter mean that the corresponding bits configured for the source_address parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

---

`any`
Specifies that the rule definition applies to all packets.

`host`
Specifies that the rule definition applies to a specific host as determined by its IP address.

`source_host_address`
The IP address of the source host to filter against expressed in IPv4 dotted-decimal notation.

`dest_host_address`
The IP address of the destination host to filter against expressed in IPv4 dotted-decimal notation.

`eq source_port`
Specifies a single, specific source TCP port number to be filtered. `source_port` must be configured to an integer value from 0 to 65535.

`gt source_port`
Specifies that all source TCP port numbers greater than the one specified are to be filtered. `source_port` must be configured to an integer value from 0 to 65535.

`lt source_port`
Specifies that all source TCP port numbers less than the one specified are to be filtered. `source_port` must be configured to an integer value from 0 to 65535.

`neq source_port`
Specifies that all source TCP port numbers not equal to the one specified are to be filtered. `source_port` must be configured to an integer value from 0 to 65535.

`range start_source_port end_source_port`
Specifies that all source TCP ports within a specific range are to be filtered. `start_source_port` is the initial port in the range and `end_source_port` is the final port in the range. Both `start_source_port` and `end_source_port` can be configured to an integer value from 0 to 65535.

`dest_address`
The IP address(es) to which the packet is to be sent. This option is used to filter all packets to a specific IP address or a group of IP addresses. When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the `dest_wildcard` parameter.
dest_wildcard

This option is used in conjunction with the dest_address option to specify a group of addresses for which packets are to be filtered. The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the dest_address parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the dest_address parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.

eq dest_port

Specifies a single, specific destination TCP port number to be filtered. dest_port must be configured to an integer value from 0 to 65535.

gt dest_port

Specifies that all destination TCP port numbers greater than the one specified are to be filtered. dest_port must be configured to an integer value from 0 to 65535.

lt dest_port

Specifies that all destination TCP port numbers less than the one specified are to be filtered. dest_port must be configured to an integer value from 0 to 65535.

neq dest_port

Specifies that all destination TCP port numbers not equal to the one specified are to be filtered. dest_port must be configured to an integer value from 0 to 65535.

range start_dest_port end_dest_port

Specifies that all destination TCP ports within a specific range are to be filtered. start_dest_port is the initial port in the range and end_dest_port is the final port in the range. Both start_dest_port and end_dest_port can be configured to an integer value from 0 to 65535.

**Usage**

Block IP packets when the source and destination are of interest but for only a limited set of ports.

**Important:** The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the Engineering Rules appendix in the System Administration Guide.

**Important:** Also note that “redirect” rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

**Example**
The following command defines a rule definition that redirects packets to the charging service named `chgsvcl`, and UDP packets coming from any host are matched:

```
redirect css service chgsvcl downlink udp any
```

The following sets the insertion point before the rule definition above:

```
before redirect css service chgsvcl downlink udp any
```

The following command sets the insertion point after the first rule definition above:

```
after redirect css service chgsvcl downlink udp any
```

The following deletes the rule definition above:

```
no redirect css service chgsvcl downlink udp any
```
**redirect css service (for uplink, any)**

Redirects subscriber sessions based on any packet received in the uplink (to the Mobile Node) direction (Content Service Steering). This command is also used to set the access control list insertion point.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > ACL Configuration

`configure > context context_name > ip access-list acl_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-acl)#
```

**Syntax**

```
redirect css service service_name [ log ] uplink any
after redirect css service service_name [ log ] uplink any
before redirect css service service_name [ log ] uplink any
no redirect css service service_name [ log ] uplink any
```

- **after**
  Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.
  This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

> **Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

- **before**
  Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.
  This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

> **Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

- **no**
  Removes the rule definition which exactly matches the options specified.
**css service service_name**

The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the `show active-charging service all` command to display the names of all configured charging services. `service_name` must be an alphanumeric string from 1 through 15 characters.

**uplink**

Apply this rule definition only to packets in the uplink (to the Mobile Node) direction.

**log**

Default: packets are not logged. Indicates all packets which match the redirect are to be logged.

**any**

Indicates all packets will match the redirect regardless of source and/or destination.

**Usage**

Define a catch all rule definition to place at the end of the list of rule definitions to provide explicit handling of rule definitions which do not fit any other criteria.

**Important:** It is suggested that any rule definition which is added to be a catch all should also have the `log` option specified. The logged packets may be used to determine if the current list of rule definitions is adequate or needs modification to ensure proper security.

**Important:** The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*.

**Important:** Also note that “redirect” rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

**Example**

The following command defines a rule definition that redirects packets to the charging service with the name `chgsvcl` and any source IP:

```
redirect css service chgsvcl uplink any
```

The following sets the insertion point before the rule definition above:

```
before redirect css service chgsvcl uplink any
```

The following command sets the insertion point after the first rule definition above:

```
after redirect css service chgsvcl uplink any
```

The following deletes the first rule definition above:

```
no redirect css service chgsvcl uplink any
```
redirect css service (for uplink, by host IP address)

Redirects subscriber sessions based on the targeted host IP address in the uplink (to the Mobile Node) direction (Content Service Steering).

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > ACL Configuration

```
configure > context context_name > ip access-list acl_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-acl)#
```

**Syntax**

```
redirect css service service_name [ log ] uplink host source_host_address
after redirect css service service_name [ log ] uplink host source_host_address
before redirect css service service_name [ log ] uplink host source_host_address
no redirect css service service_name [ log ] uplink host source_host_address
```

**uplink**

Apply this rule definition only to packets in the uplink (to the Mobile Node) direction.

**after**

Indicates all rule definitions defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

**before**

Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.
no
Removes the rule definition which exactly matches the options specified.

```css
service service_name
```
The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the `show active-charging service all` command to display the names of all configured charging services. `service_name` must be an alphanumeric string from 1 through 15 characters.

```uplink
```
Apply this rule definition only to packets in the uplink (to the Mobile Node) direction.

```log
```
Default: packets are not logged. Indicates all packets which match the redirect are to be logged.

```host
```
Specifies that the rule definition applies to a specific host as determined by its IP address.

```source_host_address
```
The IP address of the source host to filter against expressed in IPv4 dotted-decimal notation.

### Usage
Define a rule definition when a very specific remote host is to be blocked. In simplified networks where the access controls need only block a few hosts, this command allows the rule definitions to be very clear and concise.

**Important:** The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the Engineering Rules appendix in the System Administration Guide.

**Important:** Also note that “redirect” rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

### Example
The following command defines a rule definition that redirects packets to the charging service with the name `chgsvcl` and a host IP address of `192.168.200.11`:

```redirect css service chgsvcl uplink host 192.168.200.11
```

The following sets the insertion point before the rule definition above:

```before redirect css service chgsvcl uplink host 192.168.200.11
```

The following command sets the insertion point after the first rule definition above:

```after redirect css service chgsvcl uplink host 192.168.200.11
```
The following deletes the first rule definition above:

```
no redirect css service chgsvc1 uplink host 192.168.200.11
```
redirect css service (for uplink, by ICMP packets)

Redirects subscriber sessions based on the internet control message protocol packets in the uplink (to the Mobile Node) direction (Content Service Steering).

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > ACL Configuration

configure > context context_name > ip access-list acl_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-acl)#

Syntax

redirect css service service_name [ log ] uplink icmp { any | host source_host_address | source_address source_wildcard } { any | host dest_host_address | dest_address dest_wildcard } [ icmp_type [ icmp_code ]

after redirect css service service_name [ log ] uplink icmp { any | host source_host_address | source_address source_wildcard } { any | host dest_host_address | dest_address dest_wildcard } [ icmp_type [ icmp_code ]

before redirect css service service_name [ log ] uplink icmp { any | host source_host_address | source_address source_wildcard } { any | host dest_host_address | dest_address dest_wildcard } [ icmp_type [ icmp_code ]

no redirect css service service_name [ log ] uplink icmp { any | host source_host_address | source_address source_wildcard } { any | host dest_host_address | dest_address dest_wildcard } [ icmp_type [ icmp_code ]

---

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

---

**before**

Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.
**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

`no`
Removes the rule definition which exactly matches the options specified.

`css service service_name`
The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the `show active-charging service all` command to display the names of all configured charging services.

`service_name` must be an alphanumeric string from 1 through 15 characters.

`uplink`
Apply this rule definition only to packets in the uplink (to the Mobile Node) direction.

`log`
Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

`source_address`
The IP address(es) from which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the `source_wildcard` parameter.

`source_wildcard`
This option is used in conjunction with the `source_address` option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

`any`
Specifies that the rule definition applies to all packets.

`host`
Specifies that the rule definition applies to a specific host as determined by its IP address.
source_host_address
The IP address of the source host to filter against expressed in IPv4 dotted-decimal notation.

dest_host_address
The IP address of the destination host to filter against expressed in IPv4 dotted-decimal notation.

dest_address
The IP address(es) to which the packet is to be sent.
This option is used to filter all packets to a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the dest_wildcard parameter.

dest_wildcard
This option is used in conjunction with the dest_address option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:
- Zero-bits in this parameter mean that the corresponding bits configured for the dest_address parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the dest_address parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.0.7.15 is not acceptable since the one-bits are not contiguous.

icmp_type
Specifies that all ICMP packets of a particular type are to be filtered. The type can be an integer value between 0 and 255.

icmp_code
Specifies that all ICMP packets of a particular code are to be filtered. The type can be an integer value between 0 and 255.

Usage
Define a rule definition to block ICMP packets which can be used for address resolution and possibly be a security risk.
The IP redirecting allows flexible controls for pairs of individual hosts or groups by IP masking which allows the redirecting of entire subnets if necessary.

**Important:** The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the Engineering Rules appendix in the System Administration Guide.

**Important:** Also note that “redirect” rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.
Example

The following command defines a rule definition that redirects packets to the charging service named chgsvcl, and ICMP packets in the uplink (to the Mobile Node) direction from the host with the IP address 198.162.100.25:

```
redirect css service chgsvcl uplink icmp host 192.168.100.25
```

The following sets the insertion point before the rule definition above:

```
before redirect css service chgsvcl uplink icmp host 192.168.100.25
```

The following command sets the insertion point after the first rule definition above:

```
after redirect css service chgsvcl uplink icmp host 192.168.100.25
```

The following deletes the first rule definition above:

```
no redirect css service chgsvcl uplink icmp host 192.168.100.25
```
redirect css service (for uplink, by IP packets)

Redirects subscriber sessions based on the internet protocol packets in the uplink (to the Mobile Node) direction (Content Service Steering).

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > ACL Configuration

configure > context context_name > ip access-list acl_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-acl)#

**Syntax**

redirect css service service_name [ log ] uplink ip { any | host source_host_address | source_address source_wildcard } { any | host dest_host_address | dest_address dest_wildcard } [ fragment ]

after redirect css service service_name [ log ] uplink ip { any | host source_host_address | source_address source_wildcard } { any | host dest_host_address | dest_address dest_wildcard } [ fragment ]

before redirect css service service_name [ log ] uplink ip { any | host source_host_address | source_address source_wildcard } { any | host dest_host_address | dest_address dest_wildcard } [ fragment ]

no redirect css service service_name [ log ] uplink ip { any | host source_host_address | source_address source_wildcard } { any | host dest_host_address | dest_address dest_wildcard } [ fragment ]

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

**after**

Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

**before**

Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.
**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>no</strong></td>
<td>Removes the rule definition which exactly matches the options specified.</td>
</tr>
<tr>
<td><strong>css service</strong></td>
<td>The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the <code>show active-charging service all</code> command to display the names of all configured charging services. <code>service_name</code> must be an alphanumeric string from 1 through 15 characters.</td>
</tr>
<tr>
<td><strong>uplink</strong></td>
<td>Apply this rule definition only to packets in the uplink (to the Mobile Node) direction.</td>
</tr>
<tr>
<td><strong>log</strong></td>
<td>Default: packets are not logged. Indicates all packets which match the redirect are to be logged.</td>
</tr>
<tr>
<td><strong>source_address</strong></td>
<td>The IP address(es) from which the packet originated. This option is used to filter all packets from a specific IP address or a group of IP addresses. When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the <code>source_wildcard</code> parameter.</td>
</tr>
</tbody>
</table>
| **source_wildcard** | This option is used in conjunction with the `source_address` option to specify a group of addresses for which packets are to be filtered. The mask must be entered as a complement:  
  - Zero-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be identical.  
  - One-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be ignored. |
| **any**          | Specifies that the rule definition applies to all packets.                  |
| **host**         | Specifies that the rule definition applies to a specific host as determined by its IP address. |
source_host_address

The IP address of the source host to filter against expressed in IPv4 dotted-decimal notation.

dest_host_address

The IP address of the destination host to filter against expressed in IPv4 dotted-decimal notation.

dest_address

The IP address(es) to which the packet is to be sent.
This option is used to filter all packets to a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the dest_wildcard parameter.

dest_wildcard

This option is used in conjunction with the dest_address option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:
• Zero-bits in this parameter mean that the corresponding bits configured for the dest_address parameter must be identical.
• One-bits in this parameter mean that the corresponding bits configured for the dest_address parameter must be ignored.

fragment

Indicates packet redirection is to be applied to IP packet fragments only.

Usage

Block IP packets when the source and destination are of interest.

⚠️ Important: The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the Engineering Rules appendix in the System Administration Guide.

Example

The following command defines a rule definition that redirects packets to the charging service named chgsvc1, and uplink IP packets going to the host with the IP address 198.162.100.25, and fragmented packets for any destination are matched:

```
redirect css service chgsvc1 uplink ip host 198.162.100.25 any fragment
```

The following sets the insertion point before the rule definition above:

```
before redirect css service chgsvc1 uplink ip host 198.162.100.25 any fragment
```

The following command sets the insertion point after the first rule definition above:

```
after redirect css service chgsvc1 uplink ip host 198.162.100.25 any fragment
```

The following command deletes the first rule definition above:
no redirect css service chgsvc1 uplink ip host 198.162.100.25 any fragment
redirect css service (for uplink, by source IP address masking)

Redirects subscriber sessions based on the IP address mask sent by the source in the uplink (to the Mobile Node) direction (Content Service Steering).

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > ACL Configuration

configure > context context_name > ip access-list acl_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-acl)#

**Syntax**

redirect css service service_name [ log ] uplink source_address source_wildcard

after redirect css service service_name [ log ] uplink source_address source_wildcard

before redirect css service service_name [ log ] uplink source_address source_wildcard

no redirect css service service_name [ log ] uplink source_address source_wildcard

**after**
Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

**before**
Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

**no**
Removes the rule definition which exactly matches the options specified.

css service service_name

The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the show active-charging service all command to display the names of all configured charging services.

*service_name* must be an alphanumeric string from 1 through 15 characters.
ACL Configuration Mode Commands

redirect css service (for uplink, by source IP address masking)

<table>
<thead>
<tr>
<th>uplink</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apply this rule definition only to packets in the uplink (to the Mobile Node) direction.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>log</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default: packets are not logged. Indicates all packets which match the filter are to be logged.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>source_address</th>
</tr>
</thead>
<tbody>
<tr>
<td>The IP address(es) from which the packet originated. This option is used to filter all packets from a specific IP address or a group of IP addresses. When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the <code>source_wildcard</code> parameter.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>source_wildcard</th>
</tr>
</thead>
<tbody>
<tr>
<td>This option is used in conjunction with the <code>source_address</code> option to specify a group of addresses for which packets are to be filtered. The mask must be entered as a complement:</td>
</tr>
<tr>
<td>- Zero-bits in this parameter mean that the corresponding bits configured for the <code>source_address</code> parameter must be identical.</td>
</tr>
<tr>
<td>- One-bits in this parameter mean that the corresponding bits configured for the <code>source_address</code> parameter must be ignored.</td>
</tr>
</tbody>
</table>

**Usage**

Define a rule definition when any packet from the IP addresses which fall into the group of addresses matching the IP address masking. This allows the reduction of filtering rule definitions as it does not require a rule definition for each source and destination pair.

**Important:** The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the Engineering Rules appendix in the System Administration Guide.

**Example**

The following command defines a rule definition to redirect packets to a charging service named `chgsvcl`:

```
redirect css service chgsvcl uplink 10.2.3.0 0.0.0.31
```
redirect css service (for uplink, by TCP/UDP packets)

Redirects subscriber sessions to a charging service based on the transmission control protocol/user datagram protocol packets in the uplink (to the Mobile Node) direction (Content Service Steering).

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > ACL Configuration

```bash
configure > context context_name > ip access-list acl_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-acl)#
```

**Syntax**

```bash
redirect css service service_name [ log ] uplink { tcp | udp } { { source_address source_wildcard | any | source_host_address } [ eq source_port | gt source_port | lt source_port | neq source_port | range start_source_port end_source_port ] } { { dest_address dest_wildcard | any | host dest_host_address } [ eq dest_port | gt dest_port | lt dest_port | neq dest_port | range start_dest_port end_dest_port ] }
```

**after redirect css service service_name [ log ] uplink { tcp | udp } { { source_address source_wildcard | any | source_host_address } [ eq source_port | gt source_port | lt source_port | neq source_port | range start_source_port end_source_port ] } { { dest_address dest_wildcard | any | host dest_host_address } [ eq dest_port | gt dest_port | lt dest_port | neq dest_port | range start_dest_port end_dest_port ] }

**before redirect css service service_name [ log ] uplink { tcp | udp } { { source_address source_wildcard | any | source_host_address } [ eq source_port | gt source_port | lt source_port | neq source_port | range start_source_port end_source_port ] } { { dest_address dest_wildcard | any | host dest_host_address } [ eq dest_port | gt dest_port | lt dest_port | neq dest_port | range start_dest_port end_dest_port ] }

**no redirect css service service_name [ log ] uplink { tcp | udp } { { source_address source_wildcard | any | source_host_address } [ eq source_port | gt source_port | lt source_port | neq source_port | range start_source_port end_source_port ] } { { dest_address dest_wildcard | any | host dest_host_address } [ eq dest_port | gt dest_port | lt dest_port | neq dest_port | range start_dest_port end_dest_port ] }

**after**
Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.
before
Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed. This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

no
Removes the rule definition which exactly matches the options specified.

css service service_name
The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the show active-charging service all command to display the names of all configured charging services. service_name must be an alphanumeric string from 1 through 15 characters.

uplink
Apply this rule definition only to packets in the uplink (to the Mobile Node) direction.

log
Default: packets are not logged. Indicates all packets which match the redirect are to be logged.

tcp | udp
Specifies the redirect is to be applied to IP based transmission control protocol or the user datagram protocol.
  • tcp: Redirect applies to TPC packets.
  • udp: Redirect applies to UDP packets.

source_address
The IP address(es) from which the packet originated. This option is used to filter all packets from a specific IP address or a group of IP addresses. When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the source_wildcard parameter.

source_wildcard
This option is used in conjunction with the source_address option to specify a group of addresses for which packets are to be filtered. The mask must be entered as a complement:
  • Zero-bits in this parameter mean that the corresponding bits configured for the source_address parameter must be identical.
  • One-bits in this parameter mean that the corresponding bits configured for the source_address parameter must be ignored.

any
Specifies that the rule definition applies to all packets.
**host**
Specifies that the rule definition applies to a specific host as determined by its IP address.

**source_host_address**
The IP address of the source host to filter against expressed in IPv4 dotted-decimal notation.

**dest_host_address**
The IP address of the destination host to filter against expressed in IPv4 dotted-decimal notation.

**eq source_port**
Specifies a single, specific source TCP port number to be filtered. 
source_port must be configured to an integer value from 0 to 65535.

**gt source_port**
Specifies that all source TCP port numbers greater than the one specified are to be filtered. 
source_port must be configured to an integer value from 0 to 65535.

**lt source_port**
Specifies that all source TCP port numbers less than the one specified are to be filtered. 
source_port must be configured to an integer value from 0 to 65535.

**neq source_port**
Specifies that all source TCP port numbers not equal to the one specified are to be filtered. 
source_port must be configured to an integer value from 0 to 65535.

**range** **start_source_port** **end_source_port**
Specifies that all source TCP ports within a specific range are to be filtered. 
start_source_port is the initial port in the range and end_source_port is the final port in the range. 
Both start_source_port and end_source_port can be configured to an integer value from 0 to 65535.

**dest_address**
The IP address(es) to which the packet is to be sent. 
This option is used to filter all packets to a specific IP address or a group of IP addresses. 
When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the dest_wildcard parameter.

**dest_wildcard**
This option is used in conjunction with the dest_address option to specify a group of addresses for which packets are to be filtered. 
The mask must be entered as a complement:
  - Zero-bits in this parameter mean that the corresponding bits configured for the dest_address parameter must be identical.
  - One-bits in this parameter mean that the corresponding bits configured for the dest_address parameter must be ignored.
eq dest_port

Specifies a single, specific destination TCP port number to be filtered.
dest_port must be configured to an integer value from 0 to 65535.

gt dest_port

Specifies that all destination TCP port numbers greater than the one specified are to be filtered.
dest_port must be configured to an integer value from 0 to 65535.

lt dest_port

Specifies that all destination TCP port numbers less than the one specified are to be filtered.
dest_port must be configured to an integer value from 0 to 65535.

neq dest_port

Specifies that all destination TCP port numbers not equal to the one specified are to be filtered.
dest_port must be configured to an integer value from 0 to 65535.

range start_dest_port end_dest_port

Specifies that all destination TCP ports within a specific range are to be filtered.
start_dest_port is the initial port in the range and end_dest_port is the final port in the range.
Both start_dest_port and end_dest_port can be configured to an integer value from 0 to 65535.

Usage

Block IP packets when the source and destination are of interest but for only a limited set of ports.

**Important:** The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*.

Example

The following command defines a rule definition that redirects packets to the charging service named chgsvcl, and UDP packets coming from any host are matched:

```
redirect css service chgsvcl uplink udp any
```

The following sets the insertion point before the rule definition above:

```
before redirect css service chgsvcl uplink udp any
```

The following command sets the insertion point after the first rule definition above:

```
after redirect css service chgsvcl uplink udp any
```

The following deletes the rule definition above:

```
no redirect css service chgsvcl uplink udp any
```
redirect nexthop (by IP address masking)

Redirects subscriber sessions based on the IP address mask sent by the source to the mobile node or the network.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > ACL Configuration

configure > context context_name > ip access-list acl_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-acl)#

Syntax

redirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ]
source_address source_wildcard

after redirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ]
source_address source_wildcard

before redirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ]
source_address source_wildcard

no redirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ]
source_address source_wildcard

after
Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

Important: If the options specified do not exactly match an existing rule, the insertion point does not change.

before
Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

Important: If the options specified do not exactly match an existing rule, the insertion point does not change.
**redirect nexthop (by IP address masking)**

- **no**
  Removes the rule which exactly matches the options specified.

- **nexthop** *nexthop_addr*
  The directly connected IP address to which the IP packets are forwarded.

- **context** *context_id*
  The context identification number of the context to which packets are redirected. At the executive mode prompt, use the `show context all` command to display context names and context IDs.

- **interface** *interface_name*
  The name of the logical interface to which the packets should be redirected. *interface_name* must be an alphanumeric string from 1 to 79 characters.

- **log**
  Default: packets are not logged.
  Indicates all packets which match the redirect are to be logged.

- **source_address**
  The IP address(es) from which the packet originated. This option is used to filter all packets from a specific IP address or a group of IP addresses. When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the `source_wildcard` parameter.

- **source_wildcard**
  This option is used in conjunction with the `source_address` option to specify a group of addresses for which packets are to be filtered. The mask must be entered as a complement:
  - Zero-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be identical.
  - One-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be ignored.

**Important**: The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.

**Usage**
Define a rule when any packet from the IP addresses which fall into the group of addresses matching the IP address masking. This allows the reduction of redirect rules as it does not require a rule for each source and destination pair.

**Important**: The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*. 

---

*Cisco ASR 5x00 Command Line Interface Reference*
**Important:** Also note that “redirect” rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

**Example**

The following command defines a rule that redirects packets to the next hop host at 192.168.10.4, the context with the context ID of 23 and the source IP and wildcard of 192.168.22.0 and 0.0.0.31:

```plaintext
redirect nexthop 192.168.10.4 context 23 198.162.22.0 0.0.0.31
```

The following sets the insertion point before the rule defined above:

```plaintext
before redirect nexthop 192.168.10.4 context 23 198.162.22.0 0.0.0.31
```

The following command sets the insertion point after the first rule defined above:

```plaintext
after redirect nexthop 192.168.10.4 context 23 198.162.22.0 0.0.0.31
```

The following deletes the first rule defined above:

```plaintext
no redirect nexthop 192.168.10.4 context 23 198.162.22.0 0.0.0.31
```
redirect nexthop (any)

Redirects subscriber sessions based on any packet received. This command is also used to set the access control list insertion point.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > ACL Configuration

`configure > context context_name > ip access-list acl_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-acl)#
```

**Syntax**

```
redirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ]
any
```

```
after redirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ]
any
```

```
before redirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ]
any
```

```
no redirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ]
any
```

---

**after**
Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

---

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

---

**before**
Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

---

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.
no
Removes the rule which exactly matches the options specified.

nexthop  nexthop_addr
The directly connected IP address to which the IP packets are forwarded.

context  context_id
The context identification number of the context to which packets are redirected. At the executive mode prompt, use the show context all command to display context names and context IDs.

interface  interface_name
The name of the logical interface to which the packets should be redirected. interface_name must be an alphanumeric string from 1 to 79 characters.

log
Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

any
Indicates all packets will match the redirect regardless of source and/or destination.

Usage
Define a catch all rule to place at the end of the list of rules to provide explicit handling of rules which do not fit any other criteria.

**Important:** Any rule which is added to be a catch all should also have the log option specified. The logged packets may be used to determine if the current list of rules is adequate or needs modification to ensure proper security.

**Important:** The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the Engineering Rules appendix in the System Administration Guide.

**Important:** Also note that “redirect” rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example
The following command defines a rule that redirects packets to the next hop host at 192.168.10.4, the context with the context ID of 23 and any source IP:

```
redirect nexthop 192.168.10.4 context 23 any
```

The following sets the insertion point before the rule defined above:

```
before redirect nexthop 192.168.10.4 context 23 any
```

The following command sets the insertion point after the first rule defined above:
after redirect nexthop 192.168.10.4 context 23 any

The following deletes the first rule defined above:

no redirect nexthop 192.168.10.4 context 23 any
redirect nexthop (by host IP address)

Redirects subscriber sessions based on the targeted host IP address sent by the source to the mobile node or the network.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > ACL Configuration

`configure > context context_name > ip access-list acl_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-acl)#
```

**Syntax**

```
redirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ]
host source_ipv4_address

after redirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ]
host source_ipv4_address

before redirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ]
host source_ipv4_address

no redirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ]
host source_ipv4_address
```

**after**
Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

**before**
Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.
no
Removes the rule which exactly matches the options specified.

nexthop  nexthop_addr
The directly connected IP address to which the IP packets are forwarded.

custom  context_id
The context identification number of the context to which packets are redirected. At the executive mode prompt, use the show context all command to display context names and context IDs.

interface  interface_name
The name of the logical interface to which the packets should be redirected. interface_name must be an alphanumeric string from 1 to 79 characters.

log
Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

host
Specifies that the rule applies to a specific host as determined by its IP address.
	source_ipv4_address
The IP address of the source host to filter against expressed in IPv4 dotted-decimal notation.

Usage
Define a rule when a very specific remote host is to be blocked. In simplified networks where the access controls need only block a few hosts, this command allows the rules to be very clear and concise.

Important: The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the Engineering Rules appendix in the System Administration Guide.

Important: Also note that “redirect” rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example
The following command defines a rule that redirects packets to the next hop host at 192.168.10.4, the context with the context ID of 23 and a host IP address of 192.168.200.11:

    redirect nexthop 192.168.10.4 context 23 host 192.168.200.11

The following sets the insertion point before the rule defined above:

    before redirect nexthop 192.168.10.4 context 23 host 192.168.200.11

The following command sets the insertion point after the first rule defined above:
after redirect nexthop 192.168.10.4 context 23 host 192.168.200.11

The following deletes the first rule defined above:

no redirect nexthop 192.168.10.4 context 23 host 192.168.200.11
redirect nexthop (by source ICMP packets)

Redirects subscriber sessions based on the internet control message protocol packets sent by the source to the mobile node or the network.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > ACL Configuration

```
configure > context context_name > ip access-list acl_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ac)#
```

**Syntax**

```
redirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ]
icmp { source_address source_wildcard | any | host source_host_address } { dest_address dest_wildcard | any | host dest_host_address } [ icmp_type [ icmp_code ] ]
```

```
after redirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ]
icmp { source_address source_wildcard | any | host source_host_address } { dest_address dest_wildcard | any | host dest_host_address } [ icmp_type [ icmp_code ] ]
```

```
before redirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ]
icmp { source_address source_wildcard | any | host source_host_address } { dest_address dest_wildcard | any | host dest_host_address } [ icmp_type [ icmp_code ] ]
```

```
no redirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ]
icmp { source_address source_wildcard | any | host source_host_address } { dest_address dest_wildcard | any | host dest_host_address } [ icmp_type [ icmp_code ] ]
```

---

**after**

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

---

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

---

**before**

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.
**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

```markdown
no
```
Removes the rule which exactly matches the options specified.

```markdown
nexthop nexthop_addr
```
The directly connected IP address to which the IP packets are forwarded.

```markdown
context context_id
```
The context identification number of the context to which packets are redirected. At the executive mode prompt, use the `show context all` command to display context names and context IDs.

```markdown
interface interface_name
```
The name of the logical interface to which the packets should be redirected. `interface_name` must be an alphanumeric string from 1 through 79 characters.

```markdown
log
```
Default: packets are not logged. Indicates all packets which match the redirect are to be logged.

```markdown
source_address
```
The IP address(es) from which the packet originated. This option is used to filter all packets from a specific IP address or a group of IP addresses. When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the `source_wildcard` parameter.

```markdown
source_wildcard
```
This option is used in conjunction with the `source_address` option to specify a group of addresses for which packets are to be filtered. The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.

```markdown
any
```
Specifies that the rule applies to all packets.

```markdown
host
```
Specifies that the rule applies to a specific host as determined by its IP address.
**redirect nexthop (by source ICMP packets)**

*source_host_address*

The IP address of the source host to filter against expressed in IPv4 dotted-decimal notation.

*dest_host_address*

The IP address of the destination host to filter against expressed in IPv4 dotted-decimal notation.

*dest_address*

The IP address(es) to which the packet is to be sent. This option is used to filter all packets to a specific IP address or a group of IP addresses. When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the *dest_wildcard* parameter.

*dest_wildcard*

This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered. The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.

*icmp_type*

Specifies that all ICMP packets of a particular type are to be filtered. The type can be an integer value between 0 and 255.

*icmp_code*

Specifies that all ICMP packets of a particular code are to be filtered. The type can be an integer value between 0 and 255.

**Usage**

Define a rule to block ICMP packets which can be used for address resolution and possible be a security risk. The IP redirecting allows flexible controls for pairs of individual hosts or groups by IP masking which allows the redirecting of entire subnets if necessary.

**Important:** The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*.

**Important:** Also note that “redirect” rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.
Example

The following command defines a rule that redirects packets to the next hop host at 192.168.10.4, the context with the context ID of 23, and ICMP packets coming from the host with the IP address 198.162.100.25:

```
redirect nexthop 192.168.10.4 context 23 icmp host 192.168.100.25
```

The following sets the insertion point before the rule defined above:

```
before redirect nexthop 192.168.10.4 context 23 icmp host 192.168.100.25
```

The following command sets the insertion point after the first rule defined above:

```
after redirect nexthop 192.168.10.4 context 23 icmp host 192.168.100.25
```

The following deletes the first rule defined above:

```
no redirect nexthop 192.168.10.4 context 23 icmp host 192.168.100.25
```
redirect nexthop (by IP packets)

Redirects subscriber sessions based on the internet protocol packets sent by the source to the mobile node or the network.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > ACL Configuration

```
configure > context context_name > ip access-list acl_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-acl)#
```

**Syntax**

```
redirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ]
ip { source_address source_wildcard | any | host source_host_address } { dest_address dest_wildcard | any | host dest_host_address } [ fragment ] [ protocol num ]
```

```
after redirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ]
ip { source_address source_wildcard | any | host source_host_address } { dest_address dest_wildcard | any | host dest_host_address } [ fragment ] [ protocol num ]
```

```
before redirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ]
ip { source_address source_wildcard | any | host source_host_address } { dest_address dest_wildcard | any | host dest_host_address } [ fragment ] [ protocol num ]
```

```
no redirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ]
ip { source_address source_wildcard | any | host source_host_address } { dest_address dest_wildcard | any | host dest_host_address } [ fragment ] [ protocol num ]
```

---

**after**

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

---

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

---

**before**

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.
**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

- **no**
  Removes the rule which exactly matches the options specified.

- **nexthop nexthop_addr**
  The directly connected IP address to which the IP packets are forwarded.

- **context context_id**
  The context identification number of the context to which packets are redirected. At the executive mode prompt, use the `show context all` command to display context names and context IDs.

- **interface interface_name**
  The name of the logical interface to which the packets should be redirected. `interface_name` must be an alphanumeric string from 1 through 79 characters.

- **log**
  Default: packets are not logged.
  Indicates all packets which match the redirect are to be logged.

- **source_address**
  The IP address(es) from which the packet originated.
  This option is used to filter all packets from a specific IP address or a group of IP addresses. When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the `source_wildcard` parameter.

- **source_wildcard**
  This option is used in conjunction with the `source_address` option to specify a group of addresses for which packets are to be filtered.
  The mask must be entered as a complement:
  - Zero-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be identical.
  - One-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.

- **any**
  Specifies that the rule applies to all packets.

- **host**
  Specifies that the rule applies to a specific host as determined by its IP address.
redirect nexthop (by IP packets)

source_host_address
The IP address of the source host to filter against expressed in IPv4 dotted-decimal notation.

dest_host_address
The IP address of the destination host to filter against expressed in IPv4 dotted-decimal notation.

dest_address
The IP address(es) to which the packet is to be sent.
This option is used to filter all packets to a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the dest_wildcard parameter.

dest_wildcard
This option is used in conjunction with the dest_address option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:
- Zero-bits in this parameter mean that the corresponding bits configured for the dest_address parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the dest_address parameter must be ignored.

Important: The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.

fragment
Indicates packet redirection is to be applied to IP packet fragments only.

protocol num
Indicates that the packet filtering is to be applied to a specific protocol number.
num can be an integer ranging from 0 to 255.

Usage
Block IP packets when the source and destination are of interest.

Important: The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the Engineering Rules appendix in the System Administration Guide.

Important: Also note that “redirect” rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example
The following command defines a rule that redirects packets to the next hop host at 192.168.10.4, the context with the context ID of 23, and IP packets coming from the host with the IP address 192.168.100.25, and fragmented packets for any destination are matched:

```
redirect nexthop 192.168.10.4 context 23 ip host 192.168.100.25 any fragment
```

The following sets the insertion point before the rule defined above:

```
before redirect nexthop 192.168.10.4 context 23 ip host 192.168.100.25 any fragment
```

The following sets the insertion point after the first rule defined above:

```
after redirect nexthop 192.168.10.4 context 23 ip host 192.168.100.25 any fragment
```

The following deletes the first rule defined above:

```
no redirect nexthop 192.168.10.4 context 23 ip host 192.168.100.25 any fragment
```
redirect nexthop (by TCP/UDP packets)

Redirects subscriber sessions based on the transmission control protocol/user datagram protocol packets sent by the source to the mobile node or the network.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > ACL Configuration

```acl
configure > context context_name > ip access-list acl_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-acl)#
```

**Syntax**

```acl
redirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ] { tcp | udp } { { source_address source_wildcard | any | host source_host_address } [ eq source_port | gt source_port | lt source_port | neq source_port ] } { { dest_address dest_wildcard | any | host dest_host_address } [ eq dest_port | gt dest_port | lt dest_port | neq dest_port ] }
```

```acl
after redirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ] { tcp | udp } { { source_address source_wildcard | any | host source_host_address } [ eq source_port | gt source_port | lt source_port | neq source_port ] } { { dest_address dest_wildcard | any | host dest_host_address } [ eq dest_port | gt dest_port | lt dest_port | neq dest_port ] }
```

```acl
before redirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ] { tcp | udp } { { source_address source_wildcard | any | host source_host_address } [ eq source_port | gt source_port | lt source_port | neq source_port ] } { { dest_address dest_wildcard | any | host dest_host_address } [ eq dest_port | gt dest_port | lt dest_port | neq dest_port ] }
```

```acl
no redirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ] { tcp | udp } { { source_address source_wildcard | any | host source_host_address } [ eq source_port | gt source_port | lt source_port | neq source_port ] } { { dest_address dest_wildcard | any | host dest_host_address } [ eq dest_port | gt dest_port | lt dest_port | neq dest_port ] }
```

**after**

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed. This moves the insertion point to immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.
**before**

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

---

**no**

Removes the rule which exactly matches the options specified.

---

**nexthop**  *nexthop_addr*

The directly connected IP address to which the IP packets are forwarded.

---

**context**  *context_id*

The context identification number of the context to which packets are redirected. At the executive mode prompt, use the `show context all` command to display context names and context IDs.

---

**interface**  *interface_name*

The name of the logical interface to which the packets should be redirected.  *interface_name* must be an alphanumeric string from 1 through 79 characters.

---

**log**

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

---

**tcp | udp**

Specifies the redirect is to be applied to IP based transmission control protocol or the user datagram protocol.

- **tcp**: Redirect applies to TPC packets.
- **udp**: Redirect applies to UDP packets.

---

**source_address**

The IP address(es) from which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the `source_wildcard` parameter.

---

**source_wildcard**

This option is used in conjunction with the `source_address` option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be ignored.
**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>any</em></td>
<td>Specifies that the rule applies to all packets.</td>
</tr>
<tr>
<td><em>host</em></td>
<td>Specifies that the rule applies to a specific host as determined by its IP address.</td>
</tr>
<tr>
<td><em>source_host_address</em></td>
<td>The IP address of the source host to filter against expressed in IPv4 dotted-decimal notation.</td>
</tr>
<tr>
<td><em>dest_host_address</em></td>
<td>The IP address of the destination host to filter against expressed in IPv4 dotted-decimal notation.</td>
</tr>
<tr>
<td><em>eq source_port</em></td>
<td>Specifies a single, specific source TCP port number to be filtered. <em>source_port</em> must be an integer from 0 through 65535.</td>
</tr>
<tr>
<td><em>gt source_port</em></td>
<td>Specifies that all source TCP port numbers greater than the one specified are to be filtered. <em>source_port</em> must be an integer from 0 through 65535.</td>
</tr>
<tr>
<td><em>lt source_port</em></td>
<td>Specifies that all source TCP port numbers less than the one specified are to be filtered. <em>source_port</em> must be an integer from 0 through 65535.</td>
</tr>
<tr>
<td><em>neq source_port</em></td>
<td>Specifies that all source TCP port numbers not equal to the one specified are to be filtered. <em>source_port</em> must be an integer from 0 through 65535.</td>
</tr>
<tr>
<td><em>dest_address</em></td>
<td>The IP address(es) to which the packet is to be sent. This option is used to filter all packets to a specific IP address or a group of IP addresses. When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the <em>dest_wildcard</em> parameter.</td>
</tr>
<tr>
<td><em>dest_wildcard</em></td>
<td>This option is used in conjunction with the <em>dest_address</em> option to specify a group of addresses for which packets are to be filtered. The mask must be entered as a complement: <em>Zero-bits in this parameter mean that the corresponding bits configured for the <em>dest_address</em> parameter must be identical.</em></td>
</tr>
</tbody>
</table>
• One-bits in this parameter mean that the corresponding bits configured for the `dest_address` parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>eq dest_port</td>
<td>Specifies a single, specific destination TCP port number to be filtered. dest_port must be an integer from 0 through 65535.</td>
</tr>
<tr>
<td>gt dest_port</td>
<td>Specifies that all destination TCP port numbers greater than the one specified are to be filtered. dest_port must be an integer from 0 through 65535.</td>
</tr>
<tr>
<td>lt dest_port</td>
<td>Specifies that all destination TCP port numbers less than the one specified are to be filtered. dest_port must be an integer from 0 through 65535.</td>
</tr>
<tr>
<td>neq dest_port</td>
<td>Specifies that all destination TCP port numbers not equal to the one specified are to be filtered. dest_port must be an integer from 0 through 65535.</td>
</tr>
</tbody>
</table>

**Usage**
Block IP packets when the source and destination are of interest but for only a limited set of ports.

**Important:** The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*.

**Important:** Also note that “redirect” rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

**Example**
The following command defines a rule that redirects packets to the next hop host at 192.168.10.4, the context with the context ID of 23, and UDP packets coming from any host are matched:

```
redirect nexthop 192.168.10.4 context 23 udp any
```

The following sets the insertion point before the rule defined above:

```
before redirect nexthop 192.168.10.4 context 23 udp any
```

The following command sets the insertion point after the first rule defined above:

```
after redirect nexthop 192.168.10.4 context 23 udp any
```

The following deletes the first rule defined above:
no redirect nexthop 192.168.10.4 context 23 udp any
Chapter 6
ACS Bandwidth Policy Configuration Mode Commands

The ACS Bandwidth Policy Configuration Mode is used to create and manage Active Charging Service (ACS) Bandwidth Policies.

**Mode**

Exec > ACS Configuration > Bandwidth Policy Configuration

`active-charging service service_name > bandwidth-policy policy_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-bandwidth-policy)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
down
```

**Usage**

Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
exit
```

Usage
Use this command to return to the parent configuration mode.
flow limit-for-bandwidth

This command allows you to configure the flow limit-for-bandwidth parameter for the current bandwidth policy.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Bandwidth Policy Configuration

```
active-charging service service_name > bandwidth-policy policy_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-bandwidth-policy)#
```

**Syntax**

```
flow limit-for-bandwidth id bandwidth_id group-id group_id

no flow limit-for-bandwidth id bandwidth_id
```

**Usage**

Use this command to configure the flow limit-for-bandwidth configuration for a bandwidth policy.

**Example**

The following command configures the Flow Limit-for-Bandwidth configuration with bandwidth policy ID test123 and group ID 123:

```
flow limit-for-bandwidth id test123 group-id 123
```
**group-id**

This command allows you to configure the group ID for the current bandwidth policy.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Bandwidth Policy Configuration

active-charging service service_name > bandwidth-policy policy_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-bandwidth-policy)#

**Syntax**

```
group-id  group_id  direction { downlink | uplink }  peak-data-rate  peak_data_rate  peak-burst-size  peak_burst_size  violate-action { discard | lower-ip-precedence }  [ committed-data-rate  committed_data_rate  committed-burst-size  committed_burst_size  [ exceed-action { discard | lower-ip-precedence } ] ]  

{ default | no }  group-id  group_id  direction { downlink | uplink }  
```

**default**

Configures this command with default settings for the specified group ID.

**no**

If previously configured, removes the specified group ID configuration from the current bandwidth policy.

**group_id**

 Specifies the group ID.

`group_id` must be an integer from 1 through 65535.

**direction { downlink | uplink }**

Specifies the direction for which bandwidth will be controlled.

**peak-data-rate peak_data_rate**

Specifies the peak data rate, in bits per second.

`peak_data_rate` must be an integer from 1 through 4294967295.

Default: 0

**peak-burst-size peak_burst_size**

Specifies the peak burst size, in bytes.

`peak_burst_size` must be an integer from 1 through 4294967295.

Default: 0
**ACS Bandwidth Policy Configuration Mode Commands**

- **group-id**
  - **violate-action { discard | lower-ip-precedence }**
    - Specifies the action to be taken if Peak Data Rate is surpassed.
      - **discard**: Specifies to discard the packet.
      - **lower-ip-precedence**: Specifies to lower IP precedence of the packet.
  - **committed-data-rate committed_data_rate**
    - Specifies the committed Data Rate, in bits per second. This can also be used to specify the Guaranteed Bit Rate (GBR) for Network Controlled QoS (NCQoS) without exceed-action.
    - `committed_data_rate` must be an integer from 1 through 4294967295.
    - Default: 0
  - **committed-burst-size committed_burst_size**
    - Specifies the committed burst size, in bytes.
    - `committed_burst_size` must be an integer from 1 through 4294967295.
    - Default: 0
  - **exceed-action { discard | lower-ip-precedence }**
    - Specifies the action to be taken if Committed Data Rate is surpassed.
      - **discard**: Specifies to discard the packet.
      - **lower-ip-precedence**: Specifies to lower IP precedence of the packet.

**Usage**

Use this command to configure the Group ID for an bandwidth policy.

**Example**

The following command configures the group ID 111 to control bandwidth in the downlink direction specifying peak data rate of 10000 bits per second and peak burst size of 10000 bytes while specifying the action to be taken on violation as discard:

```
group-id 111 direction downlink peak-data-rate 10000 peak-burst-size 10000 violate-action discard
```
Chapter 7
ACS Charging Action Configuration Mode Commands

The ACS Charging Action Configuration Mode is used to configure Active Charging Service (ACS) charging actions.

Mode

Exec > ACS Configuration > Charging Action Configuration

`active-charging service service_name > charging-action charging_action_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-charging-action)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
allocation-retention-priority

This command allows you to configure the Allocation Retention Priority (ARP).

**Product**

All

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > ACS Configuration > Charging Action Configuration

```
active-charging service service_name > charging-action charging_action_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name (config-charging-action)#
```

**Syntax**

```
allocation-retention-priority priority [pci pci_value | pvi pvi_value ]
```

```
no allocation-retention-priority
```

- **no**
  
  If previously configured, disables ARP configuration in the current charging action.

- **priority**
  
  `priority` must be an integer from 1 through 15.

- **pci **pci_value**
  
  Specifies the Pre-emption Capability Indicator (PCI).

  `pci_value` must be integer 0 or 1.

  **Important:** If not explicitly enabled, then the default value of 1 will hold true.

- **pvi** pvi_value
  
  Specifies the Pre-emption Vulnerability Indicator (PVI).

  `pvi_value` must be integer 0 or 1.

  **Important:** If not explicitly enabled, then the default value of 0 will hold true.

**Usage**

This command configures the ARP, which indicates the priority of allocation and retention of the service data flow. The ARP resolves conflicts in demand for network resources. At the time of resource crunch, this parameter prioritizes allocation of resources during bearer establishment and modification. In a congestion...
situation, a lower ARP flow may be dropped to free up capacity. Once a service flow is successfully established, this parameter plays no role in quality of service (QoS) experienced by the flow.

Example

The following command sets the ARP to 10:

```
allocation-retention-priority 10
```
billing-action

This command allows you to configure the billing action for packets that match specific rule definitions (ruledefs).

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Charging Action Configuration

```
active-charging service service_name > charging-action charging_action_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-charging-action)#
```

**Syntax**

In StarOS 12.2 and later releases:

```
billing-action { create-edrs { charging-edr charging_edr_format_name | reporting-edr reporting_edr_format_name } | wait-until-flow-ends | egcdr | exclude-from-udrs | radius | rf } +
```

```
no billing-action [ create-edrs | egcdr | exclude-from-udrs | radius | rf ] +
```

In StarOS 12.1 and earlier releases:

```
billing-action { edr edr_format_name [ wait-until-flow-ends ] | egcdr | exclude-from-udrs | radius | rf } +
```

```
no billing-action [ edr | egcdr | exclude-from-udrs | radius | rf ] +
```

**Important:** This option is available only in 12.1 and earlier releases. In 12.2 and later releases, it is deprecated and is replaced by the `create-edrs charging-edr` option.

```
edr edr_format_name [ wait-until-flow-ends ]
```

**Important:** Enables EDR billing for packets matching this charging action. `edr_format_name` must be the name of an existing EDR format, and must be an alphanumeric string of 1 through 63 characters.

**Important:** If the EDR format name specified here is not configured in the EDR Format Configuration Mode, or has been deleted, the system accepts it without applying any EDR format for the billing action in this ACS service.
If this option is configured, the system generates an EDR immediately when a packet is received and it matches a ruledef that is associated with this charging action. Other events configured for flow end-condition, flow action, termination, and/or session control also create the triggers for EDR generation.

**wait-until-flow-ends:** By default, the EDR is generated immediately after a ruledef hit results in this charging action. When this keyword is specified, no EDR is generated on a ruledef hit. When the flow ends, an attempt is made to generate an EDR with the format specified.

```plaintext
create-edrs { charging-edr charging_edr_format_name | reporting-edr reporting_edr_format_name } + [ wait-until-flow-ends ]
```

**Important:** This option is available only in 12.2 and later releases.

Enables EDR billing for packets matching this charging action.

- **charging-edr charging_edr_format_name:** Specifies to generate charging EDR.  
  
  *charging_edr_format_name* must be the name of a charging EDR format, and must be an alphanumeric string of 1 through 63 characters.

- **reporting-edr reporting_edr_format_name:** Specifies to generate reporting EDR.  
  
  *reporting_edr_format_name* must be the name of a reporting EDR format, and must be an alphanumeric string of 1 through 63 characters.

If the above options are configured, the system generates an EDR immediately when a packet is received and it matches a ruledef that is associated with this charging action. Other events configured for flow end-condition, flow action, termination, and/or session control also creates the triggers for EDR generation.

- **wait-until-flow-ends:** By default, the EDR is generated immediately after a ruledef hit results in this charging action. When this keyword is specified, no EDR is generated on a ruledef hit. When the flow ends, an attempt is made to generate an EDR with the format specified.

**egcdr**

Enables eG-CDR billing for packets matching this charging action.

If this option is configured, the system generates an eG-CDR when the subscriber session ends or an interim trigger condition occurs. The interim triggers are configurable in the ACS Rulebase Configuration Mode. In addition, whenever there is an SGSN-to-SGSN handoff the system treats that as a trigger.

To generate an eG-CDR the **accounting-mode** command in the APN Configuration Mode must be configured with the “none” option.

The format of enhanced G-CDRs is controlled by the **inspector** CLI command in the Context Configuration Mode.

**exclude-from-udrs**

By default, statistics are accumulated on a per content ID basis for possible inclusion in UDRs. The **exclude-from-udrs** keyword causes the system to not include the packet’s statistics in UDRs.

When this option is disabled, (the default setting) UDRs will be generated based on the UDR format specified in the rulebase.

Default: Disabled.

**radius**

Enables billing action as RADIUS Charging Data Records (CDRs) for packets matching this charging action, and the data packet statistics will be included in the postpaid RADIUS accounting.

Default: Disabled.
rf

Enables Rf accounting.
Rf accounting is applicable only for dynamic and predefined rules that are marked for it. Dynamic rules have a field offline-enabled to indicate this. To mark a predefined rule as offline-enabled, use this keyword and the billing-records CLI in the ACS Rulebase Configuration Mode.

Usage

Use this command to enable an EDR, eG-CDR and/or RADIUS CDR type of billing for content matching this charging action.

Example

In 12.1 and earlier releases, the following command enables the EDR billing type with EDR format chargel_format:

```
billing-action edr chargel_format
```

In 12.2 and later releases, the following command is applied to both charging and reporting EDRs since the trigger for both the EDRs is the same:

```
billing-action create-edrs charging-edr charging_edrformat1 reporting-edr reporting_edrformat1 wait-until-flow-ends
```
CCA Charging Credit

This command allows you to enable/disable Credit Control Application (CCA) and configure the RADIUS/Diameter prepaid charging behavior.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Charging Action Configuration

```
active-charging service service_name > charging-action charging_action_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-charging-action)#
```

**Syntax**

```
cca charging credit [ rating-group coupon_id ] [ preemptively-request ]
{ default | no } cca charging
```

- **no**
  If previously configured, disables RADIUS/Diameter Prepaid Credit Control Charging in the current charging action.

- **default**
  Disables RADIUS/Diameter Prepaid Credit Control Charging.

- **credit**
  Specifies RADIUS/Diameter Prepaid Credit Control Charging Credit behavior.

- **preemptively-request**
  Specifies RADIUS/Diameter prepaid credit preemptively requested charging credit behavior. If this option is used, a quota is requested for the specific type of content during session initialization.

- **rating-group coupon_id**
  Specifies the coupon ID used in prepaid charging as rating-group which maps to the coupon ID for prepaid customer.

  - coupon_id must be an integer from 0 through 65535.

  This option also assigns different content-types for the same charging action depending upon whether or not prepaid is enabled.

**Important:** This rating-group overrides the content ID, if present in the same charging-action for the prepaid customer in Diameter Credit Control Application (DCCA). But only the content IDs will be used in eG-CDRs irrespective of the presence of rating-group in that charging action.
Usage

Use this command to configure RADIUS/Diameter Prepaid Credit Control Charging behavior. This command selects reservation based credit control. A CCR-Initial is used to reserve quota upon the first traffic, then a series of CCR-updates are issued as the traffic proceeds and quota dwindles. A CCR-Terminate is issued at the end of the session or at the end of the quota-hold-time.

Example

The following is an example of this command:

```
cca charging credit
```
charge-units

This command allows you to configure the charge units for RADIUS/DCCA charging calculation.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Charging Action Configuration

```
active-charging service service_name > charging-action charging_action_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-charging-action)#
```

**Syntax**

```
charge-units units

{ default | no } charge-units

default

Configures this command with its default setting.
Default: 0; disables the counter, same as no charge-units

no

If previously configured, disables the charge-units configuration in the current charging action.

units

Specifies the service-specific fixed unit counter per content ID for RADIUS/DCCA charging.

units is the value set for charging unit, and must be an integer from 1 through 65535.

**Usage**

This command configures the unit amount counters for charging calculation on per content ID basis for different protocols and packets regardless of packet direction (uplink or downlink).

**Important:** For more information on content ID, refer to the if-protocol command in the ACS Ruledef Configuration Mode Commands chapter.

**Example**

The following command sets the charging unit to 1024:

```
charge-units 1024
```
charge-volume

This command allows you to configure how the volume amount counter for eG-CDRs, UDRs, and DCCA charging are calculated.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Charging Action Configuration

active-charging service service_name > charging-action charging_action_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-charging-action)#

Syntax

charge-volume { { dns | ftp-control | ftp-data | http | icmp | imap | ip | mms | pop3 | pptp | rtcp | rtp | rtsp | sdp | secure-http | sip | smtp | tcp | tftp | udp | wap | wtp } { bytes | packet-length | packets } [ downlink | uplink ] | constant fixed_value }

{ default | no } charge-volume

default

Configures this command with its default setting.
Default: charge-volume ip bytes

no

If previously configured, deletes the charge-volume configuration in the current charging action.

{ dns | ftp-control | ftp-data | http | icmp | imap | ip | mms | pop3 | pptp | rtcp | rtp | rtsp | sdp | secure-http | sip | smtp | tcp | tftp | udp | wap | wtp }

Specifies the charge volume method for the specific rule definition.

• dns: Charge volume for DNS
• ftp-control: Charge volume for FTP-Control
• ftp-data: Charge volume for FTP-Data
• http: Charge volume for HTTP
• icmp: Charge volume for ICMP
• imap: Charge volume for Internet Message Access Protocol (IMAP)
• ip: Charge volume for IP
• mms: Charge volume for MMS
• pop3: Charge volume for POP3
• pptp: Charge volume for PPTP
 ACS Charging Action Configuration Mode Commands

- **rtcp**: Charge volume for RTCP
- **rtp**: Charge volume for RTP
- **rtsp**: Charge volume for RTSP
- **sdp**: Charge volume for SDP
- **secure-http**: Charge volume for secure-https
- **sip**: Charge volume for SIP
- **smtp**: Charge volume for SMTP
- **tcp**: Charge volume for TCP
- **tftp**: Charge volume for TFTP
- **udp**: Charge volume for UDP
- **wsp**: Charge volume for WSP
- **wtp**: Charge volume for WTP

**bytes**
Sets charge volume for bytes.

**packet-length**
Sets charge volume for packet length.

**packets**
Sets charge volume for packets.

**constant** *fixed_value*
This sets the fixed increment value for charging.

*fixed_value* is the value set for charging, and must be an integer from 0 through 65535.
If **constant** 3 is configured for every invocation of this Charging Action, the system adds 3 to the
downlink/uplink volume counter, depending on the direction of packet.

**Usage**
This command provides the method for charging volume calculation for different protocols and packets.
For information on supported protocols see the *ACS Ruledef Configuration Mode Commands* chapter.
If **charge-volume rtp packets** is configured, system computes volume amounts for different options for
RTP as follows:

<table>
<thead>
<tr>
<th>Volume</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Volume amount</td>
<td>Total (downlink and uplink) RTP packets</td>
</tr>
<tr>
<td>Volume amount uplink</td>
<td>Uplink RTP packets</td>
</tr>
<tr>
<td>Volume amount downlink</td>
<td>Downlink RTP packets</td>
</tr>
<tr>
<td>Volume amount uplink packets</td>
<td>Uplink RTP packets</td>
</tr>
<tr>
<td>Volume amount downlink packets</td>
<td>Downlink RTP packets</td>
</tr>
<tr>
<td>Volume amount uplink bytes</td>
<td>Uplink RTP bytes</td>
</tr>
</tbody>
</table>
### ACS Charging Action Configuration Mode Commands

**charge-volume**

<table>
<thead>
<tr>
<th>Volume</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Volume amount downlink bytes</td>
<td>Downlink RTP bytes</td>
</tr>
</tbody>
</table>

**Important:** Whenever service counts volume, it counts all packets that the relevant analyzers accepted.

**Important:** If a TCP packet is routed to the HTTP analyzer but there is no HTTP payload, then the TCP statistics will be updated but the HTTP statistics will not be updated (except for the “packets ignored by the HTTP analyzer” statistic).

**Example**

The following command sets the charging volume of downlink packets for RTP:

```
charge-volume rtp packets downlink
```
content-filtering processing server-group

This command allows you to enable/disable Category-based Content Filtering.

**Product**
CF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Charging Action Configuration

```
active-charging service service_name > charging-action charging_action_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-charging-action)#
```

**Syntax**

```
content-filtering processing server-group

{ default | no } content-filtering processing
```

- **default**
  - Configures this command with its default setting.
  - Default: Content filtering configured for the rulebase is attempted

- **no**
  - Specifies to bypass content filtering.
  - This configuration should only be specified for charging actions that are performed when known safe sites are being accessed.

**Usage**

Use this command to enable or disable Category-based Content Filtering in the charging action.

This command works as second-level filter to process the HTTP/WAP GET request with Internet Content Adaptation Protocol (ICAP) after ruledef matching. The first-level filtering is in the rulebase configuration.

This CLI command is only effective when the `content-filtering mode server-group` command is configured in the rulebase.

**Example**

The following command enables content filtering in the current charging action:

```
content-filtering processing server-group
```
**content-id**

This command allows you to specify the content ID to use in the generated billing records, as well as the AVP used by the Credit Control Application, such as the “Rating-Group” AVP for use by the Diameter Credit Control Application (DCCA).

**Product**

All

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > ACS Configuration > Charging Action Configuration

```
active-charging service service_name > charging-action charging_action_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-charging-action)#
```

**Syntax**

```
content-id content_id
no content-id
```

- **no**
  
  Removes the content ID configuration from the charging action.

- **content_id**
  
  Specifies the content ID for credit control service.

  In 12.1 and earlier releases `content_id` must be an integer from 1 through 65535.

  In 12.2 and later releases, `content_id` must be an integer from 1 through 2147483647.

**Usage**

This command specifies an optional content ID to use in the generated billing records. This identifier assists the carrier’s billing post processing and also used by credit-control system to use independent quotas for different value of `content-id`. If the specified ruledef uses the `if-protocol` command to select a value for content ID, then the `content_id` specified through this command is not used for billing record generation.

**Important:** For more information on `content-id`, refer to the `if-protocol` command in the *ACS Ruledef Configuration Mode Commands* chapter.

**Example**

The following command sets the content ID in the current charging action to 23:

```
content-id 23
```
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
```
exit
```

**Usage**
Use this command to return to the parent configuration mode.
**flow action**

This command allows you to specify the action to take on packets that match rule definitions.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Charging Action Configuration

`active-charging service service_name > charging-action charging_action_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-charging-action)#
```

**Syntax**

In StarOS 12.2 and later releases:

```
flow action { conditional user-agent end-token end_token_name | discard [ downlink | uplink ] | random-drop interval interval_start to interval_end pkts-to-drop packet_min to packet_max | readaddress [ [ server ipv4_address/ipv6_address [ discard-on-failure ] [ dns-proxy-bypass ] ] [ port port_number [ discard-on-failure ] [ dns-proxy-bypass ] ] | server-list server_list_name [ hierarchy ] [ round-robin ] [ dns-proxy-bypass ] [ discard-on-failure ] ] | redirect-ocs-url | redirect-url redirect_url [ [ encryption { blowfish128 | blowfish64 } [ encrypted ] key key ] [ clear-quota-retry-timer ] [ first-request-only { post-redirect { allow | discard | terminate } } ] ] | rulebase-change rulebase_name | terminate-flow | terminate-session }
```

`no flow action`

In StarOS 12.1 and earlier releases:

```
flow action { conditional user-agent end-token end_token_name | discard [ downlink | uplink ] | random-drop interval interval_start to interval_end pkts-to-drop packet_min to packet_max | redirect-url redirect_url [ clear-quota-retry-timer ] | readaddress [ server ipv4_address/ipv6_address ] [ port port_number ] | terminate-flow | terminate-session }
```

`no flow action`

If previously configured, deletes the flow action configuration in the current charging action.

**conditional user-agent end-token end_token_name**

Specifies to conditionally redirect the HTTP packets matched to a configured user-agent to a specified URL. The user agent is configured using the `redirect user-agent` command in the ACS Configuration Mode. `end_token_name` must be an alphanumeric string of 1 through 32 characters, and is configured with this command to end the redirection condition.
flow action

discard [ downlink | uplink ]

Specifies to discard the specified packets.

- **downlink**: Downlink packets
- **uplink**: Uplink packets

If **downlink** or **uplink** keyword is not specified, both downlink and uplink packets will be discarded.

random-drop interval interval_start to interval_end pkts-to-drop packet_min to packet_max

Specifies to drop a group of consecutive packets (**pkts-to-drop**) to be dropped in the specified time interval (**random-drop interval**). This will cause degradation in user experience. P2P VoIP would need more than one packet to be dropped, since that type of protocol is geared to handle occasional single packet drops.

- **random-drop interval interval_start to interval_end**: Specifies the random drop interval, in seconds, at which the voice packets will be dropped. 
  
  *interval_start* and *interval_end* must be integers from 1 through 999.

- **pkts-to-drop packet_min to packet_max**: Specifies the number of voice packets to be dropped at a time in a flow when the packets have to be dropped. 
  
  *packet_min* and *packet_max* must be integers from 1 through 100.

readdress [ [ server ipv4_address/ipv6_address [ discard-on-failure ] [ dns-proxy-bypass ] ] ] [ port port_number [ discard-on-failure ] [ dns-proxy-bypass ] ] ] [ server-list server_list_name [ hierarchy ] [ round-robin ] [ discard-on-failure ] [ dns-proxy-bypass ] ] ]

Specifies to readdress the location of the uplink packets for charging action.

- **server ipv4_address/Ipv6**: Specifies the re-address server’s IPv4/IPv6 address.

- **port port_number**: Specifies the re-address server’s port number. 
  
  *port_number* must be an integer from 1 through 65535.

**Important**: You can optionally keep the original destination address and just change the destination TCP/UDP port number.

- **server-list server_list_name**

**Important**: This option is available only in StarOS 14.1 and later releases. This keyword is license dependent. For more information please contact your Cisco account representative.

Specifies to readdress the packet flow to the DNS servers configured under the server list. For more information about configuring the server list, see the **ACS Readdress Server List Configuration Mode** chapter.

- **discard-on-failure**

**Important**: This option is available only in StarOS 14.0 and later releases.
Specifies to discard the packets if readdressing fails due to duplicate key. If this keyword is not configured, no action is taken and the packets are allowed to pass.

If already configured, to revert the behavior, configure the `flow action readdress` command again without the `discard-on-failure` keyword.

- `dns-proxy-bypass`

  - **Important**: This option is available only in StarOS 12.3 and later releases.

  Specifies the DNS packets to bypass interception at the session manager when readdressing for flow occurs, and go through ECS-based DNS redirection. If this keyword is not configured, DNS redirection from ECS is disabled.

- `redirect-ocs-url`

  - **Important**: This option is available only in StarOS 12.3 and later releases.

  Specifies to redirect to the URL provided by OCS only for post-processing dynamic rules.

  ```
  redirect-url redirect_url [ [ encryption { blowfish128 | blowfish64 } [ encrypted ] key key ] [ clear-quota-retry-timer ] [ first-request-only [ post-redirect { allow | discard | terminate } ] ] ] ]
  ```

  Specifies to return a redirect response to the subscriber, and terminate the TCP connections (to the subscriber and server). The subscriber's Web browser should automatically send the original HTTP packet to the specified URL. Redirection is only possible for certain types of HTTP packets (for example, GET requests), which typically are only sent in the uplink direction. If the flow is not HTTP, the `redirect-url` option is ignored, that the packet is forwarded normally, except for SIP. For SIP, a Contact header with the redirect information is inserted.

- `redirect_url` specifies the redirect URL. `redirect_url` must be an alphanumeric string of 1 through 511 characters. It may include one or more dynamic fields (up to 16 may be specified). For example, `http://search.com/subtag=#HTTP.URL#`. Dynamic fields must be enclosed in “#” (hash).

  Up to 16 dynamic fields out of the following 23 are allowed:

  - `#BEARER.CALLED-STATION-ID#`
  - `#BEARER.CALLING-STATION-ID#`
  - `#BEARER.NAS-IP-ADDRESS#`
  - `#BEARER.USER-NAME#`
  - `#BEARER.ACCT-SESSION-ID#`
  - `#BEARER.CORRELATION-ID#`
  - `#BEARER.RULEBASE#`
  - `#BEARER.SERVED-BSA-ADDR#`
  - `#BEARER.SERVICE-NAME#`
  - `#BEARER.SUBSCRIBER-ID#`
  - `#BEARER.MSISDN#`
•HTTP.URL#
•HTTP.URI#
•HTTP.HOST#
•RTSP.URI#
•WSP.URL#
•CONTENT-ID-LABEL#
•CONTENT-ID-LABEL-CAUSING-REDIRECTION#
•BEARER.HWID#
•BEARER.IMSI#
•BEARER.IMEI#
•BEARER.ESN#
•BEARER.MEID#

Concatenated fields separated by ; (semi colon) can also be inserted. For example, #BEARER.IMSI;BEARER.IMEI#

•encryption { blowfish128 | blowfish64 } [ encrypted ] key key

**Important:** This option is available only in StarOS 12.2 and later releases.

•encryption: Specifies to enable encryption for dynamic fields of the redirect URL.
  •blowfish128: Specifies to use Blowfish encryption with 128 bit key for encrypting the dynamic fields.
  •blowfish64: Specifies to use Blowfish encryption with 64 bit key for encrypting the dynamic fields.
  •aes128: Specifies to use AES-CBC encryption with 128 bit key for encrypting the dynamic fields.
  •aes256: Specifies to use AES-CBC encryption with 256 bit key for encrypting the dynamic fields.
  •salt: Specifies to use salt with AES-CBC encryptions of the dynamic fields.

•encrypted: Specifies to encrypt the key.

•key key: Specifies the key to use for encryption of dynamic fields.
  key must be an alphanumeric string of 1 through 523 characters.

Note that encryption is supported only for the following fields:
•BEARER.CALLING-STATION-ID#
•BEARER.MSISDN#
•BEARER.IMEI#
•BEARER.MEID#
•BEARER.IMSI#
•BEARER.USERNAME#
•BEARER.ESN#
Also, concatenated fields having any of the above will be encrypted.

%3furl= can be used as a delimiter between URL. As in http://search.com/subtarg/%3furl=#HTTP.URL# format.

● **clear-quota-retry-timer**: Specifies to reset Credit Control Application (CCA) Quota Retry Timer upon redirection.

● **first-request-only** [ post-redirect { allow | discard | terminate } ]

- **Important**: This option is available only in StarOS 12.3 and later releases.

- **first-request-only**: Specifies the url-redirection to be performed only once per session after the first web traffic has been detected.

- **post-redirect**: Specifies the action to be taken on subsequent flow packets that invoke this charging action after the first url-redirection has been performed for that session.

The following are the different actions allowed on the flow packets:

- **allow**: allows the packets subsequent to the first url-redirection to flow
- **discard**: discards the packets subsequent to the first url-redirection
- **terminate**: terminates the flow of packets on receiving packets subsequent to the first url-redirection

To disable this option if configured earlier, reuse the same `flow action redirect-url` `redirect_url` command without the **first-request-only** keyword.

- **Important**: Disabling the **first-request-only** keyword will not affect the existing subscriber calls.

`rulebase-change rulebase_name`  
Specifies the rulebase to change to when the charging action is applied. The new rulebase will be applied to the next packet on the call, and applied only to the current PDN.

`terminate-flow`  
Specifies to terminate the flow. Terminates the TCP connection gracefully between the subscriber and external server and sends a TCP FIN to the subscriber and a TCP RST to the server. If the flow does not use TCP, this option simply discard the packets. This option is applicable only for flows that use TCP.

`terminate-session`  
Specifies to terminate the session. When a rule pointing to a charging action configured with the terminate-session keyword is hit, then the corresponding session will be terminated.

**Usage**  
Use this command to specify the action to take on packets, for example to discard, terminate, or redirect. When a readdress server is configured for a charging action, the `show configuration` command will display the readdress related configuration only if server address is configured. The `show configuration verbose` command will display the readdress sever if configured, else will display “no flow action”.

Cisco ASR 5x00 Command Line Interface Reference
The redirect-url option can be used to redirect SIP requests as well. The following is a sample configuration:

```
configure

active-charging service s1

charging-action ca_sip_redir
  content-id 10
  flow action redirect-url sip:test@sip.org
  exit

ruledef sip_req
  sip request packet = TRUE
  exit

rulebase plan1
  action priority 08 ruledef sip_req charging-action ca_sip_redir
  /* other rules, routing rules for sip, etc */
  end
```

This would mean any SIP request that hits the `sip_req` ruledef, would get redirected to the url given in `ca_sip_redir`. This involves creating a redirection packet with the following response line and “Contact” header in the response.

```
SIP/2.0 302 Moved Temporarily
302 Moved Temporarily
```

Most of the header fields are copied directly from the request, so that the mandatory SIP headers are present. If content-length header was seen in the original message, it is replaced in the reply with “Content-Length: 0”.

**Example**

The following command sets the flow action to terminate:

```
flow-action terminate-flow
```

The following command resets quota retry timer upon redirection of flow to HTTP URL `http://search.com/?url=#http://msn.com#`:

```
flow action redirect-url http://search.com/?url=#http://msn.com# clear-quota-retry-timer
```
flow idle-timeout

This command allows you to configure the maximum duration a flow can remain idle after which the system automatically terminates the flow.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Charging Action Configuration

```
active-charging service service_name > charging-action charging_action_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-charging-action)#
```

**Syntax**

```
flow idle-timeout { idle_timeout | flow-mapping flow_timeout }
{ default | no } flow idle-timeout [ flow-mapping ]
```

- **no**
  Enables the idle-timeout configuration; sets the idle-timeout to 0 seconds.

- **default**
  Configures this command with its default setting.
  Default: 300 seconds

- **idle-timeout idle_timeout**
  Specifies the maximum duration, in seconds, a flow can remain idle.
  `idle_timeout` must be an integer from 0 through 86400.

- **flow-mapping flow_timeout**
  Specifies the maximum duration of flow-mapping timeout, in seconds.
  `flow_timeout` must be an integer from 0 through 86400.

**Usage**

Use this command to configure the maximum duration a flow can remain idle after which the system automatically terminates the flow.

**Example**

The following command configures the idle-timeout setting to 400 seconds:

```
flow idle-timeout 400
```
flow limit-for-bandwidth

For Session Control functionality this command allows you to enable/disable bandwidth limiting and configure the uplink and downlink bandwidth limits for subscriber.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Charging Action Configuration
active-charging service service_name > charging-action charging_action_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-charging-action)#

Syntax

flow limit-for-bandwidth { { direction { downlink | uplink } peak-data-rate bps peak-burst-size bytes violate-action { discard | lower-ip-precedence } [ committed-data-rate bps committed-burst-size bytes [ exceed-action { discard | lower-ip-precedence } ] ] } | { id id } }

{ default | no } flow limit-for-bandwidth { direction { downlink | uplink } | id }

no
If previously configured, disables bandwidth control traffic policing for the specified direction for the current subscriber.

default
Configures this command with its default setting.

direction { downlink | uplink }
Specifies the direction of flow to apply bandwidth limit:
  • downlink: Flow of data towards subscriber.
  • uplink: Flow of data from subscriber.

peak-data-rate bps
Specifies the peak data-rate for the subscriber, in bps (bits per second).
bps must be an integer from 1 through 4294967295.
Default: 256000

peak burst-size bytes
The peak burst size allowed, in bytes.
bytes must be an integer from 1 through 4294967295.
Default: 3000
### Important:
It is recommended that this parameter be configured to at least the greater of the following two values: 1) three times greater than packet MTU for the subscriber connection, OR 2) three seconds worth of token accumulation within the “bucket” for the configured peak-data-rate.

```plaintext
violate-action { discard | lower-ip-precedence }
```

Specifies the action to take on packets that exceed both the committed-data-rate and the peak-data-rate. The following actions are supported:
- **discard**: Discard the packet
- **lower-ip-precedence**: Transmit the packet after lowering the IP precedence

Default: **discard**

### committed-data-rate bps

The committed data rate (guaranteed-data-rate) in bits per second (bps).
In releases prior to 15.0, the committed-data-rate based policing was not effected for non-GBR bearers even if it is configured in Charging Action configuration mode. In 15.0 and later releases, the committed-data-rate policing can be implemented for both GBR bearers and non-GBR bearers. If the customer does not want to implement the committed-data-rate policing for non-GBR bearers, then the **committed-data-rate** keyword should not configured with the **flow limit-for-bandwidth** command in Charging Action configuration mode.

- *bps* must be an integer from 1 through 4294967295.
- Default: 144000

### committed-burst-size bytes

The committed burst size allowed, in bytes.

- *bytes* must be an integer from 1 through 4294967295.
- Default: 3000

### exceed-action { discard | lower-ip-precedence }

The action to take on the packets that exceed the committed-data-rate but do not violate the peak-data-rate. The following actions are supported:
- **discard**: Discard the packet
- **lower-ip-precedence**: Transmit the packet after lowering the ip-precedence

If exceed-action is not configured, the packets are forwarded.

Default: **lower-ip-precedence**

### id id

**Important**: This option is available only in StarOS 8.1 and later releases.

Specifies the bandwidth limiting identifier.

- *id* must be an integer from 1 through 65535.

This identifier enables traffic policing based on a separate identifier other than content ID. This identifier will always take priority over content ID. If this identifier is not configured, traffic policing will be based on the content ID.
Usage
Use this command to limit the bandwidth a subscriber uses in the uplink and downlink directions under Session Control.

**Important:** If the exceed/violate action is set to “lower-ip-precedence”, the TOS value for the outer packet becomes “best effort” for packets that exceed/violate the traffic limits regardless of what the `ip user-datagram-tos copy` command is configured to. In addition, the `lower-ip-precedence` option may also override the `ip qos-dscp` command configuration. Therefore, it is recommended that command not be used when specifying this option.

More information on the QoS feature is available in the *QoS Management* appendix of the *System Administration Guide*.

Example

The following command sets an uplink peak data rate of 128000 bps and lowers the IP precedence when the committed-data-rate and the peak-data-rate are exceeded:

```
flow limit-for-bandwidth uplink peak-data-rate 128000 violate-action lower-ip-precedence
```

The following command sets a downlink peak data rate of 256000 bps and discards the packets when the committed-data-rate and the peak-data-rate are exceeded:

```
flow limit-for-bandwidth downlink peak-data-rate 256000 violate-action discard
```
flow limit-for-flow-type

This command allows you to specify the maximum number of simultaneous flows (of this type) that a subscriber may have, and the action to take if the limit is reached.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Charging Action Configuration

active-charging service service_name > charging-action charging_action_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-charging-action)#

Syntax

flow limit-for-flow-type limit over-limit-action { discard | redirect-url url | terminate-flow | terminate-session }

no flow limit-for-flow-type

no

If previously configured, deletes the flow limit-for-flow-type configuration in the current charging action.

limit

Specifies the maximum number of flows of a type exceeding which the specified over-limit-action triggers. limit must be an integer from 1 through 4000000000.

over-limit-action { discard | redirect-url url | terminate-flow | terminate-session }

Specifies the action to take on exceeding limit for a flow type:

• discard: Discards the packets
• redirect-url url: Redirects the flow to the specified URL. url must be an alphanumeric string of 1 through 511 characters. For example, http://search.com.
• terminate-flow: Terminates the flow to which this packet belongs
• terminate-session: Terminates the session to which this packet belongs

Usage

Use this command to specify the number of simultaneous flows (of a type) that a subscriber may have, and the action to take if the limit is reached.

All flows with the same content-id are considered to be the same type. This limit applies to the total of all flows for a subscriber connection (that is, an individual PDP context or individual A10 tunnel).

If the flow is not HTTP, the redirect-url option is ignored, that is the packet is forwarded normally. Refer to the flow action CLI command.
If the limit specified by the `flow limit-across-applications` command in the Rulebase Configuration Mode is also exceeded, action is taken for that over-limit condition rather than the action configured here.

**Example**

The following command terminates the flow if total number of flows of a type exceeds 1024:

```
flow limit-for-flow-type 1024 over-limit-action terminate-flow
```
ip tos

This command allows you to configure the IP Type of Service (ToS) octets.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Charging Action Configuration

```
active-charging service service_name > charging-action charging_action_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-charging-action)#
```

**Syntax**

```
ip tos { af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be | ef | lower-bits tos_value } [ uplink | downlink ]
```

- **default**
  Configures this command with its default setting.
  Default: IP ToS is not modified.

- **no**
  If previously configured, deletes the IP ToS configuration in the current charging action.

- **af xx**
  Specifies the use of an assured forwarding \( xx \) per hop behavior (PHB).

- **be**
  Specifies the use of best effort forwarding PHB.

- **ef**
  Specifies the use of expedited forwarding PHB.

- **lower-bits tos_value**

**Important:** In StarOS 8.1 and later releases, this option is “lower-bits tos_value”. In StarOS 8.0, it is tos_value.

Specifies the least-significant 6 bits in the TOS byte with the specified numeric value.

*tos_value* must be an integer from 0 through 63.
**downlink**
Specifies the ToS only for downlink packets.

**uplink**
Specifies the ToS only for uplink packets.

**Usage**
Use this command to specify the IP Type of Service (ToS) octets to use in the charging action. If one of the enumerated values is set, the DSCP bits which are the six most-significant bits in the TOS byte are marked. If the integer value is set, it will be written into the six least-significant bits of the TOS byte. If **downlink** or **uplink** keywords are not specified, the command applies to both directions.

This command may be used multiple times. For example, the following sequence of commands will cause to set the ToS to af11 in the uplink direction, but not modify the ToS in the downlink direction:

```
ip tos af11
no ip tos downlink
```

**Example**
The following command sets the IP ToS to **be** with **downlink**:

```
ip tos be downlink
```
ip vlan

This command allows you to configure the VLAN identifier to be associated with the subscriber traffic in the destination context.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Charging Action Configuration

active-charging service service_name > charging-action charging_action_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-charging-action)#

Syntax

ip vlan vlan_id

{ default | no } ip vlan

-------

default

Configures this command with its default setting.
Default: Disable this IP VLAN configuration. Same as no ip vlan command.

-------

no

If previously configured, deletes the IP VLAN configuration in the current charging action. Whatever value is configured for the VLAN tag in the subscriber configuration or IP pool configuration (or no VLAN tag if there is no configuration elsewhere) is used.

-------

vlan_id

Specifies the VLAN ID.

vlan_id must be an integer from 1 through 4094.

Usage

This command configures the subscriber VLAN ID which is used with the assigned address for the subscriber session to receive packets. If the IP pool from which the address is assigned is configured with a VLAN ID, then this subscriber configured VLAN ID overrides it.

Subscriber traffic can be routed to specific VLANs based on the configuration of their user profile. Using this functionality provides a mechanism for routing all traffic from a subscriber over the specified VLAN. All packets destined for the subscriber must also be sent using only IP addresses valid on the VLAN or they will be dropped.

Example

The following command sets the IP VLAN range to go up to 500:

    ip vlan 500
The following command sets the IP VLAN range back to default.

```
default ip vlan
```
nexthop-forwarding-address

This command allows you to configure the nexthop forwarding address.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Charging Action Configuration

```
active-charging service service_name > charging-action charging_action_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-charging-action)#
```

**Syntax**

```
exthop-forwarding-address ipv4_address

no nexthop-forwarding-address
```

- **no**
  If previously configured, deletes the nexthop-forwarding-address configuration in the current charging action.

- **ipv4_address**
  Specifies the nexthop-forwarding-address for the current charging action.
  `ipv4_address` must be the nexthop forwarding address, and must be an IPv4 address.

**Usage**

Use this command to configure the nexthop-forwarding-address for a charging action. When an uplink packet matches a rule and a charging action is applied to it this nexthop forwarding address is used.

There are different methods to configure a nexthop forwarding address, they are prioritized as follows:

- The nexthop forwarding address, if configured, in a redirect ACL is used
- Else, the nexthop address configured in the charging action is used
- Else, the nexthop address, if configured, in the IP pool is used

**Example**

The following command sets the nexthop forwarding address for the current charging action to 10.1.1.1:

```
nexthop-forwarding-address 10.1.1.1
```
**pco-custom1**

This command configures the Protocol Configuration Options (PCO) value that will be sent to all UEs, and relates to the PCO for UE Notification feature.

**Product**
P-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Charging Action Configuration

```
active-charging service service_name > charging-action charging_action_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-charging-action)#
```

**Syntax**

```
pco-custom1 custom1_value
{ no | default } pco-custom1
```

- **default**
  - Configures custom1 with the default setting.
  - Default: 0

- **no**
  - If previously configured, resets the pco-custom1 value to the default setting.

- **custom1_value**
  - Specifies the PCO custom1 value.
  - custom1_value must be an integer from 0 through 255.

**Usage**

Use this command to configure the PCO custom1 value to be sent to the MS GTP messages. To enable or disable sending customized PCO options, use the `pco-options` command in the APN Configuration Mode.

**Example**

The following command configures PCO custom1 value to 5:

```
pco-custom1 5
```
product-offer-id-avp

This command enables sending the “Product-Offer-ID” AVP with traffic identifier for Home Agent (HA)/Content Charging Gateway (CCG) instead of the “Rating-Group” AVP. This allows to identify and report application service traffic interval or volume.

**Important:** This command is customer-specific. For more information please contact your Cisco account representative.

**Product**
- HA
- PDSN

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > ACS Configuration > Charging Action Configuration

```bash
active-charging service service_name > charging-action charging_action_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-charging-action)#
```

**Syntax**

`product-offer-id-avp`

**Usage**

Use this command to send the “Product-Offer-ID” AVP in Diameter message instead of the “Rating-Group” AVP for HA/CCG implementation. This implementation means that HA/CCG is deployed to work with both AAA server and OCS via Diameter Gy Online Charging Protocol for content based billing on both offline and online charging.

**Important:** If there is no mapping label configured for a content-id with the `label content-id` command in Active Charging Service Configuration Mode, the rating group will be sent in Product-Offer-ID AVP as Label.
**qos-class-identifier**

This command allows you to configure the QoS Class Identifier (QCI).

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Charging Action Configuration

```
active-charging service service_name > charging-action charging_action_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-charging-action)#
```

**Syntax**

```
qos-class-identifier qos_class_identifier

no qos-class-identifier
```

- **no**
  If previously configured, deletes the QCI configuration in the current charging action.

- **qos_class_identifier**
  Specifies the QCI.
  `qos_class_identifier` must be an integer from 1 through 9 or from 128 through 254 (Operator specific).

**Usage**

Use this command to configure the QCI for a charging action.

**Example**

The following command configures the QCI as 3:

```
qos-class-identifier 3
```
qos-renegotiate

This command allows you to configure the QoS traffic class for the Layer 7 QoS Renegotiation feature, enabling the triggering of QoS renegotiation from a rule.

**Important:** This command is license dependent. For more information please contact your Cisco account representative.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Charging Action Configuration

**Syntax**

```plaintext
qos-renegotiate traffic-class \{ background | conversational | interactive priority | streaming \}
```

**no qos-renegotiate**

- **no**
  If previously configured, deletes the qos-renegotiate traffic-class configuration in the current charging action.

- **background**
  Specifies the traffic class as Background, for traffic patterns in which the data transfer is not time-critical (for example e-mail exchange).

- **conversational**
  Specifies the traffic class as Conversational, for traffic patterns in which there is a constant flow of packets.

- **interactive priority**
  Specifies the traffic class as Interactive, for traffic patterns in which there is an intermittent flow of packets. *priority* specifies the traffic handling priority, and must be an integer from 1 through 3.

- **streaming**
  Specifies the traffic class as Streaming, for traffic patterns in which there is a constant flow of data in one direction, either upstream or downstream.
Usage

Use this command to configure the QoS traffic class for a charging action for the Layer 7 QoS Renegotiation feature, enabling triggering QoS renegotiation from an active-charging rule. Layer 7 QoS Renegotiation is an extension of the Dynamic QoS Renegotiation feature. Upon matching a particular layer 7 rule, for example the access of a particular URL, the GGSN triggers the renegotiation of the PDP context.

Example

The following command sets the QoS traffic class in the charging action to streaming:

```
qos-renegotiate traffic-class streaming
```
service-detection

The `service-detection session-update` command enables the support for users’ QoS updation by PDSN/PCEF based on service start or stop.

**Important:** This command is customer specific. For more information contact your Cisco account representative.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Charging Action Configuration

```
active-charging service service_name > charging-action charging_action_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-charging-action)#
```

**Syntax**

```
configure

active-charging service service-name

charging-action action-name

[no] service-detection session-update qos

end
```

**Usage**

Use this command to configure the service detection to enable the support for users’ QoS updation by PDSN/PCEF based on service start or stop.
Example

The following command configures service detection for a subscriber session and sets the QoS updation.

```
service-detection session-update qos
```
tft packet-filter

This command allows you to specify the packet filter to use in TFTs sent to the MS.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Charging Action Configuration

active-charging service service_name > charging-action charging_action_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-charging-action)#

Syntax

[ no ] tft packet-filter packet_filter_name

no
If previously configured, removes the specified packet filter from the current charging action.

packet_filter_name
Specifies the packet filter to add/remove from the current charging action.
packet_filter_name must be the name of a packet filter, and must be an alphanumeric string of 1 through 63 characters.

Usage
Use this command to configure the packet filter to be sent to the MS. Up to eight packet filters can be specified in a charging action.

Example
The following command configures the packet filter filter23 to be sent to the MS:

tft packet-filter filter23
tft-notify-ue

This command allows you to control whether TFT updates are sent to UE or not.

Product

All

Privilege

Security Administrator, Administrator

Mode

Exec > ACS Configuration > Charging Action Configuration

active-charging service service_name > charging-action charging_action_name

Entering the above command sequence results in the following prompt:

[local] host_name(config-charging-action) #

Syntax

[ no ] tft-notify-ue

no

If this option is configured, TFTs for that charging action are not sent to UE if certain trigger conditions are met.

Usage

Use this command to suppress the selected TFT updates from being sent to the UE. This helps to identify if the appropriate TFT defined in the charging action needs to be sent to the UE or not. This CLI command is supported for both default and dedicated bearers. The ability to include TFTs in the initial session creation are also controlled through this command. This way, the operator can suppress any unwanted TFTs to the UE.

Releases prior to 15.0, all predefined rules charging actions are associated with TFTs and the system includes TFTs towards the UE for all scenarios. In some scenarios it results in creating duplicate TFTs. This CLI-based approach is developed to overcome this situation.

NOTE: The TFT updates are not sent to UE based on certain trigger conditions.
**tos**

This command allows you to configure the Type of Service (ToS) octets.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Charging Action Configuration

```
active-charging service service_name > charging-action charging_action_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-charging-action)#
```

**Syntax**

```
tos { af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be | ef | lower-bits tos_value } [ downlink | uplink ]
no tos [ downlink | uplink ]
```

- **no**
  Disables the ToS being used in the charging action.

- **af** xx
  Specifies the use of an assured forwarding xx Per Hop Behavior (PHB).

- **be**
  Specifies use of Best Effort forwarding PHB.

- **ef**
  Specifies use of Expedited Forwarding PHB.

- **lower-bits tos_value**

**Important:** In StarOS 8.1 and later releases, this option is “lower-bits tos_value”. In StarOS 8.0 release, it is tos_value.

Sets the least-significant 6 bits in the ToS byte with the specified numeric value. tos_value must be an integer from 0 through 63.

- **downlink**
  Specifies the ToS only for downlink packets.
uplink
Specifies the ToS only for uplink packets.

Usage
Use this command to set the ToS octets used in the charging action. If one of the enumerated values is set, the Differentiated Services Code Point (DSCP) bits (the six most-significant bits (MSBs) in the ToS byte) are marked. If the integer value is set, it will be written into the six least-significant bits (LSBs) of the ToS byte.

Example
The following command sets the ToS to be for downlink packets:

```
tos be downlink
```
tpo profile

The Traffic Performance Optimization (TPO) in-line service is not supported in this release.
**video bitrate**

This command allows you to specify the default target bit rate to use for the video pacing feature on the Mobile Video Gateway. This value is also used as the suggested maximum bit rate for the video optimization policy control feature.

**Product**
MVG

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Charging Action Configuration

```
active-charging service service_name > charging-action charging_action_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-charging-action)#
```

**Syntax**

```
[ default | no ] video bitrate bit_rate [ -noconfirm ]
```

- **default**
  Sets video bitrate to its default value.

- **no**
  Deletes the video bit rate if previously configured.

```
video bitrate bit_rate
```

Specifies the bit rate, in bits per second, at which the TCP video flow should be paced during video pacing. This value is also used as the suggested maximum bit rate for the video optimization policy control feature. For video pacing, this default bit rate is used on each video flow until the rate determination function calculates the optimal bit rate for pacing.

- **bit_rate** must be an integer from 0 to 25600000.
- Default: 0

- **-noconfirm**
  Specifies that the command must execute without prompting for confirmation.

**Usage**

Use this command to specify the default bit rate to use for the video pacing feature, and the suggested maximum bit rate for the video optimization policy control feature.

**Example**

The following command sets the bit rate for the video flow at 300000 (300kbps):

```
video bitrate 300000
```
video cae-readdressing

This command allows you to enable CAE (Content Adaptation Engine) re-addressing, allowing video traffic to be fetched from the CAEs in the CAE group. The CAE is an optional component of the Mobile Videoscape.

**Product**
MVG

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Charging Action Configuration

```
active-charging service service_name > charging-action charging_action_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-charging-action)#
```

**Syntax**

```
[ no ] video cae-readdressing [ xheader-format xheader_format_name ]
```

- **no**
  Disables CAE re-addressing if previously configured.

- **video cae-readdressing**
  Enables CAE re-addressing, allowing video traffic to be fetched from the CAEs in the CAE group.

- **xheader-format xheader_format_name**
  Specifies an HTTP x-header (Extension header) format for readdressing. When specified, the MVG inserts a destination IP address and TCP port number in a proprietary HTTP x-header in the HTTP request to the CAE. The CAE uses this information to connect to the OS (Origin Server) to retrieve selected video clips for adaptation. 
  `xheader_format_name` must be an alphanumeric string of 1 through 63 characters.

**Usage**

Use this command to enable CAE re-addressing on the Mobile Video Gateway.

**Example**

The following command enables CAE re-addressing:

```
video cae-readdressing xheader-format format_1
```
video detailed-statistics

This command allows you to enable the collection of detailed video statistics.

Product
MVG

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Charging Action Configuration

active-charging service service_name > charging-action charging_action_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-charging-action)#

Syntax

[ default | no ] video detailed-statistics [ -noconfirm ]

---

**default**
Sets video detailed-statistics to its default value, which is the same as [ no ].

**no**
Disables the video statistics feature if previously enabled.

**video detailed-statistics**
Enables the video statistics feature. When a flow matches a rule definition for video during DPI (Deep Packet Inspection), the video statistics feature begins collecting detailed statistics for the video flow.

**-noconfirm**
Specifies that the command must execute without prompting for confirmation.

Usage
Use this command to enable the video statistics feature.

Example
The following command enables the video statistics feature:

```
video detailed-statistics
```
video optimization-preprocessing all

This command allows you to enable CAE re-addressing by enabling the Active Charging Service (ACS) to re-address video requests to the CAEs in the CAE group.

**Product**
MVG

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Charging Action Configuration

```
active-charging service service_name > charging-action charging_action_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-charging-action)#
```

**Syntax**

```
[ no ] video optimization-preprocessing all
```

- **no**
  Disables CAE re-addressing if currently enabled.

  ```
  video optimization-preprocessing cae-readdressing
  ```

  Enables CAE re-addressing by enabling the ACS to re-address video requests to the CAEs in the CAE group.

**Usage**

Use this command to enable CAE re-addressing by enabling the ACS to re-address video requests to the CAEs in the CAE group.

**Example**

The following command enables CAE re-addressing:

```
video optimization-preprocessing all
```
video optimization-preprocessing cae-readdressing

This command allows you to enable CAE re-addressing by enabling the Active Charging Service (ACS) to re-address video requests to the CAEs in the CAE group.

**Product**
MVG

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Charging Action Configuration

```
active-charging service service_name > charging-action charging_action_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-charging-action)#
```

**Syntax**

```
[ no ] video optimization-preprocessing cae-readdressing
```

- **no**
  Disables CAE re-addressing if currently enabled.

- **video optimization-preprocessing cae-readdressing**
  Enables CAE re-addressing by enabling the ACS to re-address video requests to the CAEs in the CAE group.

**Usage**

Use this command to enable CAE re-addressing by enabling the ACS to re-address video requests to the CAEs in the CAE group.

**Example**

The following command enables CAE re-addressing:

```
video optimization-preprocessing cae-readdressing
```
video pacing by-policing

This command allows you to enable the video pacing feature.

Product
MVG

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Charging Action Configuration

active-charging service service_name > charging-action charging_action_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-charging-action)#

Syntax

[ default | no ] video pacing by-policing [ initial-burst-duration value ] [ normal-burst-duration value ] [ -noconfirm ]

---

default
Sets video pacing by-policing to its default value, which is the same as [ no ].

---

no
Deletes the video pacing by-policing settings and disables video pacing if previously configured.

---

video pacing by-policing

Enables the video pacing feature. When enabled, video pacing is applied per TCP video flow. The command syntax by-policing enables pacing enforcement by the policing method, which is the available method for this software release.

---

initial-burst-duration value

Specifies the duration, in seconds, for the allowed initial burst of video content. Note that the initial burst is configured in terms of time, so that for video files with different encoding bit rates, the amount of bytes allowed without enforcing pacing gets adjusted accordingly. The amount of bytes allowed is calculated by (video encoding rate * initial-burst-duration).
value must be an integer between 1 and 30.
Default: 10 seconds

---

normal-burst-duration value

Specifies the duration, in seconds, for the allowed normal burst of video content after the initial burst is completed. Like the initial burst, the normal burst is also configured in terms of time, so that for video files with different encoding bit rates, the amount of bytes allowed without enforcing pacing gets adjusted accordingly. The amount of bytes allowed is calculated by (video encoding rate * normal-burst-duration).
value must be an integer between 1 and 30.
Default: 3 seconds
video pacing by-policing

-noconfirm

Specifies that the command must execute without prompting for confirmation.

Usage

Use this command to enable video pacing by policing.

Example

The following command enables video pacing by policing with an initial burst duration of 15 seconds and a normal burst duration of 3 seconds:

```
video pacing by-policing initial-burst-duration 15 normal-burst-duration 3
```
xheader-insert

This command allows you to specify the extension-header (x-header) format whose fields have to be inserted in HTTP GET and POST request packets.

**Important:** This command is license dependent. For more information please contact your Cisco account representative.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > ACS Configuration > Charging Action Configuration

`active-charging service service_name > charging-action charging_action_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-charging-action)#
```

**Syntax**

```
xheader-insert xheader-format xheader_format_name [ encryption rc4md5 [ encrypted ] key key ] [ first-request-only ] [ -noconfirm ]

no xheader-insert
```

no

Removes previously configured x-header format name.

```
xheader-format xheader_format_name
```

Enables x-header mode configuration, and specifies the x-header format whose fields are to be inserted in the packets.

`xheader_format_name` must be the name of an x-header format, and must be an alphanumeric string of 1 through 63 characters.

```
encryption rc4md5 [ encrypted ] key key
```

If the x-header format has any encrypted fields defined, specifies to use RC4MD5 encryption. After configuring this option, the fields in xheader format having “encrypt” enabled will be encrypted as follows:

1. The MD5 hash of the configure key will be calculated.
2. This MD5 hash will be used as a key for RC4 encryption.
3. This encrypted value will be base64 encoded to get the final X-header value. The final inserted X-header will be X-alias: base64(RC4(MD5(key),MSISDN)).

In the default case, if encryption is not enabled as above, the plain text value of the xheader field will be inserted.
Note that if the value of the key is changed on the fly, it will take effect only in case of new calls. Also, if the per rulebase RSA encryption is also enabled in the same config, per charging-action RC4MD5 encryption will take precedence over it.

`key` specifies the key as an alphanumeric string of 8 through 15 characters.

`encryption` specifies use of encryption.

The `key` can be configured either as plain text or encrypted. However, in the output of the `show configuration` command it will always be displayed as encrypted. And, in the output of the `show configuration showsecrets` command it will be displayed as plain text.

---

**first-request-only**

Specifies x-header insertion only for the first HTTP request in the IP flow. If not configured, the default behavior is insertion for all requests.

---

`-noconfirm`

Specifies that the command must execute without any prompts and confirmation from the user.

---

**Usage**

Use this command to enable x-header mode, and specify the x-header format name whose fields are to be inserted in HTTP GET and POST request packets.

Also, see the `xheader-format` command in the *ACS Configuration Mode Commands* and *ACS X-header Format Configuration Mode Commands* chapters.

**Example**

The following command enables x-header mode, and specifies the x-header format name as `test12`:

```
xheader-insert xheader-format test12
```
Chapter 8
ACS Configuration Mode Commands

The ACS Configuration Mode is used to manage active charging service (ACS)/enhanced charging service (ECS) configurations. ACS provides flexible, differentiated, and detailed billing to subscribers through Layer 3 through Layer 7 packet inspection and the ability to integrate with back-end billing mediation systems.

**Important:** In this release only one active charging service can be configured per system.

Mode

Exec > ACS Configuration

active-charging service service_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs)#

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
access-ruledef

This command allows you to create/configure/delete access rule definitions (ruledefs).

**Important:** This command is available only in StarOS 8.1 and in StarOS 9.0 and later releases, and must be used to configure the Policy-based Stateful Firewall and NAT features.

**Product**
- NAT
- PSF

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > ACS Configuration

```
active-charging service service_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acd)#
```

**Syntax**

```
access-ruledef access_ruledef_name [ -noconfirm ]
```

```
no access-ruledef access_ruledef_name
```

**no**

If previously configured, deletes the specified access ruledef.

**access_ruledef_name**

Specifies the access ruledef to add/configure/delete.

**access_ruledef_name** must be the name of an access ruledef, and must be an alphanumeric string of 1 through 63 characters, and can contain punctuation characters. Each access ruledef must have a unique name. If the named access ruledef does not exist, it is created, and the CLI mode changes to the Firewall-and-NAT Access Ruledef Configuration Mode wherein the ruledef can be configured. If the named access ruledef already exists, the CLI mode changes to the Firewall-and-NAT Access Ruledef Configuration Mode for that access ruledef.

**-noconfirm**

Specifies that the command must execute without prompting for confirmation.

**Usage**

Use this command to create/configure/delete an access ruledef. A ruledef contains different conditions/criteria to permit, drop, or reject a packet/connection/traffic based on one or more parameters. The ruledef name must be unique within the service. Host pool, port map, IMSI pool, and access/firewall, routing, and charging ruledefs configured in the active charging service must all have unique names.
ACS Configuration Mode Commands

access-ruledef

Important: An access ruledef can be referenced by multiple Stateful Firewall rulebases.

Important: Access ruledefs are different from ACS ruledefs.

On entering this command, the CLI prompt changes to:

```
[context_name]hostname(config-acs-fw-ruledef)#
```

Also see the Firewall-and-NAT Access Ruledef Configuration Mode Commands chapter.

Example

The following command creates an access ruledef named `ruledef1`, and enters the Firewall-and-NAT Access Ruledef Configuration Mode:

```
access-ruledef ruledef1
```
bandwidth-policy

This command allows you to create/configure/delete bandwidth policies.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration

active-charging service service_name
Entering the above command sequence results in the following prompt:

[local]host_name(config-acs)#

Syntax

bandwidth-policy bandwidth_policy_name [ -noconfirm ]

no bandwidth-policy bandwidth_policy_name

no

If previously configured, deletes the specified bandwidth policy from the active charging service.

bandwidth_policy_name

Specifies the bandwidth policy to add/configure/delete. 

bandwidth_policy_name must be the name of a bandwidth policy, and must be an alphanumeric string of 1 through 63 characters. Each bandwidth policy must have a unique name.

If the named bandwidth policy does not exist, it is created, and the CLI mode changes to the ACS Bandwidth Policy Configuration Mode wherein the bandwidth policy can be configured.

If the named bandwidth policy already exists, the CLI mode changes to the ACS Bandwidth Policy Configuration Mode for that bandwidth policy.

-noconfirm

Specifies that the command must execute without prompting for confirmation.

Usage

Use this command to create/configure/delete a bandwidth policy.

In 12.3 and earlier releases, a maximum of 64 bandwidth policies can be configured.

In 14.0 and later releases, a maximum of 256 bandwidth policies can be configured.

On entering this command, the CLI prompt changes to:

[context_name]host_name(config-bandwidth-policy)#

Also see the ACS Bandwidth Policy Configuration Mode Commands chapter.

Example

The following command creates a bandwidth policy named test73, and enters the ACS Bandwidth Policy Configuration Mode:
bandwidth-policy test73
buffering-limit

This command allows you to configure packet buffering limits.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration

active-charging service service_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs)#

Syntax

buffering-limit { flow-max-packets flow_max_packets | subscriber-max-packets subscriber_max_packets }

{ default | no } buffering-limit { flow-max-packets | subscriber-max-packets }

default

Configures this command with its default setting.
Default: In 14.0 and earlier releases, no limit, other than the maximum amount of available memory.
Default: In 14.1 and later releases, 255

no

Disables the buffering limit configuration.

flow-max-packets flow_max_packets

Specifies the maximum number of packets that can be buffered per flow.
flow_max_packets must be an integer from 1 through 255.

subscriber-max-packets subscriber_max_packets

Specifies the maximum number of packets that can be buffered per subscriber.
subscriber_max_packets must be an integer from 1 through 255.

Usage

Use this command to configure the limits for buffering packets sent by a subscriber, while waiting for a
response from the Diameter server. Packets need to be buffered for various reasons, such as, waiting for
Credit Control Authorization or waiting for the result of a content filtering rating request.

Example

The following command sets the buffering limit per flow to 55:

    buffering-limit flow-max-packets 55
charging-action

This command allows you to create/configure/delete ACS charging actions.

Important: A maximum of 2048 charging actions can be configured in the active charging service.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration

**active-charging service** service_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-ac)#

Syntax

[ no ] charging-action charging_action_name [ -noconfirm ]

no

If previously configured, deletes the specified charging action from the active charging service.

charging_action_name

Specifies the charging action to add/configure/delete. charging_action_name must be the name of a charging action, and must be an alphanumeric string of 1 through 63 characters and can contain punctuation characters. Each charging action must have a unique name.

If the named charging action does not exist, it is created, and the CLI mode changes to the ACS Charging Action Configuration Mode wherein the charging action can be configured.

If the named charging action already exists, the CLI mode changes to the ACS Charging Action Configuration Mode for that charging action.

-noconfirm

Specifies that the command must execute without prompting for confirmation.

Usage

Use this command to create/configure/delete an ACS charging action. A charging action represents actions to be taken when a configured rule is matched. Actions could range from generating an accounting record (for example, an EDR) to dropping the IP packet, etc. The charging action will also determine the metering principle—whether to count retransmitted packets and which protocol field to use for billing (L3/L4/L7 etc).

On entering this command, the CLI prompt changes to:

[context_name]hostname(config-charging-action)#
Also see the *ACS Charging Action Configuration Mode Commands* chapter.

**Example**

The following command creates a charging action named `action123` and changes to the ACS Charging Action Configuration Mode:

```
charging-action action123
```
content-filtering category match-method

This command allows you to specify the match method to look up URLs in the Category-based Content Filtering database.

**Product**
CF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration
```
active-charging service service_name
```
Entering the above command sequence results in the following prompt:
```
[local]host_name(config-ac)#
```

**Syntax**
```
content-filtering category match-method { exact | generic }
```

**default content-filtering category match-method**

- **default**
  Configures this command with its default setting.
  Default: *generic*

- **exact**
  Specifies the exact-match method, wherein URLs are rated only on exact match with URLs present in the Category-based Content Filtering database.

- **generic**
  Specifies the generic match method, wherein normalization, multi-lookups, and rollback algorithms are applied to URLs during look up. URLs are rated on generic match with URLs present in the Category-based Content Filtering database.

**Usage**
Use this command to set the match method to look up URLs in the Category-based Content Filtering database.

**Example**
The following command sets the exact-match method to look up URLs in the Category-based Content Filtering database:
```
content-filtering category match-method exact
```
content-filtering category policy-id

This command allows you to create/configure/delete Content Filtering Category Policies for Category-based Content Filtering support.

**Important:** A maximum of 64 Content Filtering Category Policies can be configured in the active charging service.

**Product**
CF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration

```
active-charging service service_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-accs)#
```

**Syntax**

```
content-filtering category policy-id cf_policy_id [ description [ description_string ] ]
[ -noconfirm ]

no content-filtering category policy-id cf_policy_id
```

**no**
If previously configured, deletes the specified Content Filtering Category Policy from the active charging service.

**cf_policy_id**
Specifies the Content Filtering Category Policy ID to add/configure/delete.

cf_policy_id must be an integer from 1 through 4294967295.

If the specified policy ID does not exist, it is created and the CLI mode changes to the Content Filtering Policy Configuration Mode, wherein the policy can be configured.

If the specified policy ID already exists, the CLI mode changes to the Content Filtering Policy Configuration Mode for that policy.

**description [ description_string ]**
Specifies a description for the Content Filtering Category Policy.

description_string must be an alphanumeric string of 1 through 31 characters.

Note that both description and description_string are optional.

“description description_string” saves description_string as the new description.

“description” removes the previously specified description.

This description is displayed in the output of the “show content-filtering category policy-id id” and “show active-charging service name service_name” commands.
-noconfirm

Specifies that the command must execute without prompting for confirmation.

Usage

Use this command to create/configure/delete a Content Filtering Category Policy. On entering this command, the CLI prompt changes to:

```
[context_name]hostname(config-acsp-content-filtering-policy)#
```

Also see the Content Filtering Policy Configuration Mode Commands chapter.

Example

The following command creates a Content Filtering Policy with the ID 101, and enters the Content Filtering Policy Configuration Mode:

```
content-filtering category policy-id 101
```
credit-control

This command allows you to enable/disable Prepaid Credit Control Configuration Mode.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration

active-charging service service_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs)#

Syntax

[ no ] credit-control [ group cc_group_name ]

no
Disables the specified Prepaid Credit Control Application configuration.

group cc_group_name

Important: This option is only available in StarOS 8.1 and later releases.

Specifies the credit control group to add/configure/delete.

cc_group_name must be the name of a credit control group, and must be an alphanumeric string of 1 through 63 characters. Each credit control group must have a unique name.

If the named credit control group does not exist, it is created, and the CLI mode changes to the Credit Control Configuration Mode, wherein the credit control group can be configured.

If the named credit control group already exists, the CLI mode changes to the Credit Control Configuration Mode for that credit control group.

Creating different credit control groups enables applying different credit control configurations (DCCA dictionary, failure-handling, session-failover, Diameter endpoint selection, etc.) to different subscribers on the same system.

Without credit control groups, only one credit control configuration is possible on a system. All the subscribers in the system will have to use the same configuration.

Usage

Use this command to enable/disable Prepaid Credit Control Configuration for RADIUS/Diameter charging mode.

On entering this command, the CLI prompt changes to:
[context_name]hostname(config-dcca)#

Also see the Credit Control Configuration Mode Commands chapter.

Example
The following command enables prepaid credit control accounting to use RADIUS and/or Diameter interface mode:

```
credit-control
```
diameter credit-control

Description This command has been deprecated, and is replaced by the credit-control command.
edr-format

This command allows you to create/configure/delete ACS Event Data Record (EDR) formats.

**Important:** A maximum of 256 EDR plus UDR formats can be configured in the active charging service.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration

```
active-charging service service_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

**Syntax**

```
edr-format edr_format_name [ -noconfirm ]
```

```
no edr-format edr_format_name
```

- **no**
  
  If previously configured, deletes the specified EDR format from the active charging service.

  - **edr_format_name**
    
    Specifies the EDR format to add/configure/delete.
    
    *edr_format_name* must be an alphanumeric string of 1 through 63 characters. Each EDR format must have a unique name.
    
    If the named EDR format does not exist, it is created, and the CLI mode changes to the EDR Format Configuration Mode wherein the EDR format can be configured.
    
    If the named EDR format already exists, the CLI mode changes to the EDR Format Configuration Mode for that EDR format.
    
  - **-noconfirm**
    
    Specifies that the command must execute without prompting for confirmation.

**Usage**

Use this command to create/configure/delete an EDR format.

On entering this command, the CLI prompt changes to:

```
[context_name]hostname(config-acs-edr)#
```

Also see the *EDR Format Configuration Mode Commands* chapter.

**Example**
The following command creates an EDR format named \textit{edr\_format1}, and enters the EDR Format Configuration Mode:

\texttt{edr\_format edr\_format1}
edr-ipproto-port-map

This command enables IP protocol and server port mapping for Event Data Records (EDR).

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration

active-charging service service_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs)#

Syntax

[ default | no ] edr-ipproto-port-map

default
Configures this command with its default setting.
Default: Disabled

no
If previously enabled, disables the IP protocol and server port mapping for EDR.

Usage
Use this command to enable IP protocol and server port mapping for EDR. As part of EDR generation, packets can be mapped based on IP header protocol and Transport Header Port. Generating statistics based on IP Protocol and Transport Port number is an added advantage for offline packet analysis.
**edr-udr-flow-control**

This command allows you to enable/disable flow control between Session Managers (SessMgrs) and the CDRMOD process.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > ACS Configuration

```bash
active-charging service service_name
```

Entering the above command sequence results in the following prompt:

```bash
[local] host_name(config-acs)#
```

**Syntax**

```bash
edr-udr-flow-control [ unsent-queue-size unsent_queue_size ]
```

```bash
{ default | no } edr-udr-flow-control
```

- **no**
  
  If previously enabled, disables the flow control configuration.

- **default**
  
  Configures this command with its default setting.
  
  Default: Flow control is enabled; `unsent-queue-size`: 375

- **unsent-queue-size unsent_queue_size**
  
  Specifies the flow control unsent queue size at Session Manager (SessMgr) level.
  
  `unsent_queue_size` must be an integer from 1 through 2500.

**Usage**

Use this command to enable Flow Control between SessMgr and the CDRMOD process, and configure the unsent queue size.

**Example**

The following command enable Flow Control between SessMgrs and the CDRMOD process, and configure the unsent queue size to 1000:

```bash
edr-udr-flow-control unsent-queue-size 1000
```
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

dend

**Usage**
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```exit```

---

**Usage**

Use this command to return to the parent configuration mode.
**fair-usage deact-margin**

This command allows you to configure the deactivate margin for the Fair Usage feature.

### Product
ACS
ADC
CF
PSF
NAT

### Privilege
Security Administrator, Administrator

### Mode
Exec > ACS Configuration

**active-charging service service_name**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

### Syntax

```
fair-usage deact-margin deactivate_margin

default fair-usage deact-margin
```

- **default**
  Configures this command with its default setting.
  Default: 5 percent

- **deactivate_margin**
  Specifies that Fair Usage monitoring must be disabled when the instance-level credit usage goes
  `deactivate_margin` percentage below `usage_threshold`.
  `deactivate_margin` is a percentage value, and must be an integer from 1 through 100.

### Usage
Use this command to configure when to disable the Fair Usage feature, which enables SessMgr instance-level
load balancing for in-line service features, and resource usage control for subscribers. For additional
information, refer to the feature description in the *Enhanced Charging Service Administration Guide*.

### Example
The following command configures the deactivate margin to disable Fair Usage monitoring to 10% below the
session resource usage threshold (65%):

```
fair-usage deact-margin 10
```
fair-usage tcp-proxy

This command allows you to configure the maximum number of flows for which TCP Proxy can be used per subscriber, and what portion of ECS memory should be reserved for TCP Proxy flows.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration
active-charging service service_name

Entering the above command sequence results in the following prompt:
[local]host_name(config-ac)#

Syntax

fair-usage tcp-proxy { max-flows-per-subscriber max_flows_subscriber | memory-share memory_share }

default fair-usage [ max-flows-per-subscriber | memory-share ]

default
Configures this command with its default setting.

max-flows-per-subscriber max_flows_subscriber

Specifies the maximum number of flows for which TCP Proxy can be used per subscriber. This limit is per Session Manager.
max_flows_subscriber must be an integer from 1 through 100.
Default: 5

memory-share memory_share

Specifies what portion of ECS memory should be reserved for TCP Proxy flows.
memory_share is a percentage value, and must be an integer from 1 through 100.
Default: 10%

Usage
Use this command to configure the maximum number of flows for which TCP Proxy can be used for a subscriber, and what portion of ECS memory should be reserved for TCP Proxy flows.

Example
The following command configures 100 as the maximum number of flows for which TCP Proxy can be enabled for the subscriber:

fair-usage tcp-proxy max-flows-per-subscriber 100
fair-usage threshold-percent

This command allows you to configure the usage threshold to start Fair Usage monitoring.

**Product**
- ACS
- ADC
- CF
- PSF
- NAT

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration

**Syntax**

```
fair-usage threshold-percent usage_threshold

default fair-usage threshold-percent
```

**Usage_threshold**

Specifies the threshold to start Fair Usage monitoring. Until the credit usage hits this threshold, all session resource allocation is allowed. On crossing this threshold, any new resource allocation request is evaluated before being allowed or denied.

usage_threshold is a percentage value, and must be an integer from 1 through 100.

**Usage**

Use this command to configure the threshold to enable the Fair Usage feature, which enables SessMgr instance-level load balancing for in-line service features, and resource usage control for subscribers. For additional information, refer to the feature description in the Enhanced Charging Service Administration Guide.

**Example**

The following command enables the Fair Usage feature, and configures the session resource usage threshold to start Fair Usage monitoring to 75%:

```
fair-usage threshold-percent 75
```
firewall dos-protection flooding

This command is configured to protect servers from mobile subscribers in the uplink direction.

**Product**
- PSF
- NAT

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > ACS Configuration
  ```
  active-charging service service_name
  ```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-accs)#
```

**Syntax**

```plaintext
firewall dos-protection flooding { { icmp | tcp-syn | udp } protect-servers { all | host-pool hostpool_name } packet limit packet_limit | inactivity-timeout timeout | uplink-sample-interval interval }

default firewall dos-protection flooding { icmp | tcp-syn | udp | inactivity-timeout | uplink-sample-interval }

no firewall dos-protection flooding { icmp | tcp-syn | udp }
```

- **no**
  Disables Stateful Firewall protection for subscribers against the specified Denial of Service (DoS) attack(s).

- **default**
  Disables Stateful Firewall protection for subscribers against all DoS attacks.

- **flooding**
  Enables protection against the specified flooding attack:
  - **icmp**: Enables ICMP uplink flooding protection.
  - **tcp-syn**: Enables TCP Syn uplink flooding protection.
  - **udp**: Enables UDP uplink flooding protection.

- **all**: Enables protection for all the servers.

- **host-pool hostpool_name**: Specifies the name of the host pool. `hostpool_name` must be an alphanumeric string of 1 through 63 characters.

- **packet limit packet_limit**
  Specifies the maximum number of packets allowed during a sampling interval. `packet_limit` must be an integer from 1 through 4294967295.
  Default: 1000 packets per sampling interval for all protocols.
inactivity-timeout inactivity_timeout

Specifies the inactivity timeout period, in seconds. This allows flooding traffic if the destination is inactive for more than the configured period.

inactivity_timeout must be an integer from 1 through 4294967295.

Default: 300 seconds

uplink-sample-interval interval

Specifies the uplink sampling interval, in seconds. The maximum sampling-interval configurable is 60 seconds.

interval must be an integer from 1 through 60.

Default: 1 second

Usage

Use this command to enable Stateful Firewall protection from different types of DoS attacks for all servers or for those servers mentioned in the host pool. This allows users to safeguard their own servers and other hosts. DoS attacks are also detected in the downlink direction. The firewall dos-protection command must be configured in the FW-and-NAT Policy Configuration mode.

Example

The following command enables ICMP uplink protection for all servers with packet limit set to 10:

    firewall dos-protection flooding icmp protect-servers all packet limit 10
**firewall flow-recovery**

This command allows you to configure the Stateful Firewall’s Flow Recovery feature.

**Product**
PSF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration

```
active-charging service service_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-accs)#
```

**Syntax**

```
firewall flow-recovery { { downlink [ [ timeout timeout ] [ no-flow-creation ] + ] } | { uplink [ timeout timeout ] } } { default | no } firewall flow-recovery { downlink | uplink }
```

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>default</strong></td>
<td>Configures this command with its default setting.</td>
</tr>
<tr>
<td></td>
<td>Default: Downlink and uplink flow recovery enabled, 300 seconds</td>
</tr>
<tr>
<td><strong>no</strong></td>
<td>Disables the flow recovery configuration.</td>
</tr>
<tr>
<td><strong>downlink</strong></td>
<td>Specifies the packets:</td>
</tr>
<tr>
<td></td>
<td>• <strong>downlink</strong>: Enables flow recovery for packets from the downlink direction.</td>
</tr>
<tr>
<td><strong>uplink</strong></td>
<td>Specifies the packets:</td>
</tr>
<tr>
<td></td>
<td>• <strong>uplink</strong>: Enables flow recovery for packets from the uplink direction.</td>
</tr>
<tr>
<td><strong>timeout</strong></td>
<td>Specifies the Stateful Firewall Flow Recovery Timeout setting, in seconds.</td>
</tr>
<tr>
<td></td>
<td><strong>timeout</strong> must be an integer from 1 through 86400.</td>
</tr>
<tr>
<td></td>
<td>Default: 300 seconds</td>
</tr>
<tr>
<td><strong>no-flow-creation</strong></td>
<td>Specifies not to create data session/flow-related information for downlink-initiated packets (from the Internet to the subscriber) while the firewall downlink flow-recovery timer is running, but send to subscriber.</td>
</tr>
</tbody>
</table>

**Usage**

Use this command to configure Stateful Firewall Flow Recovery feature.
ACS Configuration Mode Commands

firewall flow-recovery

Important: NAT flows will not be recovered.

Example

The following command configures Stateful Firewall Flow Recovery for packets in downlink direction with a timeout setting of 600 seconds:

```
firewall flow-recovery downlink timeout 600
```
firewall max-ip-packet-size

Description In StarOS 8.1 and later releases, for Rulebase-based Stateful Firewall this command is available in the ACS Rulebase Configuration Mode, and for Policy-based Stateful Firewall in the Firewall-and-NAT Policy Configuration Mode. In StarOS 8.3, this command is available in the ACS Rulebase Configuration Mode.
firewall mime-flood

**Description** In StarOS 8.1 and later releases, for Rulebase-based Stateful Firewall this command is available in the ACS Rulebase Configuration Mode, and for Policy-based Stateful Firewall in the Firewall-and-NAT Policy Configuration Mode. In StarOS 8.3, this command is available in the ACS Rulebase Configuration Mode.
firewall nat-alg

This command enables/disables Network Address Translation (NAT) Application Level Gateways (ALGs).

**Product**
NAT

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration

```
active-charging service service_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-accs)#
```

**Syntax**

```
[ default | no ] firewall nat-alg { all | ftp | h323 | pptp | rtsp | sip } [ ipv4-and-ipv6 | ipv4-only | ipv6-only ]
```

---

**default**

Configures this command with the default setting for the specified parameter.

Default:

- **ftp**: Enabled
- **h323**: Enabled
- **pptp**: Disabled
- **rtsp**: Disabled
- **sip**: Disabled

---

**no**

Disables all/ or the specified NAT ALG configuration. When disabled, the ALG(s) will not do any payload translation for NATd calls.

---

**all | ftp | h323 | pptp | rtsp | sip**

Specifies the NAT ALG to enable/disable.

- **all**: Enables/disables all of the following NAT ALGs.
- **ftp**: Enables/disables File Transfer Protocol (FTP) NAT ALG.
- **h323**: Enables/disables H323 NAT ALG.
- **pptp**: Enables/disables Point-to-Point Tunneling Protocol (PPTP) NAT ALG.
- **rtsp**: Enables/disables Real Time Streaming Protocol (RTSP) ALG.
- **sip**: Enables/disables Session Initiation Protocol (SIP) NAT ALG.
firewall nat-alg

ipv4-and-ipv6 | ipv4-only | ipv6-only
Specifies to enable/disable NAT44/NAT64 ALG.
- ipv4-and-ipv6: Enables both NAT44 and NAT64 ALGs.
- ipv4-only: Enables only NAT44 ALG.
- ipv6-only: Enables only NAT64 ALG.

Usage
Use this command to enable/disable NAT ALGs.
To enable NAT ALG processing, in addition to this configuration, ensure that the routing rule for that particular protocol is added in the rulebase.

Example
The following command enables FTP NAT ALG:

```
firewall nat-alg ftp
```

The following command disables FTP NAT ALG:

```
no firewall nat-alg ftp
```

The following command enables FTP NAT ALG, and disables H.323, PPTP, RTSP, and SIP NAT ALGs:

```
default firewall nat-alg all
```
firewall no-ruledef-matches

Description In StarOS 8.1 and later releases, this command is available in the ACS Rulebase Configuration Mode.
firewall port-scan

This command allows you to configure Stateful Firewall’s Port Scan Detection algorithm.

**Product**
PSF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration

```
active-charging service service_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

**Syntax**

```
firewall port-scan { connection-attempt-success-percentage { non-scanner | scanner } [connection-attempt-success-percentage { non-scanner | scanner } | inactivity-timeout | protocol { tcp | udp } response-timeout | scanner-policy { block inactivity-timeout inactivity_timeout | log-only } ] } { inactivity-timeout | protocol { tcp | udp } response-timeout | scanner-policy }
```

<table>
<thead>
<tr>
<th>command</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Configures this command with its default setting.</td>
</tr>
</tbody>
</table>
| connection-attempt-success-percentage { non-scanner | scanner } percentage | Specifies the connection attempt success percentage.  
  *non-scanner*: Specifies the connection attempt success percentage for a non-scanner.  
  
  **Default**: 70%  
  
  *scanner*: Specifies the connection attempt success percentage for a scanner.  
  
  **Default**: 30%  
  
| inactivity-timeout | Specifes the port scan inactivity timeout period, in seconds.  
  inactivity_timeout must be an integer from 60 through 1800.  
  Default: 300 seconds  
  
| protocol { tcp | udp } response-timeout | Specifies transport protocol and response-timeout period.  
  response-timeout must be an integer from 60 through 1000.  
  Default: 300 seconds  
  
 Cisco ASR 5x00 Command Line Interface Reference 459
**firewall port-scan**

- **tcp**: Specifies response timeout for TCP.
  
  ```bash
tcp
  response_timeout must be an integer from through 30.
  ```

- **response_timeout** must be an integer from through 60.

  Default: 3 seconds

**scanner-policy { block inactivity-timeout inactivity_timeout | log-only }**

Specifies how to treat packets from a source address that has been detected as a scanner.

- **block inactivity-timeout inactivity_timeout**: Specifies blocking any subsequent traffic from the scanner. If the scanner is found to be inactive for the inactivity-timeout period, then the scanner is no longer blocked, and traffic is allowed.

  ```bash
  inactivity_timeout specifies the scanner inactivity timeout period, in seconds, and must be an integer from 1 through 4294967295.
  ```

- **log-only**: Specifies logging scanner information without blocking scanner traffic.

  Default: log-only

**Usage**

Use this command to configure the Stateful Firewall Port Scan Detection algorithm enabled by the `firewall dos-protection port-scan` CLI command.

This protection tracks all uplink source addresses, and the packets they initiate towards all subscribers that have this protection enabled.

**Example**

The following command configures the Stateful Firewall Port Scan inactivity timeout setting to 900 seconds:

```bash
firewall port-scan inactivity-timeout 900
```
firewall ruledef

This command allows you to create/configure/delete Stateful Firewall ruledefs.

**Important:** This command is available only in StarOS 8.1. This command must be used to configure the Rulebase-based Stateful Firewall and NAT features.

<table>
<thead>
<tr>
<th>Product</th>
<th>PSF</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privilege</td>
<td>Security Administrator, Administrator</td>
</tr>
<tr>
<td>Mode</td>
<td>Exec &gt; ACS Configuration</td>
</tr>
</tbody>
</table>

active-charging service service_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs)#

**Syntax**

```
firewall ruledef firewall_ruledef_name [ -noconfirm ]

no firewall ruledef firewall_ruledef_name
```

**Usage**

Use this command to create/configure/delete a Stateful Firewall ruledef. A Stateful Firewall ruledef contains different conditions to permit, drop, or reject a packet/connection/traffic based on one or more parameters. The ruledef name must be unique within the active charging service. Host pool, port map, IMSI pool, and Stateful Firewall, routing, and charging ruledefs must have unique names. A Stateful Firewall ruledef can be referenced by multiple Stateful Firewall rulebases.

```
firewall_ruledef_name

Specifies the Stateful Firewall ruledef to add/configure/delete.
```

```
firewall_ruledef_name

must be the name of a Stateful Firewall ruledef, and must be an alphanumeric string of 1 through 63 characters and can contain punctuation characters. Each ruledef must have a unique name.
```

If the named ruledef does not exist, it is created, and the CLI mode changes to the Firewall Ruledef Configuration Mode wherein the ruledef can be configured.

If the named Stateful Firewall ruledef already exists, the CLI mode changes to the Firewall Ruledef Configuration Mode for that ruledef.

```
-noconfirm

Specifies that the command must execute without prompting for confirmation.
```
**Important:** The Stateful Firewall ruledefs are different from the ACS ruledefs.

Also see the *Firewall-and-NAT Access Ruledef Configuration Mode Commands* chapter.

**Example**

The following command creates a Stateful Firewall ruledef named `fw_ruledef1`, and enters the Firewall Ruledef Configuration Mode:

```
firewall ruledef fw_ruledef1
```
**firewall tcp-syn-flood-intercept**

**Description** In StarOS 8.1 and later releases, for Rulebase-based Stateful Firewall this command is available in the ACS Rulebase Configuration Mode, and for Policy-based Stateful Firewall in the Firewall-and-NAT Policy Configuration Mode. In StarOS 8.3, this command is available in the ACS Rulebase Configuration Mode.
firewall track-list

This command allows you to configure the maximum number of server IP addresses to be tracked that are involved in any kind of denial-of-service (DoS) attacks.

Product
PSF

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration

Syntax

firewall track-list attacking-servers no_of_servers

{ default | no } firewall track-list attacking-servers

default
Configures this command with its default setting.
Default: 10 servers

no

Important: This command variant is available only in StarOS 8.3 and later releases.

If previously configured, deletes the configuration from the active charging service.

attacking-servers no_of_servers

Specifies the maximum number of servers to track.
no_of_servers must be an integer from 1 through 100.

Usage
Use this command to configure the maximum number of server IP addresses to be tracked that are involved in any kind of DoS attacks.

Example
The following command configures the maximum number of server IP addresses to be tracked that are involved in any kind of DoS attacks to 20:

firewall track-list attacking-servers 20
fw-and-nat action

This command allows you to create/configure/delete Firewall-and-NAT actions.

**Important:** This command is available only in 11.0 and later releases. This command must be used to configure the Stateful Firewall and NAT Action.

**Product**
PSF
NAT

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration

```
active-charging service service_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

**Syntax**

```
fw-and-nat action action_name [ -noconfirm ]
```

```
no fw-and-nat action action_name
```

**no**
If previously configured, deletes the specified Firewall-and-NAT action from the active charging service.

```
action_name
```
Specifies the Firewall-and-NAT action to add/configure/delete.
`action_name` must be the name of a Firewall-and-NAT action, and must be an alphanumeric string of 1 through 63 characters. Each Firewall-and-NAT action must have a unique name.

```
-noconfirm
```
Specifies that the command must execute without prompting for confirmation.

**Usage**
Use this command to create/configure/delete a Firewall-and-NAT action.
On entering this command, the CLI prompt changes to:
```
[context_name]hostname(config-fw-and-nat-action)#
```
Also see the *Firewall-and-NAT Action Configuration Mode Commands* chapter.

**Example**
The following command creates a Firewall-and-NAT action named `test1`, and changes to the Firewall-and-NAT Action Configuration Mode:
fw-and-nat action test1
fw-and-nat policy

This command allows you to create/configure/delete Firewall-and-NAT policies.

**Important:** This command is available only in StarOS 8.1 and in StarOS 9.0 and later releases. This command must be used to configure the Policy-based Stateful Firewall and NAT features.

**Product**
- PSF
- NAT

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > ACS Configuration

```plaintext
active-charging service service_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acsc)#
```

**Syntax**

```
fw-and-nat policy policy_name [ -noconfirm ]
no fw-and-nat policy fw_nat_policy_name
```

- **fw-and-nat policy policy_name**
  - Specifies the Firewall-and-NAT policy to add/configure/delete.
  - `fw_nat_policy_name` must be the name of a Firewall-and-NAT policy, and must be an alphanumeric string of 1 through 63 characters. Each Firewall-and-NAT policy must have a unique name.

- **-noconfirm**
  - Specifies that the command must execute without prompting for confirmation.

**Usage**

- Use this command to create/configure/delete a Firewall-and-NAT policy.
- On entering this command, the CLI prompt changes to:
  ```plaintext
  [context_name]hostname(config-fw-and-nat-policy)#
  ```
Also see the *Firewall-and-NAT Policy Configuration Mode Commands* chapter.

**Example**

The following command creates a Firewall-and-NAT policy named `test321`, and changes to the Firewall-and-NAT Policy Configuration Mode:

```
fw-and-nat policy test321
```
group-of-objects

This command allows you to create/configure/delete an ACS group-of-objects.

**Important:** This command is available only in StarOS 10.2 and later releases.

**Important:** A maximum of 16 object groups can be configured in the active charging service. And a maximum of 128 objects can be configured within each object group.

### Product
ACS

### Privilege
Security Administrator, Administrator

### Mode
Exec > ACS Configuration

```
active-charging service service_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

### Syntax

```
group-of-objects objects_group_name [ type string [ -noconfirm ] ]

no group-of-objects objects_group_name
```

- **no**
  - If previously configured, deletes the specified group-of-objects from the active charging service.

- **objects_group_name**
  - Specifies the group-of-objects to add/configure/delete.
  - `objects_group_name` must be the name of a group-of-objects, and must be an alphanumeric string of 1 through 63 characters. Each group-of-objects must have a unique name.
  - If the named group-of-objects does not exist, it is created, and the CLI mode changes to the ACS Group-of-Objects Configuration Mode wherein the group can be configured.
  - If the named group-of-objects already exists, the CLI mode changes to the ACS Group-of-Objects Configuration Mode for that group.

- **type**
  - Specifies the data type for the group-of-objects.

**Important:** “string” is the only data type supported in this release.
**string**

Specifies the data type as string.
When creating a group, specifying the data type is mandatory.
When modifying an existing group, specifying the data type is optional.

**-noconfirm**

Specifies that the command must execute without prompting for confirmation.

**Usage**

Use this command to create/configure/delete a group-of-objects.
On entering this command, the CLI prompt changes to:

```
[context_name] hostname(config-acs-group-of-objects)#
```

Also see the *ACS Group-of-Objects Configuration Mode Commands* chapter.

**Example**

The following command creates a group-of-objects named `test4` with the data type string, and enters the ACS Group-of-Objects Configuration Mode:

```
group-of-objects test4 type string
```
group-of-prefixed-urls

This command allows you to create/configure/delete an ACS group-of-prefixed-URLs.

Important: This command is customer specific. For more information contact your Cisco account representative.

Important: A maximum of 64 group-of-prefixed-URL groups can be configured in the active charging service.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration
active-charging service service_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-ac)#

Syntax

group-of-prefixed-urls prefixed_urls_group_name [ -noconfirm ]

no group-of-prefixed-urls prefixed_urls_group_name

no
If previously configured, deletes the specified group-of-prefixed-urls from the active charging service.

prefixed_urls_group_name
Specifies the group-of-prefixed-urls to add/configure/delete.
prefixed_urls_group_name must be the name of a group-of-prefixed-urls, and must be an alphanumeric string of 1 through 63 characters. Each group-of-prefixed-urls must have a unique name.
If the named group-of-prefixed-urls does not exist, it is created, and the CLI mode changes to the ACS Group-of-Prefixed-URLs Configuration Mode wherein the group can be configured.
If the named group-of-prefixed-urls already exists, the CLI mode changes to the ACS Group-of-Prefixed-URLs Configuration Mode for that group.

-noconfirm
Specifies that the command must execute without prompting for confirmation.

Usage
Use this command to create/configure/delete a group-of-prefixed-URLs.
On entering this command, the CLI prompt changes to:
[context_name]hostname(config-ac)#
Also see the ACS Group-of-Prefixed-URLs Configuration Mode Commands chapter.
Example

The following command creates group-of-prefixed-urls named `test5`, and enters the ACS Group-of-Prefixed-URLs Configuration Mode:

```
    group-of-prefixed-urls test5
```
group-of-ruledefs

This command allows you to create/configure/delete an ACS group-of-ruledefs.

**Important:** In 14.1 and earlier releases, a maximum of 64 group-of-ruledefs can be configured in the active charging service. In 15.0 and later releases, a maximum of 128 group-of-ruledefs can be configured.

Product

ACS

Privilege

Security Administrator, Administrator

Mode

Exec > ACS Configuration

```
active-charging service service_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ac)#
```

Syntax

```
group-of-ruledefs ruledefs_group_name [ -noconfirm ]
```

```
no group-of-ruledefs ruledefs_group_name
```

*no*

If previously configured, deletes the specified group-of-ruledefs from the active charging service.

```
ruledefs_group_name
```

Specifies the group-of-ruledefs to add/configure/delete.

*ruledefs_group_name* must be unique within the active charging service, and must be an alphanumeric string of 1 through 63 characters. Each group-of-ruledefs must have a unique name.

If the named group-of-ruledefs does not exist, it is created, and the CLI mode changes to the ACS Group-of-Ruledefs Configuration Mode wherein the group can be configured.

If the named group-of-ruledefs already exists, the CLI mode changes to the ACS Group-of-Ruledefs Configuration Mode for that group.

```
-noconfirm
```

Specifies that the command must execute without prompting for confirmation.

Usage

Use this command to create/configure/delete a group-of-ruledefs.

A group-of-ruledefs is a collection of rule definitions to use in access policy creation.

On entering this command, the CLI prompt changes to:

```
[context_name]hostname(config-group-of-ruledefs)#
```

Example

Also see the *ACS Group-of-Ruledefs Configuration Mode Commands* chapter.
The following command creates a group-of-ruledefs named `group1`, and enters the ACS Group-of-Ruledefs Configuration Mode:

```
group-of-ruledefs group1
```
h323 time-to-live

This command allows you to configure the time period for which an endpoint’s registration to an H.323 gatekeeper is valid.

Product
NAT

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration
active-charging service service_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs)#

Syntax

h323 time-to-live timeout
default h323 time-to-live

Usage

Use this command to configure the time period for which an endpoint’s registration to a gatekeeper is valid.

Example

The following command configures the time for an endpoint registration with a timeout setting of 5 seconds:

h323 time-to-live 5
### h323 timeout

This command allows you to configure the timeout intervals for various H.323 requests.

**Product**

NAT

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > ACS Configuration

```
active-charging service service_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

**Syntax**

```
h323 timeout { admission admission_timeout | discovery discovery_timeout | location location_timeout | registration registration_timeout | unregistration unregistration_timeout }

default h323 timeout { admission | discovery | location | registration | unregistration }
```

- **default**
  
  Configures this command with the default setting for the specified parameters.

- **admission admission_timeout**
  
  Configures the timeout value for the admission request sent to the gatekeeper.
  
  `admission_timeout` must be an integer from 1 through 20.
  
  Default: 10 seconds

- **discovery discovery_timeout**
  
  Configures the timeout value for the gatekeeper request message sent to the Gatekeeper.
  
  `discovery_timeout` must be an integer from 1 through 20.
  
  Default: 10 seconds

- **location location_timeout**
  
  Configures the timeout value for the location request message sent to the Gatekeeper.
  
  `location_timeout` must be an integer from 1 through 20.
  
  Default: 10 seconds

- **registration registration_timeout**
  
  Configures the timeout value for the registration request message sent to the Gatekeeper.
  
  `registration_timeout` must be an integer from 1 through 20.
  
  Default: 6 seconds
unregistration unregistration_timeout

Configures the timeout value for the unregistration request message sent to the Gatekeeper.
unregistration_timeout must be an integer from 1 through 20.
Default: 3 seconds

Usage
Use this command to configure the timeout interval for the various H.323 requests.

Example
The following command configures the admission request message with a timeout value of 15 seconds:

h323 timeout admission 15
h323 tpkt

This command allows you to configure the maximum size of Transport Protocol Data Unit Packets (TPKT) that the H.323 Application Layer Gateway (ALG) can handle.

Product
NAT

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration

active-charging service service_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs)#

Syntax

h323 tpkt max_tpkt_size

default h323 tpkt

    default
    Configures this command with its default setting.
    Default: 2048 bytes

    max_tpkt_size
    Specifies the maximum TPKT size, in bytes.
    max_tpkt_size must be an integer from 4 through 4096.

Usage

Use this command to configure the maximum packet size for the H.323 ALG.

Example

The following command configures a maximum TPKT packet size of 100 bytes:

    h323 tpkt 100
h323 version

This command allows you to configure the H.323 version number supported by an H.323 Application Layer Gateway (ALG).

Product
NAT

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration

active-charging service service_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs)#

Syntax

h323 version h323_version_number

default h323 version

default

Configures this command with its default setting.
Default: 5

h323_version_number

Specifies the H.323 version number.
h323_version_number must be an integer from 1 through 7.

Usage

Use this command to configure the H.323 version number supported by the H.323 ALG.

Example

The following command configures the H.323 version as 1:

h323 version 1
**host-pool**

This command allows you to create/configure/delete host pools.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration

*active-charging service service_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

**Syntax**

```
host-pool host_pool_name [ -noconfirm ]
no host-pool host_pool_name
```

- **no**
  If previously configured, deletes the specified host pool from the active charging service.

- **host_pool_name**
  Specifies the host pool to add/configure/delete.
  *host_pool_name* must be the name of a host pool, and must be an alphanumeric string of 1 through 63 characters and can contain punctuation characters. Each host pool must have a unique name.
  If the named host pool does not exist, it is created, and the CLI mode changes to the ACS Host Pool Configuration Mode wherein the host pool can be configured.
  If the named host pool already exists, the CLI mode changes to the ACS Host Pool Configuration Mode for that host pool.

- **-noconfirm**
  Specifies that the command must execute without prompting for confirmation.

**Usage**

Use this command to create/configure/delete ACS host pools.
A host pool is a collection of hosts and IP addresses to use in access policy creation. The host pool name must be unique with in the service. Host pool, port map, IMSI pool, and firewall, routing, and charging ruledefs must have unique names. A maximum of the 256 host pools can be created.

**Important:** Host pools configured in other ruledefs cannot be deleted.

On entering this command, the CLI prompt changes to:

```
[context_name]hostname(config-acb-host-pool)#
```
Also see the *ACS Host Pool Configuration Mode Commands* chapter.

**Example**

The following command creates a host pool named `hostpool1`, and enters the ACS Host Pool Configuration Mode:

```
host-pool hostpool1
```
idle-timeout

This command allows you to configure the maximum duration a flow can remain idle for, after which the system automatically terminates the flow.

Product
ACS
NAT
PSF

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration

```
active-charging service service_name
```

Entering the above command sequence results in the following prompt:

```
[lhost_name(config-acs)]#
```

Syntax

```
idle-timeout { alg-media | flow-mapping { tcp | udp } | icmp | tcp [ half-open ] | udp }

idle_timeout

{ default | no } idle-timeout { alg-media | flow-mapping { tcp | udp } | icmp | tcp [ half-open ] | udp }
```

---

default
Configures this command with the default setting for the specified parameter.
Default:

- **alg-media**: 120 seconds
- **flow-mapping { tcp | udp }**: 300 seconds for TCP and 0 seconds for UDP
- **icmp, tcp, udp**: 300 seconds
- **tcp half-open**: 200 seconds

---

no
Disables the idle-timeout configuration for the specified flow.

---

alg-media
Configures the ALG media for the specified flow.

---

flow-mapping { tcp | udp }

The Flow Mapping timer is an extension to the existing flow idle-timeout in ACS. This flow mapping timeout applies only for NAT enabled calls and is supported only for TCP and UDP flows. The purpose of this timer is to hold the resources (NAT IP, NAT port, Private IP NPU flow) associated with a 5-tuple flow until Mapping timeout expiry.
If the Flow Mapping timer is disabled, then the Mapping timeout will not get triggered for UDP/TCP idle timed out flows. The resources such as NAT mapping will be released along with the 5-tuple flow.

```
icmp
```

Configures the ICMP protocol for the specified flow.

```
tcp [ half-open ]
```

Configures the TCP protocol for the specified flow.

Use the `half-open` keyword to configure timeout interval for half-open TCP flows.

```
udp
```

Configures the UDP protocol for the specified flow.

```
idle_timeout
```

Specifies the timeout duration, in seconds, and must be an integer from 0 through 86400. For `alg-media` specifies the media inactivity timeout. The `idle_timeout` value gets applied on RTP and RTCP media flows that are created for SIP/H.323 calls. The timeout is applied only on those flows that actually match the RTP and RTCP media pinholes that are created by the SIP/H.323 ALG. A value of 0 disables the idle-timeout setting.

**Usage**

Use this command to configure the maximum duration a flow can remain idle, in seconds, after which the system automatically terminates the flow.

Setting the value to 0 will cause the idle-timeout setting to be disabled.

For flows other than TCP, UDP and ICMP, timeout value will always be 300 seconds (unless configured in the charging-action). Charging action’s flow idle-timeout will have precedence over ACS idle-timeout. If charging action’s flow idle-timeout is default, then flows will have the value configured in the active charging service.

**Example**

The following command configures the maximum duration a TCP flow can remain idle to 3000 seconds, after which the system automatically terminates the flow:

```
idle-timeout tcp 3000
```
**imsi-pool**

This command allows you to create/configure/delete International Mobile Subscriber Identity (IMSI) pools.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration

**Syntax**

```
imsi-pool imsi_pool_name [ -noconfirm ]

no imsi-pool imsi_pool_name
```

- **no**
  If previously configured, deletes the specified IMSI pool from the active charging service.

- **imsi_pool_name**
  Specifies the IMSI pool to add/configure/delete.
  `imsi_pool_name` must be the name of an IMSI pool, and must be an alphanumeric string of 1 through 63 characters, and can contain punctuation characters. Each IMSI pool must have a unique name.
  If the named IMSI pool does not exist, it is created, and the CLI mode changes to the ACS IMSI Pool Configuration Mode wherein the IMSI pool can be configured.
  If the named IMSI pool already exists, the CLI mode changes to the ACS IMSI Pool Configuration Mode for that IMSI pool.

- **-noconfirm**
  Specifies that the command must execute without prompting for confirmation.

**Usage**

Use this command to create/configure/delete pools of International Mobile Subscriber Identifier (IMSI) numbers having group of single or range of IMSI numbers to use in access policy creation. The IMSI pool name must be unique with in the service. Host pool, port map, IMSI pool, and firewall, routing, and charging ruledefs must have unique names. A maximum of 256 IMSI pools can be created.

**Important:** IMSI pools configured in other ruledefs cannot be deleted.

On entering this command, the CLI prompt changes to:

```
[context_name]hostname(config-acs-imsi-pool)#
```
Example

The following command creates an IMSI pool named `imsipool1`, and enters the ACS IMSI Pool Configuration Mode:

```
imsi-pool imsipool1
```
ip dns-learnt-entries

This command allows you to configure how long to keep the snooped IPv4 addresses that were extracted from DNS responses.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration
active-charging service service_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs)#

Syntax

ip dns-learnt-entries timeout timeout_period
{ default | no } ip dns-learnt-entries timeout

default
Configures this command with the default DNS-learnt-entries timeout setting.
Default: 300 seconds

no
Specifies to always use the TTL value in the DNS response, and not the timeout configured with this command.

timeout_period
Specifies the DNS-learnt-entries timeout period, in seconds.
timeout_period must be an integer from 1 through 2147483647.

Usage

Use this command to configure how long to keep the snooped IPv4 addresses that were extracted from DNS responses—for the TTL specified in the DNS response, or for the time period configured with this command, if greater.
The configurable timer will be at global ECS level and shared across all IP addresses. Internally, a five-minute (300 seconds, non configurable) timer will be started whenever DNS analyzer is enabled. On timeout of this timer, all the learnt IP addresses will be checked for TTL expiry and the expired entries will be flushed.

Example

The following command specifies to keep the snooped IPv4 addresses that were extracted from DNS responses for a time period of 900 seconds, or for the TTL value specified in the DNS response, whichever is greater:
ip dns-learnt-entries timeout 900
ip max-fragments

This command allows you to limit the maximum number of IPv4/IPv6 fragments per fragment chain.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration

active-charging service service_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs)#

**Syntax**

```
ip max-fragments max.fragments
```

**default ip max-fragments**

```
default
Configures this command with its default setting.
Default: 45
```

```
max.fragments
```

Specifies the maximum number of IPv4/IPv6 fragments per fragment chain.

*max.fragments* must be an integer from 1 through 300.

**Usage**

Use this command to limit the maximum number of IPv4/IPv6 fragments.

**Example**

The following command limits the maximum number of IPv4/IPv6 fragments to **100**: 

```
ip max-fragments 100
```
label content-id

This command allows you to specify a label (text string) to associate with a content ID for UDRs/EDRs/eG-CDRs.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration

```
active-charging service service_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs) #
```

**Syntax**

```
label content-id content_id text label_text

no label content-id content_id
```

- **content-id content_id**
  Specifies the content ID to associate with the label.
  *content_id* must be an integer from 1 through 65535.

- **text label_text**
  Specifies the label to associate with the specified content ID.
  *label_text* must be an alphanumeric string of 1 through 64 characters.

**Usage**

Use this command to create a text label to associate with a content ID.
A maximum of 2048 labels can be configured in the active charging service.

**Example**

The following command creates the label *test_charge1* to be associated with the content ID 1378:

```
label content-id 1378 text test_charge1
```
nat allocation-failure

This command allows you to configure the action to take when NAT IP/Port allocation fails.

**Important:** This command is available only in StarOS 8.3 and later releases.

<table>
<thead>
<tr>
<th>Product</th>
<th>NAT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privilege</td>
<td>Security Administrator, Administrator</td>
</tr>
<tr>
<td>Mode</td>
<td>Exec &gt; ACS Configuration</td>
</tr>
</tbody>
</table>

active-charging service service_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs)#

**Syntax**

```
nat allocation-failure send-icmp-dest-unreachable

{ default | no } nat allocation-failure
```

- **default**
  - Configures this command with its default setting.
  - Default: Packets are dropped silently

- **no**
  - If previously enabled, disables the NAT Allocation Failure configuration. Packets are dropped silently.

- **nat allocation-failure send-icmp-dest-unreachable**
  - Specifies to send ICMP Destination Unreachable message when NAT IP/Port allocation fails.

**Usage**

Use this command to configure the action to take when NAT IP/port allocation fails—to send or not to send an “ICMP destination unreachable message” when a NAT IP/port cannot be assigned to a flow in data path.

**Example**

The following command configures sending ICMP Destination Unreachable message when NAT IP/Port allocation fails:

```
nat allocation-failure send-icmp-dest-unreachable
```
**nat allocation-in-progress**

This command allows you to configure the action to take on packets when NAT IP/NPU allocation is in progress.

**Important:** This command is available only in StarOS 8.3 and later releases.

**Product**  
NAT

**Privilege**  
Security Administrator, Administrator

**Mode**  
Exec > ACS Configuration

```
active-charging service service_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

**Syntax**

```
nat allocation-in-progress { buffer | drop }
```

```
default nat allocation-in-progress
```

**Usage**

In On-demand NAT IP allocation (wherein NAT IP address is allocated to the subscriber when a packet is being sent), if no free NAT IP address is available, a NAT-IP Alloc Request is sent to the VPNMgr to get NAT-IP. During that time packets are dropped. This command enables buffering the packets received when IP Alloc Request is sent to VPNMgr.

**Example**

The following command specifies to buffer packets when NAT IP/NPU allocation is in progress:

```
nat allocation-in-progress buffer
```
nat ip downlink reassembly-timeout

This command configures the downlink IP reassembly timer.

**Product**
NAT

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration

```
active-charging service service_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

**Syntax**

```
[ default ] nat ip downlink reassembly-timeout timeout
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Configures this command with its default setting. Default: 2000 milliseconds</td>
</tr>
<tr>
<td>timeout</td>
<td>The maximum duration for which IP packet fragments can be retained, in milliseconds. <code>timeout</code> must be an integer from 1 through 3000.</td>
</tr>
</tbody>
</table>

**Usage**

Use this command to configure the downlink IP reassembly timer by setting the duration for which IP packet fragments can be retained.

**Example**

The following command configures the duration for IP packet fragments with a timeout setting of **3000** seconds:

```
nat ip downlink reassembly-timeout 3000
```
**nat tcp-2msl-timeout**

This command allows you to configure the TCP 2MSL (Maximum Segment Lifetime) timeout value for NAT.

> **Important:** This command is available only in StarOS 8.3 and later releases.

**Product**
NAT

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration

```plaintext
active-charging service service_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

**Syntax**

```plaintext
nat tcp-2msl-timeout timeout

default nat tcp-2msl-timeout
```

- **default**
  
  Configures this command with its default setting. Default: 60 seconds

- **timeout**
  
  Specifies the TCP 2MSL timeout period, in seconds. `timeout` must be an integer from 30 through 240.

**Usage**

Use this command to configure the TCP 2MSL timeout value for NAT.

**Example**

The following command configures the TCP 2MSL timeout for NAT to 120 seconds:

```
nat tcp-2msl-timeout 120
```
nat unsolicited-pkts

This command allows you to configure unsolicited packets.

Product
ACS  
NAT

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration
active-charging service service_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-ac)#

Syntax

nat unsolicited-pkts { icmp-host-unreachable { max-rate packets_num } | server-list { max-limit servers_num } }

[ default | no ] nat unsolicited-pkts { icmp-host-unreachable | server-list }

---

default
Configures this command with its default setting.
Default: Disabled

no
Configures this command with its default setting.

---

icmp-host-unreachable max-rate packets_max
Configures the maximum number of allowed ICMP response packets, in seconds.
packets_max must be an integer from 1 through 100.

---

server-list max-limit servers_num
Configures the maximum number of servers to be stored per Session Manager instance.
servers_num must be an integer from 2 through 50.

---

Usage
Use the following command to configure the number of allowed ICMP responses and the number of servers where most number of unsolicited packets are received.

Example

The following command configures the number of allowed ICMP responses per second to 10:

```
nat unsolicited-pkts host-unreachable max-rate 10
```

The following command configures the number of servers to be stored as 20:

```
nat unsolicited-pkts server-list max-limit 20
```
p2p-detection attribute

This command enables or disables the detection of SSL renegotiation flows.

**Product**
ADC

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration

`active-charging service service_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

**Syntax**

```
[ no ] p2p-detection attribute \{ attribute_list \[ sub_attribute_name sub_attribute_value \] \}
```

- **no**
  - If previously enabled, disables detection of SSL renegotiation flows.

- **attribute_list**
  - List of configurable P2P detection attributes populated from the currently loaded P2P plugin.
  - Supported attribute: `ssl-renegotiation`

- **sub_attribute_name**
  - List of configurable P2P detection sub-attributes related to the attribute selected from the attribute list. This list is populated from the currently loaded P2P plugin.
  - Supported sub-attributes if selected attribute is `ssl-renegotiation`:
    - `max-entry-per-sessmgr`: Specifies maximum SSL Session IDs tracked per session manager.
    - `id-reduce-factor`: Specifies by how much factor the SSL ID is stored in the SSL Session ID tracker table. Possible values are 1, 2, 4.

- **sub_attribute_value**
  - Value of the selected sub-attribute. If sub-attribute is not specified, the default value set in the P2P plugin will be used.
  - The value for `max-entry-per-sessmgr` must be an integer from 1 through 65535. Default: 20000
  - Possible values for `id-reduce-factor` are 1,2,4. Default: 4

**Usage**

Use this command to enable or disable the detection of SSL renegotiation flows.

**Example**

The following command enables SSL renegotiation with SSL session IDs as 40000 and factor as 4:

```
```
p2p-detection attribute ssl-renegotiation max-entry-per-sessmgr 40000 id-reduce-factor 4
p2p-detection behavioral

This command enables or disables behavioral detection for unidentified traffic.

**Product**
ADC

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration

```
active-charging service service_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

**Syntax**

```
[ no ] p2p-detection behavioral { behavioral_list | all }
```

- **no**
  
  If previously configured, disables the behavioral configuration.

- **behavioral_list**
  
  Specifies the behavior to match. The behavioral list is the list of supported behavioral detection logic populated from the currently loaded ADC plugin.
  
  `behavioral_list` must be one of the following:
  
  - **all**
    
    Enables all behavioral detection types supported by the ADC plugin
  
  - **download**
    
    Detects unknown flows which are data download using behavioral analysis
  
  - **p2p**
    
    Detects P2P and file sharing protocols using behavioral analysis
  
  - **upload**
    
    Detects unknown flows which are data upload using behavioral analysis
  
  - **voip**
    
    Detects VoIP (voice and video) protocols using behavioral analysis

**Usage**

Use this command to enable or disable behavioral detection for unidentified traffic. Behavioral VoIP is meant for zero day detection of VoIP traffic. Behavioral upload/download is similar to client-server upload/download using HTTP, FTP, SFTP, etc. It must also detect flows of non-standard ports which ECS cannot detect and falls under the client-server model. The behavioral feature is disabled by default.

**Example**

The following command specifies to configure behavioral VoIP:

```
p2p-detection behavioral voip
```
p2p-detection ecs-analysis

This command enables or disables ECS analysis for analyzers — FTP, HTTP, RTSP and SIP.

**Product**
ADC

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration

```plaintext
active-charging service service_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(configacs)#
```

**Syntax**

```
[ no ] p2p-detection ecs-analysis { all | ftp | http | rtsp | sip }
```

- **no**
  If previously enabled, disables the configured analyzers.

- **all**
  ECS analysis for all analyzers — FTP, HTTP, RTSP and SIP.

- **ftp**
  ECS analysis for FTP analyzer.

- **http**
  ECS analysis for HTTP analyzer.

- **rtsp**
  ECS analysis for RTSP analyzer.

- **sip**
  ECS analysis for SIP analyzer.

**Usage**

Use this command to enable or disable the interworking of analyzers — FTP, HTTP, RTSP and SIP. This feature is enabled by default if P2P protocols are enabled.

**Example**

The following command enables ECS analysis for the **ftp** analyzer:

```
p2p-detection ecs-analysis ftp
```
p2p-detection protocol

This command enables/disables the detection of all or specified peer-to-peer (P2P) protocols.

**Product**
ADC

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration

`active-charging service service_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

**Syntax**

```
[ no ] p2p-detection protocol [ actionvoip | actsync | adobeconnect | aimini | all | amazoncloud | antsp2p | apple-push | apple-store | applejuice | applemaps | ares | armagetron | avi | badoo | baidumovie | battlefld | bbm | bitcasa | bittorrent | bittorrent-sync | blackberry-store blackberry | blackdialer | box | callofduty | chikka | cisco-jabber | citrix | clubpenguin | clubbox | comodounite | crossfire | cyberghost | ddlink | ddi | directconnect | dofus | dropbox | ed buddy | edonkey | facebook | facetime | fasttrack | feidian | ficall | fiesta | filetopia | flash | flickr | florencia | foursquare | freenet | friendster | fring | funshion | gadugadu | gamekit | gmail | gnutella | goober | google-music | google-push | google | googleplay | googleplus | gotomeeting | gtalk | guildwars | halflife2 | hamachi | hbogo | heytell | hike-messenger | hls | hotspotvpn | hulu | hyves | iax | icall | icecast | icloud | idrive | igo | ihearthradio | imesh | imessage | imgur | imo | implus | instagram | iplayer | iptv | irc | isakmp | iskoot | itunes | jabber | jap | jumbl | kakaotalk | kik-messenger | kontiki | kugoo | kuro | linkedin | lync | magicjack | manolito | mapfactor | mapi | maplestory | meebo | mgcp | mig33 | mojo | monkey3 | mozy | msn | msrp | mute | mypeople | myspace | nateontalk | naverline | navigon | netflix | netmotion | nimbuzz | nokia-store | octoshape | off | ogg | oist | oovoo | opendrive | openft | openvpn | operamini | orb | osar | outlook | paltalk | pando | pandora | path | pcanywhere | pinterest | plingm | poco | popo | pplive | ppstream | ps3 | qq | qggame | qqlive | quake | quicktime | radio-paradise | rd | rdt | regram | rfactor | rhapsody | rmstream | rodi | rynga | samsung-store | scydo | seconline | shoutcast | silverlight | siri | skinny | skydrive | skype | slackerradio | slingbox | smartvoip | snapchat | softether | sopcast | soribada | soulseek | spdy | speedtest | splashfighter | spotify | ssdp | stealthnet | steam | stun | sudaphone | svtplay | tagged | talkatone | tango | teamspeak | teamviewer | telegram | thunder | tor | truecaller | truphone | tumblr | tunnelvoice | tvants | tvuplayer | twitch | twitter | ultrabac | ultrasurf | upc-phone | usenet | ustream | uusee | vchat | vechtv | viber | vine | voipdiscount | vopium | voxer | vvpn | vtok | vtun | warcft3 | waze | wes | wechat | weibo | whatsapp | wii | windows-azure | windows-store | winmx | winny | wmstream | wofkungfu | wofwarcraft | wuala | xbo | xdcc | xing | yahoo | yahoomail | youku | yourfreetunnel | youtube | zattoo + ]
```
no
If previously enabled, disables the detection of the specific peer-to-peer protocol.

all
Specifies to detect all supported P2P protocols.
In 12.2 and earlier releases: Specifying all is the same as configuring each of the following protocols individually.
In 14.0 and later releases: Specifying all means all of the protocols supported by the currently loaded plugin.

actionvoip
Specifies to detect ActionVoip protocol.

actsync
Specifies to detect ActiveSync protocol.

adobeconnect
Specifies to detect Adobe Connect protocol.

aimini
Specifies to detect Aimini protocol.

amazoncloud
Specifies to detect AmazonCloud protocol.

antsp2p
Specifies to detect ANts P2P protocol.

apple-push
Specifies to detect Apple Push Notification protocol.

apple-store
Specifies to detect iPhone Appstore protocol.

applejuice
Specifies to detect Applejuice protocol.

applemaps
Specifies to detect Apple Maps protocol.

ares
Specifies to detect Ares Galaxy protocol.

armagettron
Specifies to detect Armagetron protocol.
avi
Specifies to detect AVI protocol.

badoo
Specifies to detect Badoo protocol.

battlefield
Specifies to detect Battlefield protocol.

bbm
Specifies to detect BBM protocol.

bitcasa
Specifies to detect Bitcasa protocol.

bittorrent
Specifies to detect BitTorrent protocol.

bittorrent-sync
Specifies to detect BitTorrent Sync protocol.

blackberry-store
Specifies to detect Blackberry World protocol.

blackberry
Specifies to detect BlackBerry protocol.

blackdialer
Specifies to detect Blackdialer protocol.

box
Specifies to detect BOX protocol.

callofduty
Specifies to detect Call of Duty protocol.

chikka
Specifies to detect Chikka protocol.

cisco-jabber
Specifies to detect Cisco Jabber protocol.

citrix
Specifies to detect Citrix Independent Computing Architecture (ICA) protocol.
clubbox
Specifies to detect Clubbox protocol.

clubpenguin
Specifies to detect Club Penguin protocol.

comodounite
Specifies to detect Comodo EasyVPN protocol.

cyberghost
Specifies to detect CyberGhost VPN protocol.

crossfire
Specifies to detect Crossfire protocol.

ddlink
Specifies to detect DDLink protocol.

didi
Specifies to detect DiDi protocol.

directconnect
Specifies to detect Direct Connect protocol.

dofus
Specifies to detect DOFUS protocol.

dropbox
Specifies to detect Dropbox protocol.

ebuddy
Specifies to detect eBuddy protocol.

edonkey
Specifies to detect eDonkey protocol.

facebook
Specifies to detect Facebook protocol.

facetime
Specifies to detect FaceTime protocol.

Important: The facetime protocol option is available only in 9.0 and in 11.0 and later releases.
fasttrack
Specifies to detect FastTrack protocol.

feidian
Specifies to detect Feidian protocol.

ficall
Specifies to detect Ficall protocol.

fiesta
Specifies to detect FIESTA protocol.

filetopia
Specifies to detect Filetopia protocol.

flash
Specifies to detect Flash protocol.

flickr
Specifies to detect Flickr protocol.

florensia
Specifies to detect Florensia protocol.

foursquare
Specifies to detect Foursquare protocol.

freenet
Specifies to detect Freenet protocol.

friendster
Specifies to detect Friendster protocol.

fring
Specifies to detect Fring SIP protocol.

funshion
Specifies to detect Funshion protocol.

gadugadu
Specifies to detect Gadu-Gadu protocol.

gamekit
Specifies to detect GameKit protocol.
## Important: The gamekit protocol option is available only in 9.0 and in 11.0 and later releases.

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>gmail</code></td>
<td>Specifies to detect Gmail protocol.</td>
</tr>
<tr>
<td><code>gnutella</code></td>
<td>Specifies to detect Gnutella protocol.</td>
</tr>
<tr>
<td><code>goober</code></td>
<td>Specifies to detect Goober protocol.</td>
</tr>
<tr>
<td><code>google-music</code></td>
<td>Specifies to detect Google Music protocol.</td>
</tr>
<tr>
<td><code>google-push</code></td>
<td>Specifies to detect Google Push Notification protocol.</td>
</tr>
<tr>
<td><code>google</code></td>
<td>Specifies to detect Google protocol.</td>
</tr>
<tr>
<td><code>googleplay</code></td>
<td>Specifies to detect GooglePlay protocol.</td>
</tr>
<tr>
<td><code>googleplus</code></td>
<td>Specifies to detect GooglePlus protocol.</td>
</tr>
<tr>
<td><code>gotomeeting</code></td>
<td>Specifies to detect Gotomeeting protocol.</td>
</tr>
<tr>
<td><code>gtalk</code></td>
<td>Specifies to detect Google Talk protocol.</td>
</tr>
<tr>
<td><code>guildwars</code></td>
<td>Specifies to detect GuildWars protocol.</td>
</tr>
<tr>
<td><code>halflife2</code></td>
<td>Specifies to detect Half-Life 2 protocol.</td>
</tr>
<tr>
<td><code>hamachivpn</code></td>
<td>Specifies to detect Hamachi VPN protocol.</td>
</tr>
<tr>
<td><code>hbogo</code></td>
<td>Specifies to detect HBO Go protocol.</td>
</tr>
</tbody>
</table>
**heytell**
Specifies to detect HeyTell protocol.

**hike-messenger**
Specifies to detect Hike Messenger protocol.

**hls**
Specifies to detect HLS protocol.

**hotspotvpn**
Specifies to detect HotSpot VPN protocol.

**hulu**
Specifies to detect Hulu protocol.

**hyves**
Specifies to detect Hyves protocol.

**iax**
Specifies to detect Inter-Asterisk eXchange protocol.

**icall**
Specifies to detect iCall protocol.

**icecast**
Specifies to detect Icecast protocol.

**icloud**
Specifies to detect iCloud protocol.

**idrive**
Specifies to detect iDrive protocol.

**igo**
Specifies to detect IGO protocol.

**iheartradio**
Specifies to detect iHeartRadio protocol.

**imesh**
Specifies to detect iMesh protocol.

**imessage**
Specifies to detect iMessage protocol.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>imgur</td>
<td>Specifies to detect Imgur protocol.</td>
</tr>
<tr>
<td>imo</td>
<td>Specifies to detect Imo.im protocol.</td>
</tr>
<tr>
<td>implus</td>
<td>Specifies to detect IM+ protocol.</td>
</tr>
<tr>
<td>instagram</td>
<td>Specifies to detect Instagram protocol.</td>
</tr>
<tr>
<td>iplayer</td>
<td>Specifies to detect BBC iPlayer protocol.</td>
</tr>
<tr>
<td>iptv</td>
<td>Specifies to detect IPTV protocol.</td>
</tr>
<tr>
<td>irc</td>
<td>Specifies to detect IRC protocol.</td>
</tr>
<tr>
<td>isakmp</td>
<td>Specifies to detect ISAKMP protocol.</td>
</tr>
<tr>
<td>iskoot</td>
<td>Specifies to detect iSkoot protocol.</td>
</tr>
<tr>
<td>itunes</td>
<td>Specifies to detect iTunes protocol.</td>
</tr>
<tr>
<td>jabber</td>
<td>Specifies to detect Jabber protocol.</td>
</tr>
<tr>
<td>jap</td>
<td>Specifies to detect Jamp protocol.</td>
</tr>
<tr>
<td>kakaotalk</td>
<td>Specifies to detect Kakao Talk protocol.</td>
</tr>
<tr>
<td>kik</td>
<td>Specifies to detect Kik Messenger protocol.</td>
</tr>
</tbody>
</table>
kontiki
Specifies to detect Kontiki delivery protocol.

kugoo
Specifies to detect Kugoo protocol.

kuro
Specifies to detect Kuro protocol.

linkedin
Specifies to detect Linkedin protocol.

lync
Specifies to detect Microsoft Lync protocol.

magicjack
Specifies to detect MagicJack protocol.

manolito
Specifies to detect MANOLITO protocol.

mapfactor

mapi
Specifies to detect MAPI protocol.

maplestory
Specifies to detect MapleStory protocol.

meebo
Specifies to detect Meebo protocol.

mgcp
Specifies to detect Media Gateway Control Protocol.

mig33
Specifies to detect Mig33 protocol.

mojo
Specifies to detect Mojo protocol.

monkey3
Specifies to detect Monkey3 protocol.
mozy
Specifies to detect Mozy protocol.

msn
Specifies to detect MSN Messenger protocol.

msrp
Specifies to detect MSRP protocol.

mute
Specifies to detect MUTE protocol.

mypeople
Specifies to detect My People protocol.

myspace
Specifies to detect MySpace protocol.

nateontalk
Specifies to detect NateOn Talk protocol.

naverline
Specifies to detect Naver Line protocol.

navigon
Specifies to detect Navigon protocol.

netflix
Specifies to detect Netflix protocol.

netmotion
Specifies to detect NetMotion Internet Mobility Protocol.

nimbuzz
Specifies to detect Nimbuzz protocol.

nokia-store
Specifies to detect Nokia Ovi Store protocol.

octoshape
Specifies to detect Octoshape protocol.

off
Specifies to detect Off-The-Record protocol.
---

`ogg`
Specifies to detect Ogg multimedia streaming protocol.

`oist`
Specifies to detect Oist protocol.

`ooVoo`
Specifies to detect ooVoo protocol.

`opendrive`
Specifies to detect Opendrive protocol.

`openft`
Specifies to detect OpenFT protocol.

`openvpn`
Specifies to detect OpenVPN protocol.

`operamini`
Specifies to detect Operamini protocol.

`orb`
Specifies to detect Internet Inter-ORB Protocol.

`oscar`
Specifies to detect Open System for CommunicAtion in Realtime protocol.

`outlook`
Specifies to detect Outlook protocol.

`paltalk`
Specifies to detect Paltalk protocol.

`pando`
Specifies to detect Pando protocol.

`pandora`
Specifies to detect Pandora protocol.

`path`
Specifies to detect Path protocol.

`PCAnywhere`
Specifies to detect PCAnywhere protocol.
<table>
<thead>
<tr>
<th>Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pinterest</td>
<td>Specifies to detect Pinterest protocol.</td>
</tr>
<tr>
<td>plingm</td>
<td>Specifies to detect Plingm protocol.</td>
</tr>
<tr>
<td>poco</td>
<td>Specifies to detect Poco protocol.</td>
</tr>
<tr>
<td>popo</td>
<td>Specifies to detect Popo protocol.</td>
</tr>
<tr>
<td>pplive</td>
<td>Specifies to detect PPlive protocol.</td>
</tr>
<tr>
<td>ppstream</td>
<td>Specifies to detect PPstream protocol.</td>
</tr>
<tr>
<td>ps3</td>
<td>Specifies to detect PS3 protocol.</td>
</tr>
<tr>
<td>qq</td>
<td>Specifies to detect Tencent QQ protocol.</td>
</tr>
<tr>
<td>qqgame</td>
<td>Specifies to detect QQgame protocol.</td>
</tr>
<tr>
<td>qqlive</td>
<td>Specifies to detect QQlive protocol.</td>
</tr>
<tr>
<td>quake</td>
<td>Specifies to detect Quake network protocol.</td>
</tr>
<tr>
<td>quicktime</td>
<td>Specifies to detect QuickTime protocol.</td>
</tr>
<tr>
<td>radio-paradise</td>
<td>Specifies to detect Radio Paradise protocol.</td>
</tr>
<tr>
<td>rdp</td>
<td>Specifies to detect Remote Desktop protocol.</td>
</tr>
<tr>
<td>rdt</td>
<td>Specifies to detect Real Data Transport (RDT) protocol.</td>
</tr>
</tbody>
</table>
regram
Specifies to detect Regram protocol.

rfactor
Specifies to detect rFactor protocol.

rhapsody
Specifies to detect Rhapsody protocol.

rmstream
Specifies to detect RealMedia streaming protocol.

rodi
Specifies to detect Rodi protocol.

rynga
Specifies to detect Rynga protocol.

samsung-store
Specifies to detect Samsung App Store protocol.

scydo
Specifies to detect Scydo VoIP protocol.

secondlife
Specifies to detect Second Life protocol.

shoutcast
Specifies to detect SHOUTcast protocol.

silverlight
Specifies to detect Silverlight protocol.

siri
Specifies to detect Apple Siri protocol.

skinny
Specifies to detect Skinny Call Control Protocol (SCCP).

skydrive
Specifies to detect Skydrive protocol.

skype
Specifies to detect Skype protocol.
slacker-radio
Specifies to detect Slacker Radio protocol.

slingbox
Specifies to detect Slingbox protocol.

smartvoip
Specifies to detect SmartVoip protocol.

snapchat
Specifies to detect SnapChat protocol.

softether
Specifies to detect Softether protocol.

sopcast
Specifies to detect Sopcast streaming protocol.

soribada
Specifies to detect Soribada protocol.

soulseek
Specifies to detect Soulseek chat and file transfer protocol.

spdy
Specifies to detect SPDY protocol.

speedtest
Specifies to detect Speedtest protocol.

splashfighter
Specifies to detect SplashFighter protocol.

spotify
Specifies to detect Spotify music streaming protocol.

ssdp
Specifies to detect Simple Service Discovery Protocol.

stealthnet
Specifies to detect StealthNet RShare network protocol.

steam
Specifies to detect Steam file transfer protocol.
stun
Specifies to detect Session Traversal Utilities for NAT protocol.

sudaphone
Specifies to detect Sudaphone protocol.

svtplay
Specifies to detect SVTPlay protocol.

tagged
Specifies to detect Tagged protocol.

talkatone
Specifies to detect Talkatone protocol.

tango
Specifies to detect TAco Next Generation Objects hardware control system protocol.

teamspeak
Specifies to detect TeamSpeak VoIP gaming client protocol.

teamviewer
Specifies to detect TeamViewer remote control protocol.

telegram
Specifies to detect Telegram protocol.

thunder
Specifies to detect Thunder (Xunlei) download manager protocol.

truecaller
Specifies to detect Truecaller protocol.

tor
Specifies to detect Tor hidden service (anonymizer) protocol.

truphone
Specifies to detect Truphone WiFi VoIP protocol.

tumblr
Specifies to detect Tumblr protocol.

tunnelvoice
Specifies to detect Tunnel VoIP protocol.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tvants</td>
<td>Specifies to detect TVAnts protocol.</td>
</tr>
<tr>
<td>tvuplayer</td>
<td>Specifies to detect TVUPlayer protocol.</td>
</tr>
<tr>
<td>twitch</td>
<td>Specifies to detect Twitch protocol.</td>
</tr>
<tr>
<td>twitter</td>
<td>Specifies to detect Twitter protocol.</td>
</tr>
<tr>
<td>ultrabac</td>
<td>Specifies to detect UltraBac protocol.</td>
</tr>
<tr>
<td>ultrasurf</td>
<td>Specifies to detect UltraSurf protocol.</td>
</tr>
<tr>
<td>upc-phone</td>
<td>Specifies to detect UPC Phone protocol.</td>
</tr>
<tr>
<td>usenet</td>
<td>Specifies to detect Usenet Network News Transfer Protocol (NNTP) protocol.</td>
</tr>
<tr>
<td>ustream</td>
<td>Specifies to detect Ustream protocol.</td>
</tr>
<tr>
<td>uusee</td>
<td>Specifies to detect UUSee on-demand streaming protocol.</td>
</tr>
<tr>
<td>vchat</td>
<td>Specifies to detect VChat protocol.</td>
</tr>
<tr>
<td>veohdv</td>
<td>Specifies to detect VeohTV television via Internet protocol.</td>
</tr>
<tr>
<td>viber</td>
<td>Specifies to detect Viber VoIP protocol.</td>
</tr>
<tr>
<td>vine</td>
<td>Specifies to detect Vine protocol.</td>
</tr>
<tr>
<td>voipdiscount</td>
<td>Specifies to detect VoipDiscount protocol.</td>
</tr>
</tbody>
</table>
vopium
Specifies to detect Vopium protocol.

voxer
Specifies to detect Voxer Walkie Talkie protocol.

vpnx
Specifies to detect VPN-X cross-platform protocol.

vtok
Specifies to detect Vtok protocol.

vtun
Specifies to detect VTun (Virtual Tunnel) protocol.

warcft3
Specifies to detect Warcraft 3 game protocol.

waze
Specifies to detect Waze protocol.

webex
Specifies to detect Webex protocol.

wechat
Specifies to detect Wechat protocol.

weibo
Specifies to detect Weibo protocol.

whatsapp
Specifies to detect WhatsApp messaging protocol.

wii
Specifies to detect Wii Remote Bluetooth protocol.

windows-azure
Specifies to detect Windows Azure Cloud Services protocol.

windows-store
Specifies to detect Windows Phone App Store protocol.

winmx
Specifies to detect WinMX Peer Network Protocol (WPNP).
winny
Specifies to detect Winny anonymizing protocol.

wmstream
Specifies to detect Windows Media HTTP Streaming Protocol.

wofkungfu
Specifies to detect wofkungfu protocol.

wofwarcraft
Specifies to detect World of Warcraft gaming protocol.

wuala
Specifies to detect Wuala protocol.

xbox
Specifies to detect Xbox protocol.

xdcc
Specifies to detect eXtended Direct Client-to-Client protocol.

xing
Specifies to detect Xing protocol.

yahoo
Specifies to detect Yahoo! Messenger protocol.

yahoomail
Specifies to detect Yahoo Mail protocol.

youku
Specifies to detect Youku protocol.

yourfreetunnel
Specifies to detect your free Tunnel chat protocol.

youtube
Specifies to detect Youtube protocol.

zattoo
Specifies to detect Zattoo IPTV protocol.

+  
More than one of the above keywords can be entered within a single command.
Usage

Use this command to configure the detection of all or specific P2P protocol(s). Multiple keywords can be specified in a single command.

Example

The following command enables detection of all P2P protocols:

```
p2p-detection protocol all
```
packet-filter

This command allows you to create/configure/delete ACS packet filters.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration

`active-charging service service_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

Syntax

```
packet-filter packet_filter_name [ -noconfirm ]
```

```
no packet-filter packet_filter_name
```

no
If previously configured, deletes the specified packet filter from the active charging service.

```
packet_filter_name
```

Specifies the packet filter to add/configure/delete.

`packet_filter_name` must be the name of a packet filter, and must be an alphanumeric string of 1 through 63 characters. Each packet filter must have a unique name.

If the named packet filter does not exist, it is created, and the CLI mode changes to the ACS Packet Filter Configuration Mode wherein the packet filter can be configured.

If the named packet filter already exists, the CLI mode changes to the ACS Packet Filter Configuration Mode for that packet filter.

```
-noconfirm
```

Specifies that the command must execute without prompting for confirmation.

Usage

Use this command to create/configure/delete an ACS packet filter.

On entering this command, the CLI prompt changes to:

```
[context_name]host_name(config-packet-filter)#
```

Also see the ACS Packet Filter Configuration Mode Commands chapter.

Example

The following command creates a packet filter named `filter3`, and enters the ACS Packet Filter Configuration Mode:

```
packet-filter filter3
```
passive-mode

This command allows you to configure the Active Charging Service to operate in passive mode, wherein ACS passively monitors copies of packets.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration

active-charging service service_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs)#

Syntax

[ default | no ] passive-mode

no
If previously enabled, disables the passive mode configuration.

default
Configures this command with its default setting.
Default: Disabled

Usage
Use this command to put the active charging service in/out of passive mode operation, wherein ACS passively monitors copies of packets.

Example

The following command puts the active charging service into passive mode operation:

    passive-mode
pcp-service

Creates or deletes a Port Control Protocol (PCP) service.

**Important:** This command is customer specific. Contact your Cisco account representative for more information.

**Product**
- ACS
- NAT
- PSF

**Privilege**
- Security Administrator, Administrator

**Mode**
- `Exec > ACS Configuration`

```
active-charging service service_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ac)#
```

**Syntax**

```
[ no ] pcp-service pcp_service_name [ -noconfirm ]
```

- `no`
  If previously configured, deletes the specified PCP service.

- `pcp_service_name`
  Specifies the name of a PCP service.
  `pcp_service_name` must be the name of a PCP service, and must be an alphanumeric string of 1 through 63 characters. A maximum of 5 PCP services can be configured in the active charging service.
  If the named PCP service does not exist, it is created, and the CLI mode changes to the PCP Configuration Mode wherein the service can be configured. If the named PCP service already exists, the CLI mode changes to the PCP Configuration Mode.

- `-noconfirm`
  Specifies that the command must execute without any additional prompt and confirmation from the user.

**Usage**

Use this command to create or delete a PCP service.
On entering this command, the CLI prompt changes to:
```
[context_name]host_name(config-pcp-service)#
```
Also see the *PCP Configuration Mode Commands* chapter.

**Example**

The following command creates a PCP service named `pcp1`, and changes to the PCP Configuration mode:
pcp-service pcp1
policy-control bearer-bw-limit

This command allows you to enable/disable per-bearer MBR policing—bandwidth limiting.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration

`active-charging service service_name`

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs) #
```

**Syntax**

```
{ default | no } policy-control bearer-bw-limit
```

- **default**
  Configures this command with its default setting.
  Default: Enable; by default, per-bearer MBR policing is enabled.

- **no**
  Disables per-bearer MBR policing.

**Usage**

This command allows you to enable/disable per-bearer bandwidth limiting based on bitrates received over Gx. Note that there are only two variants of this command, the default and no variants.
policy-control bind-default-bearer

For PCEF Bearer Binding in 3G and when BCM mode is UE only, this command allows you to enable/disable binding rules having QoS of default bearer to the default bearer and to not ignore/ignore other rules.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration

Syntax
[ default | no ] policy-control bind-default-bearer

**default**

Configures this command with its default setting.
Default: Disables only binding those rules having QoS of default bearer to the default bearer and specifies to not ignore other rules. Rules having respective QoS will get attached to the relevant bearers. Also TFT updates towards the UE (access side) will not be suppressed.

**no**

The no keyword functionality is same as the default setting.

Usage

This CLI command is used to bind all the PCC dynamic or predef rules received from PCRF (Bearer Control Mode (BCM) is UE_only) without QoS and ARP or with the same QoS and ARP as that of the default bearer, to the default bearer. This CLI is used for UE Only mode.
In case no QoS is specified the rule gets attached to the default bearer. Also no TFT updates will be sent towards UE (access side). So only one default bearer will ever be created.
On receiving a PCC dynamic rule or predef rule from PCRF, having QoS/ARP other than the default bearer, then those rules are ignored and a response indicating that the rule could not be installed, is sent.
This CLI command will not work currently for dedicated bearers (secondary PDP contexts). Secondary bearers initiated by UE are not supported.
Releases prior to 12.2, when UE Only BCM is received from PCRF, IMSA terminates the call for P-GW (GnGp setup). Release 12.2 onwards, the P-GW call is not terminated so as to be in compliance with 3GPP standard specification TS 29.212, but Traffic Flow Template (TFT) updates towards UE (access side) will be supported.
**Important:** This CLI is applicable to all the rulebases in the chassis configuration. If the rulebase is changed to some other rulebase in the interim period or anytime later, this CLI will continue to apply to the current new rulebase too.
policy-control burst-size

This command allows you to configure the burst size for bandwidth limiting per dynamic-rule or per bearer.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration

active-charging service service_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs)#

Syntax

policy-control burst-size { auto-readjust [ duration duration ] | bytes bytes }

{ default | no } policy-control burst-size

<table>
<thead>
<tr>
<th>default</th>
<th>no</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configures this command with its default setting.</td>
<td></td>
</tr>
<tr>
<td>Default: 65535 bytes</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>duration duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configures the burst size equal to &lt;seconds&gt; of traffic.</td>
</tr>
<tr>
<td>duration must be an integer from 1 through 20.</td>
</tr>
<tr>
<td>Default: In 12.1 and earlier releases, 10 seconds. In 12.2 and later releases, 5 seconds.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>bytes bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the burst size, in bytes.</td>
</tr>
<tr>
<td>bytes must be an integer from 1 through 4000000000.</td>
</tr>
</tbody>
</table>

Usage
Use this command to configure the burst size for bandwidth limiting per dynamic-rule or per bearer.

Example
The following command configures the burst size for bandwidth limiting per dynamic-rule or per bearer equal to 10 seconds of traffic:

    policy-control burst-size auto-readjust
policy-control charging-action-override

This command has been removed from the ACS Configuration Mode, and replaced by the charging-action-override command in the ACS Rulebase Configuration Mode.
policy-control charging-rule-base-name

This command allows you to configure how the Charging-Rule-Base-Name AVP from PCRF is interpreted, either as ACS rulebase or ACS group-of-ruledefs.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration

```
active-charging service service_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

**Syntax**

```
policy-control charging-rule-base-name { active-charging-group-of-ruledefs | active-charging-rulebase [ ignore-when-removed ] [ use-first ]}

default policy-control charging-rule-base-name

no policy-control charging-rule-base-name active-charging-rulebase use-first
```

---

**default**

Configures this command with its default setting(s).

Default:

- charging-rule-base-name: active-charging-group-of-ruledefs
- use-first: Disabled

---

**no**

If multiple Charging-Rule-Base-Name are received from the PCRF, specifies to select the last rulebase. This is the default behavior.

---

**active-charging-group-of-ruledefs**

Specifies interpreting Charging-Rule-Base-Name as ACS group-of-ruledefs.

---

**active-charging-rulebase [ ignore-when-removed ] [ use-first ]**

Specifies interpreting Charging-Rule-Base-Name as ACS rulebase.

When Charging-Rule-Base-Name AVP is interpreted as ACS rulebase, if PCRF requests the removal of a Charging-Rule-Base-Name, which is the same as the rulebase used for that PDP context, the PDP context is terminated. This is because after removal of the rulebase, the PDP context will have no rulebase. This is the default behavior.

**ignore-when-removed:** Specifies to ignore PCRF request for removal of Charging-Rule-Base-Name, and take no action. If this keyword is not configured, the PDP context from which the rulebase is removed gets terminated.
**use-first**: If multiple Charging-Rule-Base-Name are received from the PCRF, since a call can only have one ACS rulebase applied, specifies to select the first rulebase. If previously enabled, to disable this configuration, use the `no policy-control charging-rule-base-name active-charging-rulebase use-first` command. If this keyword is not configured, by default, the last rulebase is selected. For each call, this interpretation is decided at call setup, and will not be changed during the life of that call. Change will only apply to new calls coming up after the change.

---

**Usage**

Use this command to configure interpretation of Charging-Rule-Base-Name AVP from PCRF either as ACS group-of-ruledefs or as ACS rulebase.

**Example**

The following command configures interpreting of Charging-Rule-Base-Name AVP as ACS rulebase:

```
policy-control charging-rule-base-name active-charging-rulebase
```
policy-control dynamic-rule-limit

This command allows you to enable/disable per-dynamic-rule MBR policing—bandwidth limiting.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration

active-charging service service_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs)#

Syntax

{ default | no } policy-control dynamic-rule-limit

default

Configures this command with its default setting.
Default: Enable; by default, per-dynamic-rule MBR policing is enabled.

no

Disables per-dynamic-rule MBR policing.

Usage

This command allows you to enable/disable per-dynamic-rule bandwidth limiting based on bitrates received over Gx. Note that there are only two variants of this command, the default and no variants.
policy-control update-default-bearer

For PCEF Bearer Binding in 4G, this command allows you to enable/disable binding rules having QoS of default bearer to the default bearer and to not ignore/ignore other rules.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration

active-charging service service_name

Entering the above command sequence results in the following prompt:

[llocal] host_name(config-acs)#

Syntax

[ default | no ] policy-control update-default-bearer

default

Configures this command with its default setting.

Disables only binding those rules having QoS of default bearer to the default bearer and specifies to not ignore other rules. Rules having respective QoS will get attached to the relevant bearers. Also TFT updates towards UE (access side) will not be suppressed.

no

Enables binding rules having QoS of default bearer to the default bearer and specifies to ignore other rules. In case no QoS is specified the rule gets attached to default bearer. Also TFT updates towards UE (access side) will be suppressed for default bearer. So only one default-bearer will ever be created.

⚠️ Caution: Upon executing this CLI command “no policy-control update-default-bearer”, system crash is likely to occur if the TFT information is not added to the charging-action.

Usage

This CLI command is used to bind all the PCC dynamic or predef rules received from PCRF without QoS and ARP or with the same QoS and ARP as that of the default bearer, to the default bearer.

On receiving a PCC dynamic rule or predef rule from PCRF, having QoS/ARP other than the default bearer, then those rules are ignored and a response indicating that the rule could not be installed, is sent.

This CLI command will not work currently for dedicated bearers (secondary PDP contexts). Secondary bearers initiated by UE are not supported.

Releases prior to 12.2 TFT updates were sent towards the UE (access side) on all bearers. Release 12.2 onwards, TFT updates will be suppressed towards the UE (access side) for default bearer, if the CLI is enabled.
Important: This CLI is applicable to all the rulebases in the chassis configuration. If the rulebase is changed to some other rulebase in the interim period or anytime later, this CLI will continue to apply to the current new rulebase too.
port-map

This command allows you to create/configure/delete port maps.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration

active-charging service service_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs)#

Syntax

port-map port_map_name [ -noconfirm ]

no port-map port_map_name

  no
  If previously configured, deletes the specified port map from the active charging service.

  port_map_name
  Specifies the port map to add/configure/delete.
  port_map_name must be the name of a port map, and must be an alphanumeric string of 1 through 63 characters, and can contain punctuation characters. Each port map must have a unique name.
  If the named port map does not exist, it is created, and the CLI mode changes to the ACS Port Map Configuration Mode wherein the port map can be configured.
  If the named port map already exists, the CLI mode changes to the ACS Port Map Configuration Mode for that port map.

  -noconfirm
  Specifies that the command must execute without prompting for confirmation.

Usage

Use this command to create/configure/delete an ACS port map.
The port map name must be unique with in the service. Host pool, port map, IMSI pool, and firewall, routing, and charging ruledefs must have unique names. A maximum of the 256 port maps can be created.

Important: Port maps in use in other ruledefs cannot be deleted.

Example

Also see the ACS Port Map Configuration Mode Commands chapter.
The following command creates a port map named `portmap1`, and enters the ACS Port Map Configuration Mode:

```
port-map portmap1
```
qos-group-of-ruledefs

This command allows you to create/configure/delete a qos-group-of-ruledefs.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration

**Syntax**
```
qos-group-of-ruledefs  qos_group_of_ruledefs_name  [  -noconfirm  ]  [  description  description  ]

no  qos-group-of-ruledefs  qos_group_of_ruledefs_name
```

- **qos_group_of_ruledefs_name**
  Specifies the qos-group-of-ruledefs to add/configure/delete.
  `qos_group_of_ruledefs_name` must be the name of a qos-group-of-ruledefs, and must be an alphanumeric string of 1 through 63 characters. Each qos-group-of-ruledefs must have a unique name.
  If the named qos-group-of-ruledefs does not exist, it is created, and the CLI mode changes to the ACS QoS-Group-of-Ruledefs Configuration Mode wherein the group can be configured.
  If the named qos-group-of-ruledefs already exists, the CLI mode changes to the ACS QoS-Group-of-Ruledefs Configuration Mode for that group.

- **-noconfirm**
  Specifies that the command must execute without prompting for confirmation.

- **description  description**
  Specifies an optional description of the group, such as purpose of setting up the group, to be included in the configuration.

**Usage**
Use this command to create/configure/delete a qos-group-of-ruledefs.
On entering this command, the CLI prompt changes to:
```
[context_name]hostname(config-qos-group-of-ruledefs)#
```

Also see the *ACS QoS-Group-of-Ruledefs Configuration Mode Commands* chapter.

**Example**
The following command creates a qos-group-of-ruledefs named \textit{group1}, and enters the ACS QoS-Group-of-Ruledefs Configuration Mode:

\begin{verbatim}
qos-group-of-ruledefs group1
\end{verbatim}
readdress-server-list

This command allows you to create/delete server list for DNS redirection.

Important: This command is license dependent. For more information please contact your Cisco account representative.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration

Syntax
[ no ] readdress-server-list server_list_name [ -noconfirm ]

no
If previously configured, deletes the specified readdress server list from the active charging service.

server_list_name
Specifies the server list to add/configure/delete for DNS redirection. server_list_name must be an alphanumeric string of 1 through 63 characters and can contain punctuation characters. Each server list must have a unique name. If the named server list does not exist, it is created, and the CLI mode changes to the ACS Readdress Server List Configuration Mode wherein the servers can be configured. If the named server list already exists, the CLI mode changes to the ACS Readdress Server List Configuration Mode for that server list.

-noconfirm
Specifies that the command must execute without prompting for confirmation.

Usage
Use this command to create/delete server list for DNS redirection. To add the servers to the server list, see the server command in the ACS Readdress Server List Configuration Mode chapter. On entering this command, the CLI prompt changes to:

[context_name]hostname(config-readdress-server-list)#

Also see the ACS Readdress Server List Configuration Mode chapter.

Example
The following command creates a charging action named `homeDNSserver` and changes to the ACS Readdress Server List Configuration Mode:

```
readdress-server-list homeDNSserver
```
redirect user-agent

This command allows you to specify the user agent for conditional redirection of traffic flows.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration

```
active-charging service service_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

**Syntax**

```
[ no ] redirect user-agent user_agent_name
```

- **no**
  If previously configured, deletes the specified user agent from the active charging service.

- **user_agent_name**
  Specifies the user agent to be used for redirecting traffic flow.
  The `user_agent_name` must be the name of a user agent, and must be an alphanumeric string of 1 through 32 characters.
  A maximum of 16 user-agents can be configured in the active charging service.

**Usage**

Use this command to redirect the traffic flow with conditions based on configured user-agent name. This user agent is used with `flow action` command in the ACS Charging Action Configuration Mode.

**Example**

The following command specifies the redirect user agent `user_rule1` for conditional redirection of traffic flow:

```
redirect user-agent user_rule1
```
rulebase

This command allows you to create/configure/delete ACS rulebases.

**Important:** A maximum of 512 rulebases can be configured in the active charging service.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration

```syntax
active-charging service service_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

**Syntax**

```syntax
rulebase rulebase_name [ -noconfirm ]
```

```syntax
no rulebase rulebase_name
```

- **no**
  
  If previously configured, deletes the specified rulebase from the active charging service.

```syntax
rulebase_name
```

Specifies the rulebase to add/configure/delete.

**rulebase_name** must be the name of an ACS rulebase, and must be an alphanumeric string of 1 through 63 characters, and can contain punctuation characters. Each rulebase must have a unique name.

If the named rulebase does not exist, it is created, and the CLI mode changes to the ACS Rulebase Configuration Mode wherein the rulebase can be configured.

If the named rulebase already exists, the CLI mode changes to the ACS Rulebase Configuration Mode for that rulebase.

- **-noconfirm**

  Specifies that the command must execute without prompting for confirmation.

**Usage**

Use this command to create/configure/delete an ACS rulebase. A rulebase is a collection of protocol rules to match a flow and associated actions to be taken for matching flow.

The default rulebase is used when a subscriber/APN is not configured with a specific rulebase to use.

On entering this command, the CLI prompt changes to:

```
[context_name]hostname(config-rule-base)#
```

Also see the *ACS Rulebase Configuration Mode Commands* chapter.

**Example**
The following command creates a rulebase named *test1*, and enters the ACS Rulebase Configuration Mode:

```
rulebase test1
```
rulebase-list

This command allows you to create and delete ACS rulebase lists.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration

active-charging service service_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs)#

Syntax

rulebase-list  rulebase_list_name  rulebase_name  [ rulebase_name + ]

no rulebase-list  rulebase_list_name

no

If previously configured, deletes the specified rulebase list from the active charging service.

rulebase_list_name

Specifies the rulebase list to add/modify/delete.

rulebase_list_name must be the name of an ACS rulebase list, and must be an alphanumeric string of 1 through 63 characters.

rulebase_name

Specifies the rulebase name(s) to add to the rulebase list.

Each rulebase list must contain a minimum of one rulebase name, and the cumulative length of all rulebase names must not exceed 256 bytes.

rulebase_name must be the name of an ACS rulebase, and each rulebase name must be an alphanumeric string of 1 through 63 characters.

Usage

Use this command to create or delete an ACS rulebase list. A rulebase list is a space-separated string of rulebase names supplied to the OCS, from which the OCS chooses the rulebase to use for the subscriber. The rulebase list to use for a subscriber is specified in the APN for the subscriber.

In 12.3 and earlier releases, a maximum of 20 rulebase lists can be configured.

In 14.0 and later releases, a maximum of 128 rulebase lists can be configured.

See the active-charging rulebase-list command in the APN Configuration Mode Commands chapter.

Example

The following command creates a rulebase list named rblist, and adds the rulebases named rulebase1, rulebase3, and rulebase5 to it:
rulebase-list rblist rulebase1 rulebase3 rulebase5

The following command deletes the rulebase list named rblist:

    no rulebase-list rblist
ruledef

This command allows you to create/configure/delete ACS rule definitions.

**Important:** A maximum of 2048 ruledefs can be configured in the active charging service.

**Product:** ACS

**Privilege:** Security Administrator, Administrator

**Mode:**

Exec > ACS Configuration

`active-charging service service_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-accs)#
```

**Syntax**

```
ruledef ruledef_name [ -noconfirm ]

no ruledef ruledef_name
```

- **no**
  If previously configured, deletes the specified ruledef from the active charging service.

- **ruledef_name**
  Specifies the ruledef to add/configure/delete.
  `ruledef_name` must be the name of an ACS ruledef, and must be an alphanumeric string of 1 through 63 characters, and can contain punctuation characters. Each ruledef must have a unique name. Host pool, port map, IMSI pool, and firewall, routing, and charging ruledefs must have unique names.
  If the named ruledef does not exist, it is created, and the CLI mode changes to the ACS Ruledef Configuration Mode wherein the ruledef can be configured.
  If the named ruledef already exists, the CLI mode changes to the ACS Ruledef Configuration Mode for that ruledef.

**Important:** If there are any changes to ruledef and the Override Control/Inheritance feature is enabled, then execute the CLI command “update active-charging override-control rulebase-config”. For more information on this command, see the *Command Line Interface Reference*.

- **-noconfirm**
  Specifies that the command must execute without prompting for confirmation.

**Usage**

Use this command to create/configure/delete an ACS ruledef.
A ruledef represents a set of matching conditions across multiple L3 – L7 protocol based on protocol fields and state information. Each ruledef can be used across multiple rulebases within the active charging service. On entering this command, the CLI prompt changes to:

```
[context_name]hostname(config-acb-ruledef)#
```

Also see the *ACS Ruledef Configuration Mode Commands* chapter.

**Example**

The following command creates an ACS ruledef named `test1`, and enters the ACS Ruledef Configuration Mode:

```
ruledef test1
```
sip advanced

This command enables SIP ALG to maintain the same tag parameters (from and to tag) for Authorization or Proxy Authentication requests.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration

active-charging service service_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs)#

Syntax

[ default | no ] sip advanced out-of-dialog-request retain-tag

---

**default**

Configures this command with its default setting.
Default: Disabled

---

**no**

If previously enabled, disables the SIP ALG configuration.

**Usage**

Use this command to enable SIP ALG to maintain the same tag parameters (from and to tag) while processing 4xx responses for Authorization or Proxy Authentication requests as described in section 8.1.3.5 of RFC 3261 (SIP: Session Initiation Protocol).
system-limit l4-flows

This command allows you to configure the system-wide Layer 4 flow limit.

**Important:** This command is customer specific. For more information contact your Cisco account representative.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration

`active-charging service service_name`

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs)#
```

**Syntax**

```
system-limit l4-flows limit
```

```
{ default | no } system-limit l4-flows
```

**default**

Configures this command with its default setting.

Default: Disabled; same as `no system-limit l4-flows`

**no**

Disables the limit checking configuration.

**limit**

Specifies the Layer 4 flows limit.

`limit` must be an integer from 1 through 2147483647.

**Usage**

Use this command to configure the system-wide limit for Layer 4 flows.

The System-wide L4 Flow Limiting feature provides the capability to limit the number of TCP and UDP flow over the system. This limiting can be applied to all subscribers attaching to the system and to all APNs. This feature is compatible with the existing per-subscriber limiting (configured using the flow limit-for-flow-type charging action). Both limiting can be active in the same time.

System-wide flow limiting is implemented by comparing the “Effective Flows” periodically (~ every 10 seconds) against the configurable “System-wide Flow Limit”. Where “Effective Flows” is the number of active data sessions, each identified by the 5-tuple key. If the “Effective Flows” exceeds the “System-wide Flow Limit”, the Resource Manager indicates it to the active charging service. When ACS is aware of the “System-wide Flow Limit” being reached, no more data sessions are setup. The packets are discarded. While
processing a successive flow-usage update from active charging service a change in behavior is indicated to active charging service to start accepting data sessions. As this relies on periodic reporting there is an inherent delay in the detection of “exceeding/returning once exceeded” to the flow limit.

Example

The following command sets the system limit for L4 flows to 100:

```system-limit l4-flows 100```
**tethering-database**

This command allows you to enable/disable the Tethering Detection feature, and load the databases from the specified files into the service.

**Important:** This command is available only if the Smartphone Tethering Detection license is enabled. For more information please contact your Cisco account representative.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration

```
active-charging service service_name
```

Entering the above command sequence results in the following prompt:
```
[local]host_name(config-acs)#
```

**Syntax**

```
tethering-database [ os-signature os_signature_db_file_name | tac tac_db_file_name | ua-signature ua_signature_db_file_name ] +

{ default | no } tethering-database
```

- **default**
  Configures this command with its default setting.
  Default: Tethering Detection feature is disabled, and the database file names are reset to their default values.

- **no**
  Disables Tethering Detection.

```
tethering-database os-signature os_signature_db_file_name
```

Specifies the OS Signature database file to load.

`os_signature_db_file_name` must be the name of the OS Signature database file, and must be an alphanumeric string of 1 through 255 characters.

```
tethering-database tac tac_db_file_name
```

Specifies the TAC database file to load.

`tac_db_file_name` must be the name of a TAC database file, and must be an alphanumeric string of 1 through 255 characters.

```
tethering-database ua-signature ua_signature_db_file_name
```

Specifies the User Agent (UA) Signature database file to load.
tethering-database

\texttt{ua\_signature\_db\_file\_name} must be the name of a UA Signature database file, and must be an alphanumeric string of 1 through 255 characters.

+ Indicates that more than one of the preceding option can be entered in a single command.

**Usage**

Use this command to enable the Tethering Detection feature, and load the OS, TAC, and UA databases from the specified files into the service. Tethering refers to the use of a smartphone as a USB dongle/modem to provide Internet connectivity to laptops/PDAs/tablets like iPad, using the smartphone's data plan. Typically many operators have in place an eat-all-you-can-get data plan for smartphones, the usage of which is intended to be from the smartphone as a mobile device. However, some users use the low rate/unlimited usage of data plan to provide Internet connectivity to their laptops in places where normal Internet connection via broadband/WiFi might be more costly/not available/insecure. Operators are interested in detecting such usage of a smartphone as a modem to better understand the usage across their networks and offer plans inline to that usage to their customers. They may also charge the tethered and non-tethered traffic separately. After Tethering Detection has been enabled here (regardless, it must also be enabled within the rulebase), this CLI command may be used to change the databases with the specified databases. The files are picked from the disk file system within the /databases directory. If a file name value is not configured, the default file names, os-db, tac-db, and ua-db, are used. For more information on the Tethering Detection feature, refer to the Enhanced Charging Services Administration Guide.

**Example**

The following command enables Tethering Detection and selects the UA Signature database file named test:

```
tethering-database ua-signature test
```
timedef

This command allows you to create/configure/delete ACS Time Definitions (timedefs).

**Important**: This command is available only in StarOS 8.1 and in StarOS 9.0 and later releases.

**Important**: A maximum of 10 timedefs can be configured in the active charging service.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration

active-charging service service_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs)#

**Syntax**

```
timedef timedef_name [ -noconfirm ]

no timedef timedef_name
```

**no**

If previously configured, deletes the specified timedef from the active charging service.

**timedef_name**

Specifies the timedef to add/configure/delete.

- **timedef_name** must be the name of a timedef, and must be an alphanumeric string of 1 through 63 characters. Each timedef must have a unique name.
- If the named timedef does not exist, it is created, and the CLI mode changes to the ACS Timedef Configuration Mode wherein timeslots for the timedef can be configured.
- If the named timedef already exists, the CLI mode changes to the ACS Timedef Configuration Mode for that timedef.

**-noconfirm**

Specifies that the command must execute without prompting for confirmation.

**Usage**

Use this command to create/configure/delete ACS timedefs for the Time-of-Day Activation/Deactivation of Rules feature. Timedefs enable activation/deactivation of ruledefs/groups-of-ruledefs such that they are available for rule matching only when they are active.

On entering this command, the CLI prompt changes to:
Example

The following command creates a timedef named `test1`, and enters the ACS Timedef Configuration Mode:

```
timedef test1
```
tpo policy

The Traffic Performance Optimization (TPO) in-line service is not supported in this release.
tpo profile

The Traffic Performance Optimization (TPO) in-line service is not supported in this release.
.udr-format

This command allows you to create/configure/delete a User Data Record (UDR) format.

**Important:** A maximum of 256 UDR plus EDR formats can be configured in the active charging service.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration

`active-charging service service_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

**Syntax**

```
udr-format udr_format_name [ -noconfirm ]

no udr-format udr_format_name
```

If previously configured, deletes the specified UDR format from the active charging service.

```
udr_format_name
```

Specifies the UDR format to add/configure/delete.

- `udr_format_name` must be the name of a UDR format, and must be an alphanumeric string of 1 through 63 characters. Each UDR format must have a unique name.
- If the named UDR format does not exist, it is created, and the CLI mode changes to the UDR Format Configuration Mode wherein the UDR format can be configured.
- If the named UDR format already exists, the CLI mode changes to the UDR Format Configuration Mode for that UDR format.

- `-noconfirm`

Specifies that the command must execute without prompting for confirmation.

**Usage**

Use this command to create/configure/delete a UDR format in the active charging service.

On entering this command, the CLI prompt changes to:

```
[context_name]host_name(config-acs-udr)#
```

Also see the *UDR Format Configuration Mode Commands* chapter.

**Example**

---

Cisco ASR 5x00 Command Line Interface Reference

554
The following command creates an UDR format named `udr_format1` and changes to the UDR Format Configuration Mode:

```
udr-format udr_format1
```
url-blacklisting match-method

This command allows you to specify the match method to look up URLs in the URL Blacklisting database.

**Product**
CF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration

```markdown
active-charging service service_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

**Syntax**

```
url-blacklisting match-method { exact | generic }
```

**default url-blacklisting match-method**

```
default
```

Configures this command with its default setting.

Default: **exact**

---

**Important**: In 14.0 and later releases, it is recommended to use the generic match method for URL Blacklisting.

```
exact
```

Specifies the exact-match method, wherein URL Blacklisting is performed only on exact match with a URL present in the URL Blacklisting database.

```
generic
```

Specifies the generic-match method, wherein URL Blacklisting is performed on a generic match with URLs present in the URL Blacklisting database.

**Usage**

Use this command to set the match method to look up URLs in the URL Blacklisting database.

**Example**

The following command sets the exact-match method to look up URLs in the URL Blacklisting database:

```
url-blacklisting match-method exact
```
**xheader-format**

This command allows you to create/configure/delete ACS extension-header (x-header) format specifications.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration

```
active-charging service service_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs)#
```

**Syntax**

```
xheader-format xheader_format_name [ -noconfirm ]
```

```
no xheader-format xheader_format_name
```

- **xheader_format_name**
  Specifies the x-header format to add/configure/delete.
  `xheader_format_name` must be the name of an xheader format, and must be an alphanumeric string of 1 through 63 characters. Each x-header format must have a unique name.
  If the named x-header format does not exist, it is created, and the CLI mode changes to the ACS X-header Format Configuration Mode wherein the x-header format can be configured.
  If the named x-header format already exists, the CLI mode changes to the ACS X-header Format Configuration Mode for that x-header format.

- **-noconfirm**
  Specifies that the command must execute without prompting for confirmation.

**Usage**

Use this command to create/configure/delete an x-header format specification in the active charging service. On entering this command, the CLI prompt changes to:

```
[context_name]host_name(config-acs-xheader)#
```

An x-header may be specified in a charging action to be inserted into HTTP GET and POST request packets. See `xheader-insert` CLI command in the *ACS Charging Action Configuration Mode Commands* chapter. Also see the *ACS X-header Format Configuration Mode Commands* chapter.

**Example**

The following command creates an x-header format named *test*, and enters the ACS X-header Format Configuration Mode:
xheader-format test
Chapter 9
ACS Group-of-Objects Configuration Mode Commands

The ACS Group-of-Objects Configuration Mode is used to configure groups of Active Charging Service (ACS) objects.

**Important:** This configuration mode is available only in 10.2 and later releases.

**Mode**

Exec > ACS Configuration > ACS Group-of-Objects Configuration

```
active-charging service service_name > group-of-objects object_name [ type string ]
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-group-of-objects)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
**exit**

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**
Use this command to return to the parent configuration mode.
member-object

This command allows you to add or remove objects from the current group-of-objects.

---

**Important:** A maximum of 128 objects can be added to a group-of-objects.

---

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > ACS Group-of-Objects Configuration

**Syntax**

```
[ no ] member-object object
```

- **no**
  - If previously added, removes the specified member object from the current group-of-objects.

- **object**
  - Specifies the member object to add to or remove from the current group-of-objects.
  - `object` must be an alpha and/or numeric string of 1 through 63 characters.

**Usage**
Use this command to add or remove member objects from a group-of-objects.

**Example**

The following command adds the object `test` to the current group-of-objects:

```
member-object test
```
Chapter 10
ACS Group-of-Prefixed-URLs Configuration Mode Commands

The ACS Group-of-Prefixed-URLs Configuration Mode is used to create and configure groups of prefixed URLs.

**Important:** This configuration mode is customer specific. For more information, contact your Cisco account representative.

Mode

Exec > ACS Configuration > ACS Group-of-Prefixed-URLs Configuration

`active-charging service service_name > group-of-prefixed-urls group_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-grp-of-prefixed-urls)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Use this command to return to the parent configuration mode.
prefixed-url

This command allows you to add or remove URLs from the current group of prefixed URLs.

**Important:** A maximum of 10 URLs can be added per group.

**Product:** ACS

**Privilege:** Security Administrator, Administrator

**Mode:**
Exec > ACS Configuration > ACS Group-of-Prefixed-URLs Configuration

```active-charging service service_name > group-of-prefixed-urls group_name```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acg-acs-grp-of-prefixed-urls)#
```

**Syntax**

```
[ no ] prefixed-url url
```

- **no**
  If added previously, removes the specified URL from the current group of prefixed URLs.

- **url**
  Specifies the URL to add/remove.
  *url* must be an alphanumeric string of 1 through 63 characters.

**Usage**

Use this command to add or remove URLs to be filtered from the group of prefixed URLs.

**Example**

The following command adds the URL `http://abc.net` to the current group of prefixed URLs:

```
prefixed-url http://abc.net
```
Chapter 11
ACS Group-of-Ruledefs Configuration Mode Commands

The ACS Group-of-Ruledefs Configuration Mode is used to configure groups of rule definitions (ruledefs).

**Important:** In 14.1 and earlier releases, a maximum of 64 group-of-ruledefs can be configured. In 15.0 and later releases, a maximum of 128 group-of-ruledefs can be configured.

**Mode**

Exec > ACS Configuration > ACS Group-of-Ruledefs Configuration

```
active-charging service service_name > group-of-ruledefs group_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acsc-group-of-ruledefs)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
add-ruledef

This command allows you to add or remove ruledefs from a group-of-ruledefs.

**Important:** A maximum of 128 ruledefs can be added to a group-of-ruledefs.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > ACS Group-of-Ruledefs Configuration

```
add-ruledef priority ruledef_priority ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs-group-of-ruledefs)#
```

**Syntax**

```
add-ruledef priority ruledef_priority ruledef ruledef_name
```

```
no add-ruledef priority ruledef_priority
```

- **no**
  If previously configured, specifies that the ruledef associated with the specified priority number be removed from the current group-of-ruledefs.

```
priority ruledef_priority
```

- **priority ruledef_priority**
  Specifies priority of the ruledef in the current group-of-ruledefs.
  `ruledef_priority` must be unique in the group-of-ruledefs, and must be an integer from 1 through 10000.

```
ruledef ruledef_name
```

- **ruledef ruledef_name**
  Specifies name of the ruledef to add to the current group-of-ruledefs.
  `ruledef_name` must be the name of an ACS ruledef, and must be an alpha and/or numeric string of 1 through 63 characters.

**Usage**

Use this command to add/remove ruledefs from a group-of-ruledefs.

A group-of-ruledefs can contain optimizable ruledefs. Whether a group is optimized or not is decided on whether all the ruledefs in the group-of-ruledefs can be optimized, and if the group is included in a rulebase that has optimization turned on, then the group will be optimized.

When a new ruledef is added, it is checked if it is included in any group-of-ruledefs, and whether it needs to be optimized, etc.

**Example**

The following command adds the ruledef `ruledef23` to the current group-of-ruledefs, and assigns it a priority of 3:

```
add-ruledef priority 3 ruledef23
```
add-ruledef priority 3 ruledef ruledef23
**dynamic-command**

This command allows you to add or remove dynamic commands from a group-of-ruledefs.

**Product**

ACS
CF

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > ACS Configuration > ACS Group-of-Ruledefs Configuration

```
active-charging service service_name > group-of-ruledefs group_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-group-of-ruledefs)#
```

**Syntax**

```
dynamic-command content-filtering category policy-id policy_id
```

```
no dynamic-command content-filtering category policy-id
```

```
no
```

Specifies to remove dynamic command configuration from the current group-of-ruledefs.

```
content-filtering category policy-id policy_id
```

Specifies the dynamic command for Content Filtering Category Policy ID configuration.

`policy_id` must be a Content Filtering Category Policy ID, and must be an integer from 1 through 4294967295.

**Usage**

Use this command to add a dynamic command to a group-of-ruledefs, which will be executed when a dynamic protocol specifies that group-of-ruledefs (via the Rulebase-Name AVP).

**Important:** This release supports only one command option, which is `dynamic-command content-filtering category policy-id policy_id`

**Example**

The following command configures a dynamic command for Content Filtering Category Policy ID configuration using the policy ID 100:

```
dynamic-command content-filtering category policy-id 100
```
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
**exit**

Exits the current mode and returns to the parent configuration mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

exit

**Usage**

Use this command to return to the parent configuration mode.
group-of-ruledefs-application

This command allows you to specify the purpose of setting up a group-of-ruledefs as either charging, post-processing, or for other purposes.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > ACS Group-of-Ruledefs Configuration
active-charging service service_name > group-of-ruledefs group_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acsp-group-of-ruledefs)#

Syntax

  group-of-ruledefs-application { charging | content-filtering | gx-alias | post-processing | tpo }

no group-of-ruledefs-application

no
If previously configured, deletes the group-of-ruledefs-application configuration from the current group-of-ruledefs.

charging
Specifies that the current group-of-ruledefs is for charging purposes.

content-filtering
Specifies that the current group-of-ruledefs is for content-filtering purposes.

gx-alias
Specifies that the current group-of-ruledefs is for Gx-alias purposes.

post-processing
Specifies that the current group-of-ruledefs is for post-processing purposes, that is, for use by the post-processing CLI command or automatic name-matching to the Diameter Filter-Id AVPs.

tpo

Important: The Traffic Performance Optimization (TPO) in-line service is not supported in this release.
Usage

Use this command to specify the purpose of setting up a group-of-ruledefs. If not specified, by default the rule-application type will be charging.

If the group-of-ruledefs-application is configured for content-filtering, no ruledef can be added to it. Similarly, if configured explicitly for charging or post-processing, a content-filtering policy cannot be configured in it.

The group-of-ruledefs may be dynamically selected by Diameter, as described by the `policy-control charging-rulebase-name` command in the Active Charging Service Configuration Mode. If so selected, the priority field of the add-ruledef instances within the group-of-ruledefs are ignored, and all of the rules named by the ruledef keyword that are also configured with the same name in the action command are selected.

Example

The following command configures the current group-of-ruledefs as for post-processing purposes:

```
   group-of-ruledefs-application post-processing
```
Chapter 12
ACS Host Pool Configuration Mode Commands

The ACS Host Pool Configuration Mode is used to define a pool of host addresses within the ACS Configuration Mode. The host pool facilitates to create rules to handle the packets coming from or going to a group of hosts within an access policy.

Mode

Exec > ACS Configuration > ACS Host Pool Configuration

active-charging service service_name > host-pool host_pool_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-host-pool)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
end

Exits the current configuration mode and returns to the Exec mode.

Product: All
Privilege: Security Administrator, Administrator
Syntax:

end

Usage:
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Use this command to return to the parent configuration mode.
ip

This command allows you to add/remove an individual or a range of host IPv4/IPv6 address(es) from the current host pool.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > ACS Host Pool Configuration

```
active-charging service service_name > host-pool host_pool_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-host-pool)#
```

**Syntax**

```
[ no ] ip { ipv4/ipv6_address | ipv4/ipv6_address/maskbit | range start_ipv4/ipv6_address to end_ipv4/ipv6_address }
```

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>If added previously, removes the specified IPv4/IPv6 address(es) from the current host pool.</td>
</tr>
<tr>
<td>ipv4/ipv6_address</td>
<td>Specifies an IPv4/IPv6 address to add to the current host pool.</td>
</tr>
<tr>
<td>ipv4/ipv6_address</td>
<td>must be an IPv4/IPv6 address.</td>
</tr>
<tr>
<td>ipv4/ipv6_address/maskbit</td>
<td>Specifies an IPv4/IPv6 address/mask bits combination to add to the current host pool.</td>
</tr>
<tr>
<td>ipv4/ipv6_address</td>
<td>must be an IPv4/IPv6 address.</td>
</tr>
<tr>
<td>maskbit</td>
<td>must be the number of bits in the subnet mask, and must be a numeric value.</td>
</tr>
<tr>
<td>range start_ipv4/ipv6_address to end_ipv4/ipv6_address</td>
<td>Specifies a range of IPv4/IPv6 addresses to add to the current host pool.</td>
</tr>
<tr>
<td>start_ipv4/ipv6_address</td>
<td>specifies the starting IPv4/IPv6 address of the range, and must be less than</td>
</tr>
<tr>
<td>end_ipv4/ipv6_address</td>
<td>end_ipv4/ipv6_address.</td>
</tr>
<tr>
<td>end_ipv4/ipv6_address</td>
<td>specifies the ending IPv4/IPv6 address of the range, and must be greater than</td>
</tr>
<tr>
<td>start_ipv4/ipv6_address</td>
<td>start_ipv4/ipv6_address.</td>
</tr>
</tbody>
</table>

**Usage**
Use this command to add an individual or a range of IPv4/IPv6 addresses to a host pool. Up to 10 sets of IPv4/IPv6 addresses can be configured in each host pool.

**Example**
The following command adds all IPv4 addresses from 10.2.3.4 through 10.4.5.6 to the current host pool:
ip range 10.2.3.4 to 10.4.5.6
Chapter 13
ACS IMSI Pool Configuration Mode Commands

The ACS IMSI Pool Configuration Mode is used to define a pool of subscriber International Mobile Station Identifier (IMSI) numbers within the ACS Configuration Mode. IMSI pool configuration facilitates creation of rules to handle the packets coming from or going to a group of subscriber of IMSI numbers within an access policy.

Mode
Exec > ACS Configuration > ACS IMSI Pool Configuration

```
active-charging service service_name > imsi-pool imsi_pool_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-imsi-pool)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**
Use this command to return to the parent configuration mode.
imsi

This command allows you to add/remove an individual or a range of subscriber IMSI numbers from the current IMSI pool.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > ACS IMSI Pool Configuration

active-charging service service_name > imsi-pool imsi_pool_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-imsi-pool)#

Syntax

[ no ] imsi { imsi_number | range start_imsi to end_imsi }

- no
  If added previously, removes the specified subscriber IMSI number(s) from the current IMSI pool.

- imsi_number
  Specifies an IMSI number to add to the current IMSI pool.
  imsi_number must be an IMSI number, and must be a sequence of hexadecimal digits between 1 and 15.

- start_imsi to end_imsi
  Specifies a range of IMSI numbers to add to the current IMSI pool.
  start_imsi specifies the starting IMSI number of the range and must be less than end_imsi.
  end_imsi specifies the ending IMSI number of the range and must be greater than start_imsi.

Usage

Use this command to add an individual or range of subscriber IMSI numbers to an IMSI pool. Up to 10 sets of IMSI numbers can be configured in each IMSI pool.

Example

The following command adds IMSI numbers from 310150987654321 to 310150987656879 to the current IMSI pool:

      imsi range 310150987654321 to 310150987656879
Chapter 14
ACS Packet Filter Configuration Mode Commands

The ACS Packet Filter Configuration Mode is used to create and configure Active Charging Service (ACS) packet filters.

Mode

Exec > ACS Configuration > Packet Filter Configuration

`active-charging service service_name > packet-filter packet_filter_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-packet-filter)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
**direction**

This command allows you to specify the direction in which the current packet filter will be applied.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Packet Filter Configuration

`active-charging service service_name > packet-filter packet_filter_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-packet-filter)#
```

**Syntax**

```
direction { bi-directional | downlink | uplink }

default direction
```

---

**default**

Configures this command with its default setting.
Default: `bi-directional`

**bi-directional**

Specifies that the packet filter has to be applied in both uplink and downlink directions.

**downlink**

Specifies that the packet filter has to be applied only in the downlink direction.

**uplink**

Specifies that the packet filter has to be applied only in the uplink direction.

**Usage**

Use this command to specify the direction in which the packet filter has to be applied.

**Example**

The following command specifies that the packet filter must be applied in the downlink direction:

```
direction downlink
```
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
exit

**Usage**
Use this command to return to the parent configuration mode.
ip local-port

This command allows you to configure the IP 5-tuple local port(s) for the current packet filter.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Packet Filter Configuration
active-charging service service_name > packet-filter packet_filter_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-packet-filter)#

Syntax

ip local-port \{ = port_number | range start_port_number to end_port_number \}

no ip local-port

---

no

If previously configured, deletes the ip local-port configuration from the current packet filter.

---

port_number

Specifies the port number of the transport protocol.

port_number must be the port number, and must be an integer from 1 through 65535.

---

range start_port_number to end_port_number

Specifies a range of port numbers.

start_port_number and end_port_number must be integers from 1 through 65535.

end_port_number must be greater than start_port_number.

---

Usage

Use this command to configure the IP local port(s) for a packet filter.

---

Example

The following command configures the IP local port as 456:

    ip local-port 456
ip protocol

This command allows you to configure the IP protocol(s) for the current packet filter.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Packet Filter Configuration

active-charging service service_name > packet-filter packet_filter_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-packet-filter)#

Syntax

In StarOS 9.0 and later releases:

```
ip protocol = protocol_number
no ip protocol
```

In StarOS 8.2 and earlier releases:

```
ip protocol { = protocol_number | range start_protocol_number to end_protocol_number }
no ip protocol
```

---

**Important:** In StarOS 9.0 and later releases this option is deprecated.

Specifies the transport protocol field in the IP header. *protocol_number* must be the numerical value of the protocol, and must be an integer from 1 through 255.

```
range start_protocol_number to end_protocol_number
```

---

**Usage**

Use this command to configure the protocol(s) for a packet filter.

**Example**

The following command configures the protocol assignment number 300:
ip protocol = 300
**ip remote-address**

This command allows you to configure the IP remote address(es) for the current packet filter.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > ACS Configuration > Packet Filter Configuration

```
cisco> active-charging service service_name > packet-filter packet_filter_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-packet-filter)#
```

**Syntax**

In StarOS 9.0 and later releases:

```
ip remote-address = { ipv4/ipv6_address | ipv4/ipv6_address/mask } no ip remote-address
```

In StarOS 8.2 and earlier releases:

```
ip remote-address { = { ipv4/ipv6_address | ipv4/ipv6_address/mask } | range { start_ipv4/ipv6_address | start_ipv4/ipv6_address/mask } to { end_ipv4/ipv6_address | end_ipv4/ipv6_address/mask } } no ip remote-address
```

If previously configured, deletes the IP remote-address configuration from the current packet filter.

```
ip remote-address = { ipv4/ipv6_address | ipv4/ipv6_address/mask }
ip4/ipv6_address specifies the IPv4/IPv6 address.
ipv4/ipv6_address/mask specifies the IPv4/IPv6 address and the number of subnet bits representing the subnet mask in shorthand.
```

```
ip remote-address range { start_ipv4/ipv6_address | start_ipv4/ipv6_address/mask } to { end_ipv4/ipv6_address | end_ipv4/ipv6_address/mask }
```

**Important:** In StarOS 9.0 and later releases this keyword has been deprecated.

```
range specifies a range of IPv4/IPv6 addresses.
start_ipv4/ipv6_address and end_ipv4/ipv6_address specify, for the range, the starting and ending IPv4/IPv6 addresses.end_ipv4/ipv6_address must be greater than start_ipv4/ipv6_address.
```
**Usage**

Use this command to configure the remote address(es) for a packet filter.

**Example**

The following command configures the IP remote address as 10.2.3.4/24:

```
ip remote-address = 10.2.3.4/24
```
## ip remote-port

This command allows you to configure the IP remote port(s) for the current packet filter.

### Product
ACS

### Privilege
Security Administrator, Administrator

### Mode
Exec > ACS Configuration > Packet Filter Configuration

```
active-charging service service_name > packet-filter packet_filter_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-packet-filter)#
```

### Syntax

```
ip remote-port { = port_number | range start_port_number to end_port_number } 
no ip remote-port
```

- **port_number**
  - Specifies the port number of the transport protocol.
  - `port_number` must be the port number, and must be an integer from 1 through 65535.

- **range start_port_number to end_port_number**
  - Specifies a range of port numbers.
  - `start_port_number` and `end_port_number` must be integers from 1 through 65535.
  - `end_port_number` must be greater than `start_port_number`.

### Usage
Use this command to configure the IP remote port(s) for a packet filter.

### Example
The following command configures the IP remote port as 789:

```
  ip remote-port = 789
```
priority

This command allows you to configure the current packet filter’s priority.

**Important:** This command is deprecated in certain 9.0 releases and in 10.0 and later releases. The precedence values of packet filters (those from both dynamic and predefined rules) are assigned by the PCEF based on an internal process.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Packet Filter Configuration

```
active-charging service service_name > packet-filter packet_filter_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-packet-filter)#
```

**Syntax**

```
priority priority
no priority
```

- **no**
  If previously configured, deletes the priority configuration in the current packet filter.

- **priority**
  Specifies this packet filter’s priority
  `priority` must be an integer from 0 through 255.

**Usage**

Use this command to configure the packet filter’s priority. The priority must be configured for the packet filter to be used in a TFT. Packets are compared against packet filters in a prioritized fashion, with 0 being the highest priority. Without this setting, this filter will not be used.

**Example**

The following command configures the packet filter’s priority as 3:

```
priority 3
```
Chapter 15
ACS Port Map Configuration Mode Commands

The ACS Port Map Configuration Mode is used to define an application-port mapping in the ACS Configuration Mode. The application-port map associates a range of TCP/UDP ports to a specific application/protocol within a rule definition (ruledef).

Mode

Exec > ACS Configuration > ACS Port Map Configuration

active-charging service service_name > port-map port_map_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-port-map)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Use this command to return to the parent configuration mode.
port

Adds or removes an individual or a range of TCP/UDP port numbers associated with an application or protocol from the current port map.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > ACS Port Map Configuration

active-charging service service_name > port-map port_map_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-port-map)#

Syntax

[ no ] port { port_number | range start_port_number to end_port_number }

no
If added previously, removes the specified TCP/UDP port numbers from the current port map.

port_number
Specifies a TCP/UDP port number to add to the current port map.
port_number is expressed an integer from 1 through 65535.

range start_port_number to end_port_number
Specifies a range of port numbers to add to the current port map.
start_port_number specifies the starting port number of the range, it must be an integer from 1 through 65535, and must be less than end_port_number.
end_port_number specifies the ending port number of the range, it must be an integer from 1 through 65535, and must be greater than start_port_number.

Usage
Use this command to add an individual or a range of TCP/UDP port numbers to a port map. Up to 10 sets of ports can be configured in each port map.

Example
The following command adds all TCP/UDP port numbers from 3112 through 5000 to the port map:

    port range 3112 to 5000
Chapter 16
ACS QoS-Group-of-Ruledefs Configuration Mode
Commands

The ACS QoS-Group-of-Ruledefs Configuration Mode is used to configure groups of rule definitions (ruledefs).

Mode

Exec > ACS Configuration > QoS-Group-of-Ruledefs Configuration

`active-charging service service_name > qos-group-of-ruledefs group_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-qos-group-of-ruledefs)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
add-group-of-ruledef

This command allows you to add or remove groups-of-ruledefs from a qos-group-of-ruledefs.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > QoS-Group-of-Ruledefs Configuration

active-charging service service_name > qos-group-of-ruledefs group_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-qos-group-of-ruledefs)#

Syntax

[ no ] add-group-of-ruledef group_of_ruledef_name

  no
  If added previously, removes the specified group-of-ruledef from the current qos-group-of-ruledefs.

  group_of_ruledef_name
  Specifies name of the group-of-ruledef to add/remove from the current qos-group-of-ruledefs.
  group_of_ruledef_name must be the name of an ACS group-of-ruledef, and must be an alphanumeric string of 1 through 63 characters.

Usage

Use this command to add/remove a group-of-ruledefs from a qos-group-of-ruledefs.

Example

The following command adds the group-of-ruledef named grpruledef1 to the current qos-group-of-ruledefs:

    add-group-of-ruledef grpruledef1
add-ruledef

This command allows you to add or remove ruledefs from a qos-group-of-ruledefs.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > QoS-Group-of-Ruledefs Configuration

```
active-charging service service_name > qos-group-of-ruledefs group_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-qos-group-of-ruledefs)#
```

**Syntax**

```
[ no ] add-ruledef ruledef_name
```

**no**
If added previously, removes the specified ruledef from the current qos-group-of-ruledefs.

**ruledef_name**
Specifies name of the ruledef to add/remove from the current qos-group-of-ruledefs.

**Usage**
Use this command to add/remove ruledefs from a qos-group-of-ruledefs.

**Example**
The following command adds the ruledef `ruledef23` to the current qos-group-of-ruledefs:

```
add-ruledef ruledef23
```
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

exit

Usage
Use this command to return to the parent configuration mode.
Chapter 17
ACS Readdress Server List Configuration Mode

The ACS Readdress Server List Configuration Mode is used to add, configure, and delete servers to the server list for DNS redirection.

Mode

Exec > ACS Configuration > Readdress Server List Configuration

```
active-charging service service_name > readdress-server-list server_list_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-readdress-server-list)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
consecutive-failures

This command allows you to configure the consecutive number of times a server can be unreachable after which the system marks the server as inactive.

**Important:** This command is license dependent. For more information contact your Cisco account representative.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Readdress Server List Configuration

```
active-charging service service_name > readdress-server-list server_list_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-readdress-server-list)#
```

**Syntax**

```
consecutive-failures consecutive_failures

default consecutive-failures
```

- **default**

  Configures this command with its default setting.

  Default: 5

- **consecutive_failures**

  Specifies the consecutive number of times a server can be unreachable after which the system marks the server as inactive.

  `consecutive_failures` must be an integer from 1 through 10.

**Important:** If not explicitly configured, the default value of 5 will be used.

**Usage**

Use this command to configure the consecutive number of response failures, after which a server is marked as inactive.

**Example**

The following command configures the number of consecutive server response failures to 4:

```
consecutive-failures 4
```
**end**

Exits the current configuration mode and returns to the Exec mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

```plaintext
end
```

**Usage**

Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
```
exit
```

**Usage**
Use this command to return to the parent configuration mode.
reactivation-time

This command allows you to configure the time duration (in seconds) after which the status of a previously inactive server is rechecked.

**Important:** This command is license dependent. For more information contact your Cisco account representative.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Readdress Server List Configuration

```
active-charging service service_name > readdress-server-list server_list_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-readdress-server-list)#
```

**Syntax**

```
reactivation-time reactivation_time

default reactivation-time
```

**default reactivation-time**

```
default
Configns this command with its default setting.
Default: 300 seconds
```

```
reactivation_time
Specifies the time duration after which the status of the inactive server is rechecked.
reactivation_time must be an integer from 1 through 1800.
```

**Important:** If not explicitly configured, the default value of 300 seconds will be used.

**Usage**

Use this command to configure the time duration (in seconds) after which the status of a previously inactive server is rechecked.

**Example**

The following command configures the reactivation time to 180 seconds:

```
reactivation-time 180
```
response-timeout

This command allows you to configure the time duration for which the system will wait for a response from the server before marking it unreachable.

**Important:** This command is license dependent. For more information contact your Cisco account representative.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Readdress Server List Configuration

```
active-charging service service_name > readdress-server-list server_list_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-readdress-server-list)#
```

**Syntax**

```
response-timeout response_timeout

default response-timeout
```

- **default**
  Configures this command with its default setting.
  Default: 1000 milliseconds

- **response_timeout**
  Specifies the time duration (in milliseconds) for which the system will wait for a response from the server before marking it unreachable.
  response_timeout must be an integer from 1 through 10000.

**Important:** If not explicitly configured, the default value of 1000 milliseconds will be used.

**Usage**

Use this command to configure the time duration (in milliseconds) for which the system will wait for a response from the server before marking it unreachable.

**Example**

The following command sets the server response timeout to 4500 milliseconds:

```
response-timeout 4500
```
server

This command allows you to configure the DNS server(s) to which flow will be readdressed.

Important: This command is license dependent. For more information contact your Cisco account representative.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Readdress Server List Configuration

active-charging service service_name > readdress-server-list server_list_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-readdress-server-list)#

Syntax

server [ipv4_address | ipv6_address] [ port port_number ]

no server [ ipv4_address | ipv6_address ]

no

If previously configured, disables the specified server configuration.

ipv4_address

Specifies the IP address of the DNS server.
ipv4_address must be expressed in IPv4 dotted-decimal notation format.
ipv6_address must be expressed in IPv6 colon-separated-hexadecimal notation.

port port_number

Specifies the TCP port of the DNS server.
port_number must be an integer from 1 through 65535.

Usage

Use this command to configure the DNS server(s) to which the flow will be readdressed based on the contents of the Fully Qualified Domain Name (FQDN).

Example

The following commands configure the DNS servers for packet flow to 192.168.12.101, 192.168.12.102, and 2607:f0d0:1002:51::4/64:

server 192.168.12.101

server 192.168.12.102
server 2607:f0d0:1002:51::4/64

The following command removes the DNS server configuration for 192.168.12.101 that was configured above:

    no server 192.168.12.101
Chapter 18
ACS Rulebase Configuration Mode Commands

The ACS Rulebase Configuration Mode is used to configure Active Charging Service (ACS) rulebases.

**Mode**

Exec > ACS Configuration > Rulebase Configuration

```
active-charging service service_name > rulebase rulebase_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
**action priority**

This command allows you to configure the action priority for a ruledef / group-of-ruledefs in the current rulebase.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Rulebase Configuration

`active-charging service service_name > rulebase rulebase_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

**Syntax**

```
action priority action_priority { [ dynamic-only | static-and-dynamic | timedef timedef_name ] { group-of-ruledefs ruledefs_group_name | ruledef ruledef_name } charging-action charging_action_name [ monitoring-key monitoring_key ] [ description description ] }
```

```
no action priority action_priority
```

If previously configured, deletes the specified action priority configuration from the current rulebase.

**priority action_priority**

Specifies a priority for the specified ruledef / group-of-ruledefs in the current rulebase.

`action_priority` must be unique in the current rulebase, and must be an integer from 1 through 65535. The priority controls the order in which this instance of the CLI command will be examined. Lower numbered priorities are examined first. Up to 2048 instances may be configured, totaled among all rulebases.

**Important:** If there are any changes to action priority and the Override Control/Inheritance feature is enabled, then execute the CLI command “update active-charging override-control rulebase-config”. For more information on this command, see the Command Line Interface Reference.
Default: Enabled

**Important:** When R7 Gx is enabled, “static-and-dynamic” rules behave exactly like “dynamic-only” rules. That is, they must be activated explicitly by the Policy and Charging Rules Function (PCRF). When Gx is not enabled, “static-and-dynamic” rules behave exactly like static rules.

```
timedef timedef_name
```

**Important:** This keyword is only available in StarOS 8.1 and StarOS 9.0 and later releases.

Associates the specified time definition with the ruledef / group-of-ruledefs. Timedefs activate or deactivate ruledefs / groups-of-ruledefs, making them available for rule matching only when they are active.

*timedef_name* must be the name of a timedef, and must be an alphanumeric string of 1 through 63 characters.

A timedef can be used with several ruledefs / group-of-ruledefs. When a packet is received, and a ruledef / group-of-ruledefs is eligible for rule matching, if a timedef is associated with the ruledef / group-of-ruledefs, before rule matching the packet-arrival time is compared with the timeslots configured in the timedef. If the packet arrived in any of the timeslots configured in the associated timedef, rule matching is undertaken, else the next ruledef / group-of-ruledefs is considered.

**Important:** The time considered for timedef matching is the system’s local time.

```
ruledef ruledef_name
```

Adds the specified ruledef to the current rulebase.

*ruledef_name* must be the name of a ruledef, and must be an alphanumeric string of 1 through 63 characters.

If the specified ruledef does not exist, there will be no ruledef triggers for this action priority within the current rulebase.

**Important:** If the ruledef specified here is deleted or is not configured, the system accepts it without applying any ruledef under current rulebase for this action priority.

```
group-of-ruledefs ruledefs_group_name
```

Adds the specified group-of-ruledefs to the current rulebase.

*ruledefs_group_name* must be the name of a group-of-ruledefs, and must be an alphanumeric string of 1 through 63 characters.

When a group-of-ruledefs is specified, if any of the ruledefs within the group matches, the specified charging-action is applied, any more of the action instances are not processed.

**Important:** If the group-of-ruledefs specified here is deleted or is not configured, the system accepts it without applying any ruledefs under current rulebase for this action priority.

```
charging-action charging_action_name
```

Specifies the charging action.
charging_action_name must be the name of a charging action, and must be an alphanumeric string of 1 through 63 characters. If the specified charging action does not exist, there will be no charging action triggers for this action priority within the current rulebase.

**Important:** If the charging action specified here is not configured or is later deleted, the system will not apply any charging action under current rulebase for this action priority.

monitoring_key monitoring_key

Associates the specified monitoring-key with ruledefs for usage monitoring. 
monitoring_key must be an integer from 1 through 4000000000.

description description

Adds specified text to the rule and action. 
description must be an alphanumeric string of 1 through 63 characters.

**Usage**

Use this command to configure action priorities for ruledefs / group-of-ruledefs in a rulebase. This CLI command can be entered multiple times to specify multiple ruledefs and charging actions. The ruledefs are examined in priority order, until a match is found and the corresponding charging action is applied.

**Example**

The following command assigns a rule and action with the action priority of 23, a ruledef named test, and a charging action named test1 to the current rulebase:

```
action priority 23 ruledef test charging-action test1
```
**active-charging rf**

This command allows you to enforce default rating group/service identifier on all PCC rules, predefined ACS rules, and static ACS rules for Rf-based accounting.

> **Important:** This command is customer specific. For more information contact your Cisco account representative.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Rulebase Configuration

```
active-charging service service_name > rulebase rulebase_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

**Syntax**

```
active-charging rf { rating-group-override rating_group | service-id-override service_id }
```

```
{ default | no } active-charging rf { rating-group-override | service-id-override }
```

---

**default**

Configures this command with its default setting.

Default: Override configuration is disabled; same as no.

---

**no**

Disables the override configuration.

**no active-charging rf rating-group-override:** Rating group override will not be enforced on the PCC rules, predefined ACS rules, and static ACS rules. If any of these rules have their own rating group, it will continue to use that.

**no active-charging rf service-id-override:** Service ID override will not be enforced on the PCC rules, predefined ACS rules, and static ACS rules. If any of these rules have their own service ID, it will continue to use that.

---

**rating-group-override rating_group**

Enforces the specified rating group on all PCC rules, predefined ACS rules, and static ACS rules. If any of these rules have their own rating group, it will be overridden by the specified rating group.

**rating_group** must be an integer from 1 through 65535.

---

**service-id-override service_id**

Enforces the specified service ID on all PCC rules, predefined ACS rules, and static ACS rules. If any of these rules have their own service ID, it will be overridden by the specified service ID.
active-charging rf

```
  service_id must be an integer from 1 through 65535.  
```

---

**Usage**

Use this command to enforce a specific rating group / service identifier on all PCC rules, predefined ACS rules, and static ACS rules for RF-based accounting. As this CLI configuration is applied at the rulebase level, all the APNs that have the current rulebase defined will inherit the configuration.

**Example**

The following command configures the service ID 100:

```
  active-charging rf service-id-override 100
```
**bandwidth default-policy**

This command allows you to configure the default bandwidth policy for the current rulebase.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Rulebase Configuration

`active-charging service service_name > rulebase rulebase_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

**Syntax**

```
bandwidth default-policy bandwidth_policy_name [ fallback-enabled ]
```

```
no bandwidth default-policy
```

- **no**
  If previously configured, deletes the bandwidth default-policy configuration from the current rulebase.

  `bandwidth_policy_name`

  Specifies the default bandwidth policy for the current rulebase.

  `bandwidth_policy_name` must be the name of a bandwidth policy, and must be an alphanumeric string of 1 through 63 characters.

- **fallback-enabled**
  Determines whether policy under rulebase can be applied as a fallback value. Fallback is disabled by default.

**Usage**

Use this command to configure the default bandwidth policy for a rulebase.

For subscribers using the current rulebase, the default bandwidth policy will be used if in the APN/Subscriber profile the `default active-charging bandwidth-policy fallback-enabled` command is configured, or no bandwidth policy is configured.

**Example**

The following command configures a bandwidth policy named `standard` for the rulebase:

```
bandwidth default-policy standard fallback-enabled 
```
**billing-records**

This command allows you to configure the type of billing to be performed for subscriber sessions.

**Product**
- GGSN
- P-GW
- SAEGW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Rulebase Configuration

`active-charging service service_name > rulebase rulebase_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

**Syntax**

```
billing-records { egcdr | radius | rf | udr udr-format udr_format_name [ failure-handling-udr-format udr_format_name ] } +

no billing-records
```

`no`

If previously configured, deletes the billing-records configuration from the current rulebase.

`egcdr`

Generates an enhanced G-CDR (eG-CDR) for GGSN / P-GW-CDR for P-GW, and/or UDR with specified format on the occurrence of an interim trigger condition at the end of a subscriber session, or an SGSN-to-SGSN handoff.

`radius`

Generates postpaid RADIUS accounting records at the start and end of a subscriber session, and on the occurrence of an interim trigger condition. RADIUS accounting records are generated for each content ID.

**Important:** In the GGSN, if in the APN configuration the “accounting-mode” is set to “none”, the system continues to send ACS-generated RADIUS accounting messages. In the PDSN, if in the subscriber default configuration the “accounting-mode” is set to “none”, the system does not send any RADIUS accounting messages (including ACS accounting messages).

`rf`

Enables Rf accounting.

Rf accounting is applicable only for dynamic and predefined rules that are marked for it. Dynamic rules have a field offline-enabled to indicate this. To mark a predefined rule as offline-enabled, use this keyword and the `billing-action` command in the ACS Charging Action Configuration Mode.
**Usage**

Use this command to generate enhanced G-CDRs (eG-CDRs), P-GW-CDR for P-GW, RADIUS CDRs and/or UDRs for billing records. The format of eG-CDRs for the default GTPP group is controlled by the `inspector` command in the Context Configuration Mode.

If, in the APN configuration, the “accounting-mode” is set as default (GTPP), and in the rulebase configuration “billing-records egcdr” is configured, both G-CDRs and eG-CDRs are generated if configured.

If, in the APN, the accounting-mode is set to “none” G-CDRs will not be generated.

**Example**

The following command sets the billing record to UDR with UDR format named `udr_format1`:

```
billing-records udr udr-format udr_format1
```
**cca diameter requested-service-unit**

This command allows you to specify the Diameter sub-AVPs to be included in the Diameter group AVP “Requested-Service-Unit” sent with DCCA Credit Control Requests (CCRs).

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Rulebase Configuration

```
active-charging service service_name > rulebase rulebase_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

**Syntax**

```
cca diameter requested-service-unit sub-avp { time cc-time duration | units cc-service-specific-units charging_unit | volume { cc-input-octets bytes | cc-output-octets bytes | cc-total-octets bytes } + }
```

```
no cca diameter requested-service-unit sub-avp
```

No sub-AVPs are included in the Requested-Service-Unit grouped AVP.

```
time cc-time duration
```

Specifies requested service unit for charging time duration in seconds in included sub-AVP. 
`duration` specifies charging time in seconds, and must be an integer from 1 through 4000000000.

```
units cc-service-specific-units charging_unit
```

Specifies requested service unit by service specific units in bytes/packets in included sub-AVP. 
`charging_unit` specifies service-specific charging unit and must be an integer from 1 through 4000000000.

```
volume { cc-input-octets bytes | cc-output-octets bytes | cc-total-octets bytes } +
```

Specifies requested service unit for charging octets by input, output, and total volume in included sub AVP. 
•`cc-input-octets`: Specifies input charging octets. 
•`cc-output-octets`: Specifies output charging octets. 
•`cc-total-octets`: Specifies total charging octets. 
•`bytes`: Specifies volume in bytes and must be an integer from 1 through 4000000000. 
+: Indicates that more than one of the previous keywords can be entered within a single command.
Usage

Use this command to include sub-AVPs based on time, volume, and service specific unit in the “Requested-Service-Unit” grouped AVP with CCRs through Gy interface.

Example

The following command sets the time based sub-AVP with charging duration of 45 seconds in “Requested-Service-Unit” group AVP on DCCA CCRs:

```
cca diameter requested-service-unit sub-avp time cc-time 45
```
cca quota

This command allows you to configure various time- and threshold-based quotas in the Prepaid Credit Control Service (Credit Control Application).

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Rulebase Configuration

active-charging service service_name > rulebase rulebase_name

Entering the above command sequence results in the following prompt:

[local] host_name(config-rule-base)#

Syntax

cca quota { holding-time holding_time content-id content_id | retry-time retry_time [ max-retries retries ] } }

{ default | no } cca quota { holding-time content-id content_id | retry-time }

holding-time holding_time

Specifies the value for the Quota Holding Time (QHT). QHT is used with both time-based and volume-based quotas. After holding_time seconds has passed without user traffic, the quota is reported back and the charging stops until new traffic starts.

holding_time must be an integer from 1 through 4000000000.

content-id content_id

Specifies the content ID (Rating group AVP) to use for the Quota holding time for the current rulebase.

ccontent_id is the content ID specified for credit control service in ACS.

In 12.1 and earlier releases, content_id must be an integer from 1 through 65535.

In 12.2 and later releases, content_id must be an integer from 1 through 2147483647.

retry-time retry_time [ max-retries retries ]

Specifies the retry time for the quota request, in seconds.

retry_time must be an integer from 0 through 86400. To disable this assign 0.

Default: 60

This parameter defines the maximum frequency at which the Credit-Control Application (CCA) tries to obtain quota for a subscriber passing traffic for a category with no/exhausted quota.

For a subscriber not passing traffic, the CCA will not try to obtain quota (except once at session start time, if so configured). The quota request from the no quota state is sent in response to user packets only (never based on a timer).

When subscriber hits a charging action that is a flow redirect, the operator can optionally specify that this redirection shall clear the retry-time timer.
This allows the immediately following chargeable user traffic to trip a quota request, even if it would otherwise have been subject to the retry time limit. Such configuration allows quite a large value for retry-time in quota charging or a top-up scenario.

`max-retries retries` configures the maximum number of retries allowed for blacklisted categories. This option has a default value of 65535 retries (the maximum value). `retries` must be an integer from 1 through 65535. To disable this assign 0.

**Usage**

Use this command to set the prepaid credit control quotas.

`cca quota retry time` allows an operator to set the amount of time that the ACS waits before it retries the prepaid server for a content ID for which quota was exhausted earlier.

When the server sends the quota holding time (QHT) it has highest priority to use that QHT regardless of the value configured in the rulebase or Credit Control Application Configuration Mode. QHT configured here has the second priority for the content ID (rating group) configured here.

If the QHT is not available from the server or rulebase configuration mode, the QHT values configured via the Credit Control Application Configuration Mode are used.

**Example**

The following command configures the prepaid credit control request retry time to 30 seconds:

```
default cca quota retry-time 30
```

The following command specifies the system to use the QHT value configured in the Credit Control Application Mode:

```
no cca quota holding-time content-id 1
```

The following command specifies the system to ignore the QHT value configured in the Credit Control Application Mode:

```
default cca quota holding-time content-id 1
```

The following command configures the prepaid credit control request retry time to 60 seconds and the maximum number of retries to 65535:

```
default cca quota retry-time max-retries
```
cca quota time-duration algorithm

This command allows you to specify the algorithm to compute time duration for Prepaid Credit Control Application quotas in the current rulebase.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Rulebase Configuration

active-charging service service_name > rulebase rulebase_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-rule-base)#

Syntax

cca quota time-duration algorithm { consumed-time seconds [ plus-idle ] | continuous-time-periods seconds | parking-meter seconds } [ content-id content_id ]

default cca quota time-duration algorithm

no cca quota time-duration algorithm { consumed-time | continuous-time-periods | parking-meter } [ content-id content_id ]

no
If previously configured, deletes the quota time-duration algorithm configuration from the current rulebase.

default
Configures this command with its default setting.

calculated-time seconds
Specifies the Quota Consumption Time (QCT) in seconds. QCT is used with active time-based quotas and to determine chargeable time envelopes for consuming time quota.
seconds must be an integer from 1 through 4294967295.
Default: 0 (disabled)
A time envelope is the basis for reporting active usage. For each time envelope, the quota consumption includes the last QCT (duration between first packet and last packet + QCT).

plus-idle
Specifies the idle time for QCT.
When used along with consumed-time it indicates the active usage + idle time, when no traffic flow occurs.

continuous-time-periods seconds
Specifies the charging quota continuous period, in seconds.
seconds must be an integer from 1 through 4294967295.
Default: 0 (disabled)
The Continuous Time Periods (CTP) mechanism constructs time-envelopes from consecutive base time intervals in which traffic has occurred up to and including a base time interval which contains no traffic. As with Quota-Consumption-Time envelopes, the end of an envelope can only be determined “retrospectively”. Again, as with Quota-Consumption-Time, the envelope for CTP includes the last base time interval (the one which contained no traffic).

`parking-meter seconds`

Specifies the Parking Meter (PM) period, in seconds, for a particular rating group.

seconds must be an integer from 1 through 4294967295.

Default: 0 (disabled)

This mechanisms utilizes time quota, but instead of consuming linearly—once a decision to consume has been taken—the granted quota is consumed discretely in “chunks” of the base time interval at the start of each base time interval. Traffic is then allowed to flow for the period of the consumed quota.

The time interval seconds defines the length of the Parking Meter. A time-envelope corresponds to exactly one PM (and thus to one base time interval).

`content-id content_id`

Specifies the content ID (Rating group AVP) to use for the CCA Quota time duration algorithm selection in the current rulebase.

content_id is the content ID specified for credit control service in ACS.

In 12.1 and earlier releases, `content_id` must be an integer from 1 through 65535.

In 12.2 and later releases, `content_id` must be an integer from 1 through 2147483647.

Usage

Use this command to set the various time charging algorithms/schemes for prepaid credit control charging.

If operator chooses `parking-meter seconds` style charging, then time is billed in `seconds` chunks.

Example

The following command configures the QCT to consumed-time duration of 400 seconds:

```
cca quota time-duration algorithm consumed-time 400
```
cca radius accounting interval

This command allows you to configure how often interim updates are generated by the RADIUS Credit Control Application to be sent to the prepaid server.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Rulebase Configuration
active-charging service service_name > rulebase rulebase_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-rule-base)#

Syntax

cca radius accounting interval interval

{ default | no } cca radius accounting interval

default
Configures the command with its default setting.
Default: Disabled; same as no cca radius accounting interval

no
Disables interim updates.

interval
Specifies the time interval, in seconds, between interim updates generated by the RADIUS Credit Control Application.
interval must be an integer from 1 through 3600.
Default: 1 (Disabled)

Usage
Use this command to specify the RADIUS accounting interval between accounting of a prepaid subscriber. The same parameters are applicable for RADIUS server group.

Example
The following command defines RADIUS accounting interval of 20 seconds for RADIUS prepaid service in the rulebase:

cca radius accounting interval 20
**cca radius charging context**

This command allows you to specify the RADIUS servers used for the current rulebase when RADIUS credit control is enabled.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Rulebase Configuration

`active-charging service service_name > rulebase rulebase_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

**Syntax**

```
cca radius charging context vpn_context [ group server_group_name ]
no cca radius charging context
```

- **no**
  RADIUS credit control will not be performed.

- **vpn_context**
  Specifies the charging context where RADIUS prepaid charging parameters are configured. `vpn_context` must be an alphanumeric string of 1 through 79 characters.

- **group server_group_name**
  Specifies the RADIUS server group. `server_group_name` must be the name of a RADIUS server group, and must be an alphanumeric string of 1 through 63 characters.

**Usage**

Use this command to specify the RADIUS charging context where RADIUS prepaid charging parameters are configured. The same parameters are applicable for RADIUS server group.

**Example**

The following command defines RADIUS charging context `prepaid_rad1` for RADIUS prepaid charging in the rulebase:

```
cca radius charging context prepaid_rad1
```
**cca radius user-password**

This command allows you to configure the value to use for the “User-Password” attribute in RADIUS messages sent to the prepaid server.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Rulebase Configuration

```
active-charging service service_name > rulebase rulebase_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

**Syntax**

```
cca radius user-password [ encrypted ] password password
```

```
no cca radius user-password
```

If previously configured, deletes the RADIUS prepaid service user password configured in the current rulebase.

```
[ encrypted ] password password
```

Specifies the password for prepaid services within the current rulebase.

In 12.1 and earlier releases, `password` must be an alphanumeric string of 1 through 63 characters with or without encryption.

In 12.2 and later releases, `password` must be an alphanumeric string of 1 through 63 characters without encryption, and 1 through 132 characters with encryption enabled.

The `encrypted` keyword is intended only for use by the system while saving configuration scripts. The system displays the `encrypted` keyword in the configuration file as a flag that the variable following the `password` keyword is the encrypted version of the plain text password. Only the encrypted password is saved as part of the configuration file.

**Usage**

Use this command to specify the RADIUS user password for prepaid services within the current rulebase.

**Example**

The following command configures the user password as `user_123` without encryption in the current rulebase:

```
cca radius user-password password user_123
```
charging-action-override

This command allows you to enable/disable overriding charging parameters of static rule with those of an ip-any rule or a specified dynamic rule.

Product
GGSN
P-GW

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Rulebase Configuration

```
active-charging service service_name > rulebase rulebase_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax

```
charging-action-override custom1 [ use-rule dynamic_rule_name ]
{ default | no } charging-action-override
```

- **default**
  Configures this command with its default setting. Default: Disables overriding charging parameters of static rule with those of an ip-any or a specified dynamic rule.

- **no**
  Disables overriding charging parameters of static rule with those of an ip-any or a specified dynamic rule.

- **custom1**
  Specifies overriding Online/Offline, Service ID, Content ID, Flow Control, ARP, and QCI.

- **use-rule dynamic_rule_name**
  Optional: Specifies the dynamic rule to inherit charging parameters from. If a dynamic rule name is not specified, the charging properties will be inherited from any dynamic rule. 
  
  `dynamic_rule_name` specifies name of the dynamic rule, and must be an alpha and/or numeric string of 1 through 63 characters in length.

Usage

Use this command to enable/disable overriding charging parameters of static rule with those of a dynamic ip-any rule or a specified dynamic rule.

Example

The following command specifies to enable overriding charging parameters of static rule with those of a dynamic rule named `test`:
charging-action-override custom1 use-rule test
charging-rule-optimization

This command allows you to configure the internal optimization level to use, for improved performance, when evaluating each instance of the action priority command.

Important: In StarOS 14.0 and later releases, this command is deprecated. In StarOS 14.0 and later releases, rule optimization is always enabled with the optimization level set to high.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Rulebase Configuration

active-charging service service_name > rulebase rulebase_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-rule-base)#

Syntax

charging-rule-optimization { high | low | medium }

default charging-rule-optimization

default

Configures this command with its default setting.
Default: In 11.0 and later releases: high In 10.0 and earlier releases: low

high

Enables the highest level of optimization with high memory utilization.

low

Enables minimal level of optimization with minimal memory utilization.

medium

Enables medium level of optimization with moderate memory utilization.

Important: In 11.0 and later releases, the medium keyword is deprecated.

Usage

Use this command to specify the level of internal optimization for improved performance when evaluating each instance of the action priority command.
Both the high and medium options cause re-organization of the entire memory structure whenever any change is made, such as on the addition of an `action priority` command.

**Example**

The following command specifies the highest optimization level for rule search and matching in the rulebase:

```
charging-rule-optimization high
```
constituent-policies

This command allows you to configure the Bandwidth, Content Based Billing (CBB), and Firewall/Firewall-and-NAT constituent policies. The combination of the values of all three policies will uniquely identify the associated rulebase.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Rulebase Configuration

active-charging service service_name > rulebase rulebase_name

Entering the above command sequence results in the following prompt:
[local]host_name(config-rule-base)#

Syntax

constituent-policies { bandwidth-policy bandwidth_policy_name | cbb-policy cbb_policy_name | firewall-policy fw_policy_name | fw-and-nat-policy fw_nat_policy_name } +

no constituent-policies

---

no

If previously configured, deletes the constituent-policies configuration from the current rulebase.

---

bandwidth-policy bandwidth_policy_name

Specifies the Bandwidth policy.

bandwidth_policy_name must be the name of a bandwidth policy, and must be an alphanumeric string of 1 through 63 characters.

---

cbb-policy cbb_policy_name

Specifies the Content Based Billing (CBB) policy.

cbb_policy_name must be the name of a CBB policy, and must be an alphanumeric string of 1 through 63 characters.

---

firewall-policy fw_policy_name

---

Important: This keyword is customer specific. For more information, please contact your Cisco account representative.

Specifies the Stateful Firewall policy.

fw_policy_name must be the name of a Stateful Firewall policy, and must be an alphanumeric string of 1 through 63 characters.
**fw-and-nat-policy** *fw_nat_policy_name*

**Important:** This keyword is customer specific, and is only available in StarOS 8.1 and in StarOS 9.0 and later releases.

Specifies the Firewall-and-NAT policy.

*fw_nat_policy_name* must be the name of a Firewall-and-NAT policy, and must be an alphanumeric string of 1 through 63 characters.

**Usage**

Use this command to configure the bandwidth, CBB, and Firewall/Firewall-and-NAT constituent policies that will identify the rulebase. The combination of the values of all three policies will uniquely identify the rulebase associated.

**Example**

The following command configures the constituent bandwidth policy named *test123*:

```
constituent-policies bandwidth-policy test123
```
content-filtering category policy-id

This command allows you to configure the Content Filtering Category Policy Identifier for Policy-based Content Filtering support in the current rulebase.

**Product**

CF

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > ACS Configuration > Rulebase Configuration

`active-charging service service_name > rulebase rulebase_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

**Syntax**

```
content-filtering category policy-id cf_policy_id

no content-filtering category policy-id [ cf_policy_id ]
```

- no
  - If previously configured, deletes the configuration from the current rulebase.
  - In StarOS 8.1 and later releases, optionally the policy ID can be specified. If the specified policy ID is invalid, or is not configured in the rulebase, an error message is displayed. If no policy ID is specified, whatever policy is configured, if any, is removed from the rulebase.

```
content-filtering category policy-id cf_policy_id

Configures the specified Content Filtering Category Policy in the current rulebase.

`cf_policy_id` must be the ID of an existing Content Filtering Category Policy, and must be an integer from 1 through 4294967295.
```

**Important:** If the specified Content Filtering Category Policy does not exist, all packets will be passed regardless of the categories/actions determined for such packets.

**Important:** The category policy ID that is configured using the `category policy-id cf_policy_id` command in the APN/Subscriber Configuration Mode prevails over this configuration.

**Usage**

Use this command to configure the Content Filtering Category Policy ID for Policy-based Content Filtering support in the rulebase.

The Content Filtering Category Policy is created/deleted in the ACS Configuration Mode, and is configured in the Content Filtering Policy Configuration Mode.

**Example**

The following command configures the Content Filtering Category Policy ID `101` in the rulebase:
content-filtering category policy-id 101
content-filtering flow-any-error

This command allows you to specify action to take on Content Filtering packets in the case of ACS error scenarios.

**Product**
CF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Rulebase Configuration

```
active-charging service service_name > rulebase rulebase_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

**Syntax**

```
content-filtering flow-any-error { deny | permit }

default content-filtering flow-any-error
```

---

### default content-filtering flow-any-error

**default**

Configures this command with its default setting.

Default: **permit**

---

### deny

Configures flow-any-error configuration as deny.

All the denied packets will be accounted for by the **discarded-flow-content-id** configuration in the Content Filtering Policy Configuration Mode. This content ID will be used to generate UDRs for packets denied via content filtering.

---

### permit

Configures flow-any-error configuration as permit.

---

**Usage**

Use this command to allow/discard content filtering packets in case of ACS error scenarios.

---

**Example**

The following command allows content filtering packets in case of an ACS error:

```
content-filtering flow-any-error permit
```
content-filtering mode

This command allows you to enable/disable the specified Category-based Content Filtering mode in the current rulebase.

**Product**
CF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Rulebase Configuration

```
active-charging service service_name > rulebase rulebase_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

**Syntax**

```
content-filtering mode { category { static-and-dynamic | static-only } | server-group cf_server_group }
```

**no content-filtering mode**

```
no
```

If previously configured, deletes the content-filtering mode configuration from the current rulebase. Content filtering will not to be performed for the current rulebase. This is the default setting.

**category { static-and-dynamic | static-only }**

Specifies the Category-based Content Filtering mode.

- **static-only**: Configures Category-based Content Filtering in static only mode, wherein all URLs are compared against an internal database to categorize the requested content.
  
  Using Category-based Content Filtering support requires configuration of the `require active-charging content-filtering category` command in the Global Configuration Mode.

- **static-and-dynamic**: Configures Category-based Content Filtering in Static-and-Dynamic mode, wherein a static rating of the URL is first performed, and only if the static rating fails to find a match, dynamic rating of the content that the server returns is then performed.

**Important**: Before enabling static-and-dynamic rating in the rulebase, it must be enabled at the global level as the resources required for dynamic rating are allocated at the global level. To enable static-and-dynamic rating at the global level, in the Global Configuration Mode use the `require active-charging content-filtering category static-and-dynamic` command.

```
server-group cf_server_group
```

Enables and configures the Content Filtering Server Group (CFSG) mode within the rulebase to manage an external content filtering server with an Internet Content Adaptation Protocol (ICAP) client system.
cf_server_group must be the name of a CFSG, and must be unique, and must be an alphanumeric string of 1 through 63 characters.
If configured, ACS attempts to establish TCP connections to every server in the named group.

**Usage**

Use this command to enable and apply the content filtering mode in the rulebase to manage a content filtering server with an ICAP client system.

**Example**

The following command enables the content filtering mode for external content filtering server group CF_Server1 in the rulebase:

```
content-filtering mode server-group CF_Server1
```

The following command enables the category based static and dynamic content filtering mode for in the rulebase:

```
content-filtering mode category static-and-dynamic
```
**dynamic-rule order**

This command allows you to specify whether dynamic rules are matched before statically configured rules.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Rulebase Configuration

`active-charging service service_name > rulebase rulebase_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

**Syntax**

```
dynamic-rule order { always-first | first-if-tied }

no dynamic-rule order
```

**no**

If previously configured, deletes the dynamic-rule order configuration from the current rulebase. By default, dynamic rules are matched against the flow prior to static rules.

**always-first**

Specifies to match all the dynamic rules against the flow prior to any static rule.

**first-if-tied**

Specifies to match rules against the flow based on their priority with the condition that dynamic rules match before a static rule of the same priority.

A rule is a combination of a ruledef, charging action, and precedence. Static rules are defined by the action CLI command in the ACS Rulebase Configuration Mode, and are applicable to all subscribers that are associated with the rulebase. Dynamic rules are obtained via a dynamic protocol, such as, the Gx-interface for a particular subscriber session.

**Usage**

Use this command to configure the order in which rules are selected for matching in between dynamic rules (per subscriber) and static rules (from rulebase).

**Example**

The following command matches all dynamic rules against the flow prior to any static rule:

```
dynamic-rule order always-first
```
**edr p2p**

This command configures generation of Event Detail Records (EDR) for P2P events. This command is associated with the Dynamic Software Upgrade process.

**Product**

ACS

ADC

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > ACS Configuration > Rulebase Configuration

```
active-charging service service_name > rulebase rulebase_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

**Syntax**

```
edr p2p p2p_event_list [ charging-edr charging_edr_format_name | edr-format edr_format_name | reporting-edr reporting_edr_format_name ] +
```

```
{ default | no } edr p2p p2p_event_list
```

---

**default**

Configures this command with its default setting.

Default: Disabled

---

**no**

If previously configured, deletes the configuration from the current rulebase.

---

**p2p_event_list**

Specifies the name of the P2P EDR Event. The plugin supports only the “audio-end” and “video-end” events. This P2P event list can be any P2P event that is supported by the plugin.

*p2p_event_list* must be an alphanumeric string of 1 through 128 characters.

---

**charging-edr charging_edr_format_name**

Specifies to generate charging EDR for P2P events.

*charging_edr_format_name* must be the name of a charging EDR format, and must be an alphanumeric string of 1 through 63 characters.

---

**edr-format edr_format_name**

Specifies to generate EDR for P2P events.

*edr_format_name* must be the name of an EDR format, and must be an alphanumeric string of 1 through 63 characters.
**reporting-edr** reporting_edr_format_name

Specifies to generate reporting EDR for P2P events. 
`reporting_edr_format_name` must be the name of a reporting EDR format, and must be an alphanumeric string of 1 through 63 characters.

**Usage**

Use this command to configure the P2P events to generate EDRs. The list of P2P events will be populated from the currently loaded plugin.

A plugin is a functional software entity that provides incremental updates to a pre-existing StarOS software component. Plugins can be dynamically loaded at runtime and do not require a system restart. For more information on the Dynamic Software Upgrade feature, refer to Application Detection and Control Administration Guide.

**Example**

The following command configures the generation of EDRs for P2P audio-end event specifying to use the EDR format named `edr1`:

```
edr p2p audio-end edr-format edr1
```
edr sn-charge-volume

This command allows you to exclude/include packets/bytes that are dropped/retransmitted by the ACS in the total charge volume — “sn-charge-volume” EDR attribute.

**Product**  
ACS

**Privilege**  
Security Administrator, Administrator

**Mode**  
Exec > ACS Configuration > Rulebase Configuration

`active-charging service service_name > rulebase rulebase_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#!
```

**Syntax**

```
[ default | no ] edr sn-charge-volume { count-dropped-units | count-retransmitted-units }
```

---

**default**  
Configures this command with its default setting.  
Default: Exclude, in the total charge volume, packets/bytes dropped/retransmitted by ACS.

---

**no**  
Exclude, in the total charge volume, packets/bytes dropped/retransmitted by ACS.

---

**count-dropped-units**  
Specifies to include dropped units in the total charge volume.

---

**count-retransmitted-units**  
Specifies to include retransmitted units in the total charge volume.

**Usage**

Use this command to exclude/include packets/bytes that are dropped/retransmitted by ACS in the total charge volume — “sn-charge-volume” EDR attribute.  
This command applies only to the “sn-charge-volume” attribute and does not affect the “sn-volume-amt” counts in any way.

**Example**

The following specifies to include units retransmitted by ACS in the sn-charge-volume EDR attribute:

```
edr sn-charge-volume count-retransmitted-units
```
**edr suppress-zero-byte-records**

This command disables/enables the creation of EDRs when there is no data for the flows.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Rulebase Configuration

**Syntax**

```
[ default | no ] edr suppress-zero-byte-records
```

- **default**
  Configures this command with its default setting.
  Default: Disabled; same as `no edr suppress-zero-byte-records`

- **no**
  Disables the suppression of zero-byte EDRs.

- **edr suppress-zero-byte-records**
  Suppresses zero-byte EDRs.

**Usage**
Use this command to disable/enable the creation of EDRs that are empty. The situation where there is a zero-byte EDR would typically be possible when two successive EDRs are generated for a flow. This CLI command suppresses the second such EDR for the flow.
edr transaction-complete

This command enables/disables the generation of an EDR on the completion of a transaction.

⚠️ **Important**: This command is available only in StarOS 8.1 and in StarOS 9.0 and later releases.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Rulebase Configuration

```
active-charging service service_name > rulebase rulebase_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

**Syntax**

In StarOS 12.2 and later releases:

```
edr transaction-complete http [ charging-edr charging_edr_format_name | edr-format edr_format_name | reporting-edr reporting_edr_format_name ] { default | no } edr transaction-complete
```

In StarOS 12.1 and earlier releases:

```
edr transaction-complete http edr-format edr_format_name
```

{ default | no } edr transaction-complete

**Default**
Configures this command with its default setting.
Default: Disabled; same as `no edr transaction-complete`

**no**
If previously configured, deletes the configuration from the current rulebase.

**edr-format edr_format_name**

⚠️ **Important**: This option is available only in 12.1 and earlier releases. In 12.2 and later releases, this option is deprecated and is replaced by the `charging-edr` option.

Specifies to generate EDR on transaction completion, for HTTP protocol.
`edr_format_name` must be the name of an EDR format, and must be an alphanumeric string of 1 through 63 characters.
edr transaction-complete

charging-edr charging_edr_format_name

**Important:** This option is available only in 12.2 and later releases.

Specifies to generate charging EDR on transaction completion.

*charging_edr_format_name* must be the name of a charging EDR format, and must be an alphanumeric string of 1 through 63 characters.

reporting-edr reporting_edr_format_name

**Important:** This option is available only in 12.2 and later releases.

Specifies to generate reporting EDR on transaction completion.

*reporting_edr_format_name* must be the name of a reporting EDR, and must be an alphanumeric string of 1 through 63 characters.

**Usage**

Use this command to configure the generation of an EDR when certain application transactions (for example, request/response pairs) complete. In this release EDR generation is supported only for HTTP protocol. Note that these EDRs are in addition to those that might be generated due to other conditions, for example, EDR configurations in a Charging Action.

**Example**

In 12.1 and earlier releases, the following command configures the generation of EDRs on the completion of transactions for HTTP protocol specifying the EDR format as *test123*:

```
edr transaction-complete http edr-format test123
```

In 12.2 and later releases, the following command configures the generation of charging EDRs on the completion of transactions for HTTP protocol specifying the EDR format as *test123*:

```
edr transaction-complete http charging-edr test123
```
edr voip-call-end

This command enables/disables generation of EDRs on the completion of Voice over IP (VoIP) calls. This command is no longer supported for ADC in 14.0 and later releases.

**Product**
ACS
ADC

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Rulebase Configuration

```
active-charging service service_name > rulebase rulebase_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

**Syntax**

In StarOS 12.2 and later releases:

```
edr voip-call-end { charging-edr charging_edr_format_name | edr-format edr_format_name | reporting-edr reporting_edr_format_name } +
{ default | no } edr voip-call-end
```

In StarOS 12.1 and earlier releases:

```
edr voip-call-end edr-format edr_format_name
{ default | no } edr voip-call-end
```

<table>
<thead>
<tr>
<th><strong>default</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Configures this command with its default setting.</td>
</tr>
<tr>
<td>Default: Disabled; same as no edr voip-call-end</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>no</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>If previously configured, deletes the edr voip-call-end configuration from the current rulebase.</td>
</tr>
</tbody>
</table>

**Important:** This option is available only in 12.1 and earlier releases. In 12.2 and later releases, it has been deprecated and is replaced by the charging-edr option.

Specifies to generate an EDR when a VoIP call ends.

*edr_format_name* must be the name of an EDR format, and must be an alphanumeric string of 1 through 63 characters.
charging-edr charging_edr_format_name

**Important:** This option is available only in 12.2 and later releases.

Specifies to generate a charging EDR when a VoIP call ends. 
*charging_edr_format_name* must be the name of a charging EDR format, and must be an alphanumeric string of 1 through 63 characters.

reporting-edr reporting_edr_format_name

**Important:** This option is available only in 12.2 and later releases.

Specifies to generate a reporting EDR when a VoIP call ends. 
*reporting_edr_format_name* must be the name of a reporting EDR format, and must be an alphanumeric string of 1 through 63 characters.

**Usage**

Use this command to generate an EDR on the completion of voice calls. Note that these EDRs are in addition to those that might be generated due to other conditions, for example EDR configurations in a Charging Action. This command facilitates P2P voice duration reporting.

**Example**

In 12.1 and earlier releases, the following command specifies generating EDRs on completion of VoIP calls using the EDR format *test13*:

```
  edr voip-call-end edr-format test13
```

In 12.2 and later releases, the following command specifies generating charging EDRs on completion of VoIP calls using the EDR format named *test23*:

```
  edr voip-call-end charging-edr test23
```
egcdr inactivity-meter

**Description** This command has been deprecated. It is included in the CLI for backward compatibility with older configuration files. When executed performs no function. Use the `egcdr threshold interval interval [regardless-of-other-triggers]` command for this functionality.
egcdr cdr-encoding

This command allows you to configure the eG-CDR encoding type.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Rulebase Configuration

\[ active-charging service service_name > rulebase rulebase_name \]

Entering the above command sequence results in the following prompt:

\[ [local]host_name(config-rule-base)# \]

**Syntax**

\[ egcdr cdr-encoding { ascii \{ delimiter \{ colon | comma | pipe \} \} | asn.1 } \]

**default egcdr cdr-encoding**

\[ default \]
Configures the default eG-CDR CDR-encoding format.
Default: \textit{asn.1}

\[ ascii \{ delimiter \{ colon | comma | pipe \} \} \]
Specifies to use ASCII encoding type to generate eG-CDR in ASCII format.
\[ delimiter \{ colon | comma | pipe \} \]: Specifies the delimiter character to use in eG-CDRs in ASCII format.
  \[ • colon: Specifies to use “;” (colon) as a delimiter in eG-CDR. \]
  \[ • comma: Specifies to use “,” (comma), as a delimiter in eG-CDR. \]
  \[ • pipe: Specifies to use “|” (pipe) as a delimiter in eG-CDR. \]
Default: \textit{pipe}

\[ asn.1 \]
Specifies to use ASN.1 encoding type to generate eG-CDR in ASN.1 format.
This is the default setting.

**Usage**
Use this command to configure the eG-CDR encoding type.
For more information on using eG-CDR ASCII encoding type in your deployment, contact your Cisco account representative.

**Example**
The following command specifies to use ASCII encoding type to generate eG-CDR in ASCII format while specifying the delimiter character as comma:
egcdr cdr-encoding ascii delimiter comma
egcdr tariff

This command allows you to configure the eG-CDR tariff time to generate new eG-CDRs for GGSN and P-GW-CDRs for P-GW.

Product

GGSN
P-GW
SAEGW

Privilege

Security Administrator, Administrator

Mode

Exec > ACS Configuration > Rulebase Configuration

**active-charging service service_name > rulebase rulebase_name**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax

```
[ no ] egcdr tariff minute minute hour hour
```

- **no**
  
  If previously configured, deletes the configuration from the current rulebase.

- **minute minute**
  
  Specifies the minute for the time-of-day configuration.
  
  *minute* must be an integer from 0 through 59.

- **hour hour**
  
  Specifies the hour for the time-of-day configuration.
  
  *hour* must be an integer from 0 through 23.

Usage

Use this command to configure the eG-CDR tariff time to generate new eG-CDRs for GGSN and P-GW-CDRs for P-GW. Up to four different time-of-day settings may be configured. When any configured tariff time is reached, the current eG-CDR/P-GW-CDR will be closed and a new eG-CDR/P-GW-CDR is opened.

Example

The following command defines an eG-CDR tariff for the 23rd minute of the 22nd hour of the day (10:23 PM):

```
egcdr tariff minute 23 hour 22
```
egcdr threshold

This command allows you to configure the thresholds for generating eG-CDRs for GGSN and P-GW-CDRs for P-GW.

Product
GGSN
P-GW
SAEGW

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Rulebase Configuration

active-charging service service_name > rulebase rulebase_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-rule-base)#

Syntax

egcdr threshold { interval interval [ regardless-of-other-triggers ] | volume { downlink | total | uplink } bytes }

{ default | no } egcdr threshold { interval | volume }

---

no

If previously configured, deletes the eG-CDR threshold configuration from the current rulebase.

---

default

Configures this command with the default settings.
Default: Disabled; same as no egcdr threshold interval and no egcdr threshold interval volume commands.

---

interval interval [ regardless-of-other-triggers ]

Specifies the time interval, in seconds, for closing the eG-CDR/P-GW-CDR if the minimum time duration thresholds are satisfied.
interval must be an integer from 60 through 40000000.
regardless-of-other-triggers: This option enables eG-CDR/P-GW-CDR generation at the fixed time interval irrespective of any other eG-CDR/P-GW-CDR triggers that may have happened in between.
Default: Disabled.

---

volume { downlink | total | uplink } bytes

Specifies the uplink/downlink volume octet counts for the generation of the interim eG-CDRs/P-GW-CDRs.

downlink bytes: Specifies the limit for the number of downlink (from network to subscriber) octets after which the eG-CDR/P-GW-CDR is closed.

bytes must be an integer from 100000 through 4000000000.
Default: 4000000000
\*total bytes\*: Specifies the limit for the total number of octets (uplink+downlink) after which the eG-CDR/P-GW-CDR is closed.

\*bytes\* must be an integer from 100000 through 4000000000.

Default: Disabled

\*uplink bytes\*: Specifies the limit for the number of uplink (from subscriber to network) octets after which the eG-CDR/P-GW-CDR is closed.

\*bytes\* must be an integer from 100000 through 4000000000.

Default: 4000000000

**Usage**

Use this command to configure thresholds to generate eG-CDRs/P-GW-CDRs. Thresholds can be specified for both time interval and for data volume, by entering the command twice (once with interval and once with volume). When either configured threshold is reached, the eG-CDR/P-GW-CDRs will be closed. The volume trigger can be specified for uplink or downlink or combined total (uplink + downlink) byte thresholds. The exact keyword forces the configured volume to exactly match the volume in the eG-CDR/P-GW-CDRs, so the triggering packet might have to be divided across two eG-CDRs/P-GW-CDRs.

When both interval and volume triggers are configured, we'll reset the interval time and accumulated volume amount whenever the eG-CDR/P-GW-CDRs is closed regardless of whether it was due to the interval time expiration or reaching the volume limit. Use the regardless-of-other-triggers optional keyword, if you want the eG-CDRs/P-GW-CDRs closed at the configured regular intervals, regardless of whether eG-CDRs/P-GW-CDRs are being closed due to reaching a volume limit.

When the PDP context is terminated, the eG-CDR/P-GW-CDRs will be closed regardless of whether the thresholds have been reached.

**Example**

The following command defines an eG-CDR threshold interval of 600 seconds:

```
egcdr threshold interval 600
```
egcdr time-duration algorithm

This command allows you to specify the algorithm to compute the duration of time utilization in an eG-CDR for the current rulebase.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Rulebase Configuration

```
active-charging service service_name > rulebase rulebase_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

**Syntax**

```
egcdr time-duration algorithm { consumed-time consumed_time [ plus-idle ] | continuous-time-periods ctp_time | parking-meter seconds }

{ default | no } egcdr time-duration algorithm
```

<table>
<thead>
<tr>
<th>no</th>
</tr>
</thead>
<tbody>
<tr>
<td>If previously configured, deletes the eG-CDR time-duration algorithm configuration from the current rulebase.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>default</th>
</tr>
</thead>
</table>
| Configures this command with its default setting.  
Default: Algorithm configured for CCA, or the CCA default if none is configured. |

<table>
<thead>
<tr>
<th>consumed-time consumed_time [ plus-idle ]</th>
</tr>
</thead>
</table>
| Specifies the actual consumption time in seconds. This is used to determine the actual used chargeable time envelopes for the purpose of consuming time quota.  
`consumed_time` must be an integer from 1 through 4294967295.  
Default: 0 (disabled)  
Time envelope is the basis for reporting active usage. For each time envelope, the time consumption includes the time duration between arrival of last packet and first packet only.  
**plus-idle:** Specifies the idle time between arrival of two packets to include in time usage record in eG-CDR.  
When used along with `consumed-time` it indicates the active usage + idle time, when no traffic flow occurs. |

<table>
<thead>
<tr>
<th>continuous-time-periods ctp_time</th>
</tr>
</thead>
</table>
| Specifies the continuous time period to compute the usage record in eG-CDR.  
`ctp_time` sets the audition, in seconds, to start a counter on arrival of the first packet and thereafter include only that period in charging in which one or more packets arrived. For the period where no packets arrived or no traffic was detected, usage will not be computed.  
`ctp_time` must be an integer from 1 through 4294967295. |
parking-meter seconds

Specifies the Parking Meter (PM) period, in seconds. seconds must be an integer from 1 through 4294967295. Parking meter is the method with which the usage time is set in the content-id containers in eG-CDRs. When a parking meter value is set, the user is charged for time in increments of the value set. For example, if the parking meter is set to 300 seconds (5 minutes) and the subscriber only uses one minute, the charge is for 5 minutes.

Usage

Use this command to set the various time charging algorithms/schemes for time usage in eG-CDR. For example, packets arrive at times T1, T2, T3 and T4. Then the typical time usage might be computed to be T4 – T1. However, if say there is an idle period between times T2 and T3, then system will compute the time usage to be (T2 – T1) + (T4 – T3). consumed-time in above scenario calculates the time duration as (T2 – T1) + (T4 – T3) where consumed-time with plus-idle calculates the time duration as (T2-T1)+I + (T4 – T3)+I or (T4-T1).

Example

The following command sets consumed time duration to 400 seconds:

    egcdr time-duration algorithm consumed-time 400
end

Exits the current configuration mode and returns to the Exec mode.

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Use this command to return to the parent configuration mode.
extract-host-from-uri

This command allows you to configure whether to use the host name embedded in the URI as the host field, when the host field option in the HTTP or Wireless Session Protocol (WSP) header is absent.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Rulebase Configuration

active-charging service service_name > rulebase rulebase_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-rule-base)#

Syntax

extract-host-from-uri { http | wsp } +
{ default | no } extract-host-from-uri

- default
  Configures this command with its default setting.
  Default: Disabled; same as no extract-host-from-uri

- no
  If previously configured, disables the extract-host-from-uri configuration, for both HTTP and WSP, from the current rulebase.

- http | wsp
  Specifies the protocol(s).

+ Indicates that more than one of the previous keywords can be entered within a single command.

Usage

If the host field is not present in HTTP/WSP header, this command will extract host from the URI, and store it in the host field to enable “http host” and “wsp host” rule matches using the stored value.

Important: Applying the extract-host-from-uri command a second time will overwrite the previous configuration. For example, if you apply the command extract-host-from-uri http wsp http, and then apply the command extract-host-from-uri wsp, extraction of host from URI will happen only for WSP analyzer.

Example
The following command configures extraction of host from URI for both HTTP and WSP protocols:

```
extract-host-from-uri http wsp
```
firewall dos-protection

This command allows you to configure Stateful Firewall protection for subscribers from Denial-of-Service (DoS) attacks.

**Important:** In StarOS 8.0, this command is available in the ACS Configuration Mode. In StarOS 8.1 and StarOS 8.3, use this command for Rulebase-based Firewall-and-NAT configuration. In StarOS 8.1 and StarOS 9.0 and later releases, for Policy-based Firewall-and-NAT configuration, this command is available in the Firewall-and-NAT Policy Configuration Mode.

**Product**
PSF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Rulebase Configuration

```
active-charging service service_name > rulebase rulebase_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

**Syntax**

```
[ no ] firewall dos-protection { all | flooding { icmp | tcp-syn | udp } | ftp-bounce | ip-unaligned-timestamp | mime-flood | port-scan | tcp-window-containment | source-router | teardrop | winnuke }
```

**default firewall dos-protection**

```
no
```

If previously enabled, disables Stateful Firewall protection for subscribers from all or specified DoS attack(s).

```
default
```

Configures this command with its default setting.
Default: Protection from all DOS attacks is disabled.

```
all
```

Enables protection against all DoS attacks supported by the Stateful Firewall in-line service.

```
flooding { icmp | tcp-syn | udp }
```

Enables protection against specified flooding attacks:

- `icmp`: Enables protection against ICMP Flood attacks
- `tcp-syn`: Enables protection against TCP SYN Flood attacks
- `udp`: Enables protection against UDP Flood attacks
ftp-bounce
Enables protection against FTP Bounce attacks.
In an FTP Bounce attack, an attacker is able to use the PORT command to request access to ports indirectly through a user system as an agent for the request. This technique is used to port scan hosts discreetly, and to access specific ports that the attacker cannot access through a direct connection.

ip-unaligned-timestamp
Enables protection against IP Unaligned Timestamp attacks.
In an IP Unaligned Timestamp attack, certain operating systems crash if they receive a frame with the IP timestamp option that is not aligned on a 32-bit boundary.

mime-flood
Enables protection against HTTP Multiple Internet Mail Extension (MIME) Header Flooding attacks.
In a MIME Flood attack an attacker sends huge amount of MIME headers which consumes a lot of memory and CPU usage.

port-scan
Enables protection against Port Scan attacks.

tcp-window-containment
Enables protection against TCP Sequence Number Out-of-Range attacks.
In a Sequence Number Out-of-Range attack the attacker sends packets with out-of-range sequence numbers forcing the system to wait for missing sequence packets.

source-router
Enables protection against IP Source Route IP Option attacks.
Source routing is an IP option mainly used by network administrators to check connectivity. When an IP packet leaves a system, its path through various networks to its destination is controlled by the routers and their current configuration. Source routing provides a means to override the control of the routers. Strict source routing specifies the path through all the routers to the destination. The same path in reverse is used to return responses. Loose source routing allows the attacker to spoof both an address and sets the loose source routing option to force the response to return to the attacker's network.

teardrop
Enables protection against Teardrop attacks.
In a Teardrop attack, overlapping IP fragments are exploited causing the TCP/IP fragmentation re-assembly to improperly handle overlapping IP fragments.

winnuke
Enables protection against WIN-NUKE attacks.
This is a type of Nuke denial-of-service attack against networks consisting of fragmented or otherwise invalid ICMP packets sent to the target, achieved by using a modified ping utility to repeatedly send this corrupt data, thus slowing down the affected computer until it comes to a complete stop.
The WinNuke exploits the vulnerability in the NetBIOS handler and a string of out-of-band data sent to TCP port 139 of the victim machine causing it to lock up and display a Blue Screen of Death.
Usage

Use this command to enable Stateful Firewall protection from different types of DoS attacks. This command can be used multiple times for different DoS attacks.

Important: The DoS attacks are detected only in the downlink direction.

Example

The following command enables Stateful Firewall protection from all supported DoS attacks:

```
firewall dos-protection all
```
firewall flooding

This command allows you to configure Stateful Firewall protection from Packet Flooding attacks.

Important: In StarOS 8.0, this command is available in the ACS Configuration Mode. In StarOS 8.1 and StarOS 8.3, use this command for Rulebase-based Firewall-and-NAT configuration. In StarOS 8.1 and StarOS 9.0 and later releases, for Policy-based Firewall-and-NAT configuration, this command is available in the Firewall-and-NAT Policy Configuration Mode.

Product
PSF

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Rulebase Configuration

active-charging service service_name > rulebase rulebase_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-rule-base)#

Syntax

```
firewall flooding { { protocol { icmp | tcp-syn | udp } packet limit packets } | { sampling-interval interval } } |

default firewall flooding { { protocol { icmp | tcp-syn | udp } packet limit } | { sampling-interval } } }
```

default

Configures this command the default setting for the specified keyword.

```
protocol { icmp | tcp-syn | udp }
```

Specifies the transport protocol:
- \*icmp: Configuration for ICMP protocol.
- \*tcp-syn: Configuration for TCP-SYN packet limit.
- \*udp: Configuration for UDP protocol.

```
packet limit packets
```

Specifies the maximum number of specified packets a subscriber can receive during a sampling interval. `packets` must be an integer from 1 through 4294967295.

Default: 1000 packets per sampling interval for all protocols.

```
sampling-interval interval
```

Specifies the flooding sampling interval, in seconds. `interval` must be an integer from 1 through 60.

Default: 1 second
Usage

Use this command to configure the maximum number of ICMP, TCP-SYN, / UDP packets allowed to prevent the packet flooding attacks to the host.

Example

The following command ensures a subscriber will not receive more that 1000 ICMP packets per sampling interval:

```
firewall flooding protocol icmp packet limit 1000
```

The following command ensures a subscriber will not receive more than 1000 UDP packets per sampling interval on different 5-tuples. That is, if an attacker is sending lot of UDP packets on different ports or using different spoofed IPs, those packets will be limited to 1000 packets per sampling interval. This way only “suspected” malicious packets are limited and not “legitimate” packets:

```
firewall flooding protocol udp packet limit 1000
```

The following command ensures a subscriber will not receive more than 1000 TCP-SYN packets per sampling interval:

```
firewall flooding protocol tcp-syn packet limit 1000
```

The following command specifies a flooding sampling interval of 1 second:

```
firewall flooding sampling-interval 1
```
**firewall icmp-destination-unreachable-message-threshold**

This command allows you to configure a threshold on the number of ICMP error messages sent by the subscriber for a particular data flow.

---

**Important:** In StarOS 8.0, this command is available in the ACS Configuration Mode. In StarOS 8.1 and StarOS 8.3, use this command for Rulebase-based Firewall-and-NAT configuration. In StarOS 8.1 and StarOS 9.0 and later releases, for Policy-based Firewall-and-NAT configuration, this command is available in the Firewall-and-NAT Policy Configuration Mode.

**Product**
PSF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Rulebase Configuration

```text
active-charging service service_name > rulebase rulebase_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-rule-base) #
```

**Syntax**

```
firewall icmp-destination-unreachable-message-threshold messages then-block-server
```  

```text
{ default | no } firewall icmp-destination-unreachable-message-threshold
```

---

**default**

Configures this command with its default setting. Default: No limit

---

**no**

If previously configured, deletes the configuration from the current rulebase.

---

**messages**

Specifies the threshold on the number of ICMP error messages sent by the subscriber for a particular data flow. 

**messages** must be an integer from 1 through 100.

---

**Usage**

Use this command to configure a threshold on the number of ICMP error messages sent by the subscriber for a particular data flow. After the threshold is reached, it is assumed that the server is not reacting properly to the error messages, and further downlink traffic to the subscriber on the unwanted flow is blocked.

Some servers that run QChat ignore the ICMP error messages (Destination Port Unreachable and Host Unreachable) from the mobiles. So the mobiles continue to receive unwanted UDP traffic from the QChat servers, and their batteries get exhausted quickly.
Example

The following command configures a threshold of 10 ICMP error messages:

```
firewall icmp-destination-unreachable-message-threshold 10 then-block-server
```
firewall max-ip-packet-size

This command allows you to configure the maximum IP packet size (after IP reassembly) allowed over Stateful Firewall.

**Important:** In StarOS 8.0, this command is available in the ACS Configuration Mode. In StarOS 8.1 and StarOS 8.3, use this command for Rulebase-based Firewall-and-NAT configuration. In StarOS 8.1 and StarOS 9.0 and later releases, for Policy-based Firewall-and-NAT configuration, this command is available in the Firewall-and-NAT Policy Configuration Mode.

**Product**
PSF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Rulebase Configuration

```
active-charging service service_name > rulebase rulebase_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

**Syntax**

```
firewall max-ip-packet-size packet_size protocol { icmp | non-icmp }
```

```
default firewall max-ip-packet-size protocol { icmp | non-icmp }
```

**Example**

```
default
```

Configures the default maximum IP packet size configuration.
Default: 65535 bytes (for both ICMP and non-ICMP)

```
packet_size
```

Specifies the maximum packet size.
`packet_size` must be an integer from 30000 through 65535.

```
protocol { icmp | non-icmp }
```

Specifies the transport protocol:

- `icmp`: Configuration for ICMP protocol.
- `non-icmp`: Configuration for protocols other than ICMP.

**Usage**

Use this command to configure the maximum IP packet size allowed for ICMP and non-ICMP packets to prevent packet flooding attacks to the host. Packets exceeding the configured size will be dropped for “Jolt Attack” and “Ping-Of-Death Attack”.

---

Cisco ASR 5x00 Command Line Interface Reference
The following command allows a maximum packet size of 60000 for ICMP protocol:

```
firewall max-ip-packet-size 60000 protocol icmp
```
**firewall mime-flood**

This command allows you to configure Stateful Firewall protection from Multipurpose Internet Mail Extensions (MIME) Flood attacks.

**Important**: In StarOS 8.0, this command is available in the ACS Configuration Mode. In StarOS 8.1 and StarOS 8.3, use this command for Rulebase-based Firewall-and-NAT configuration. In StarOS 8.1 and StarOS 9.0 and later releases, for Policy-based Firewall-and-NAT configuration, this command is available in the Firewall-and-NAT Policy Configuration Mode.

**Product**  
PSF

**Privilege**  
Security Administrator, Administrator

**Mode**  
Exec > ACS Configuration > Rulebase Configuration

```
active-charging service service_name > rulebase rulebase_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

**Syntax**

```
firewall mime-flood { http-headers-limit max_limit | max-http-header-field-size max_size }

default firewall mime-flood { http-headers-limit | max-http-header-field-size }
```

**default**  
Configures this command with its default setting.

**http-headers-limit max_limit**  
Specifies the maximum number of headers allowed in an HTTP packet. If the number of HTTP headers in a page received is more than the specified limit, the request will be denied.  
`max_limit` must be an integer from 1 through 256.  
Default: 16

**max-http-header-field-size max_size**  
Specifies the maximum header field size allowed in the HTTP header, in bytes. If the size of HTTP header in the received page is more than the specified number of bytes, the request will be denied.  
`max_size` must be an integer from 1 through 8192.  
Default: 4096 bytes

**Usage**

Use this command to configure the maximum number of headers allowed in an HTTP packet, and the maximum header field size allowed in the HTTP header to prevent MIME flooding attacks.
Example

The following command sets the maximum number of headers allowed in an HTTP packet to 100:

    firewall mime-flood http-headers-limit 100

The following command sets the maximum header field size allowed in the HTTP header to 1000 bytes:

    firewall mime-flood max-http-header-field-size 1000
firewall no-ruledef-matches

This command allows you to configure the default action for packets when no Stateful Firewall ruledef matches.

**Important:** In StarOS 8.0, this command is available in the ACS Configuration Mode. In StarOS 8.1 and StarOS 8.3, use this command for Rulebase-based Firewall-and-NAT configuration. In StarOS 8.1 and StarOS 9.0 and later releases, for Policy-based Firewall-and-NAT configuration, use the `access-rule no-ruledef-matches` command available in the Firewall-and-NAT Policy Configuration Mode.

**Product**
- PSF
- NAT

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > ACS Configuration > Rulebase Configuration

```
active-charging service service_name > rulebase rulebase_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

**Syntax**

```
firewall no-ruledef-matches { downlink | uplink } action { deny [ charging-action charging_action_name ] | permit [ bypass-nat | nat-realm nat_realm_name ] }
```

```
default firewall no-ruledef-matches { downlink | uplink } action
```

<table>
<thead>
<tr>
<th>Default</th>
<th>Configures the default action for packets with no Stateful Firewall ruledef match.</th>
</tr>
</thead>
<tbody>
<tr>
<td>downlink</td>
<td>uplink</td>
</tr>
</tbody>
</table>

Specifies the packet type:
- **downlink**: Downlink (from network to subscriber) packets with no Stateful Firewall ruledef match.
  - Default: deny
- **uplink**: Uplink (from subscriber to network) packets with no Stateful Firewall ruledef match.
  - Default: permit

```
action { deny [ charging-action charging_action_name ] | permit [ bypass-nat | nat-realm nat_realm_name ] }
```

Specifies the default action for packets with no Stateful Firewall ruledef match.

```
permit [ bypass-nat | nat-realm nat_realm_name ]: Permit packets.
```

**Important:** The `bypass-nat` keyword is only available in StarOS 8.3 and later releases.
Optionally specify:
- **bypass-nat**: Specifies to bypass Network Address Translation (NAT).
- **nat-realm nat_realm_name**: Specifies a NAT realm to be used for performing NAT on subscriber packets.
  
  *nat_realm_name* must be the name of a NAT realm, and must be an alphanumeric string of 1 through 31 characters.

**Important**: If neither bypass-nat or nat-realm are configured, NAT is performed if the nat policy nat-required CLI command is configured with the default-nat-realm option.

```
deny [ charging-action charging_action_name ]: Denies specified packets. Optionally, a charging action can be specified.

charging_action_name must be the name of a charging action, and must be an alphanumeric string of 1 through 63 characters.
```

**Usage**

Use this command to configure the default action to be taken on packets with no Stateful Firewall ruledef matches.

If, for deny action, the optional charging action is configured, the action taken depends on what is configured in the charging action. For the Stateful Firewall rule, the “flow action”, “billing action”, and “content ID” of the charging action will be used to take action. If flow exists, flow statistics are updated.

Allowing/dropping of packets is determined in the following sequence:

- Check is done to see if the packet matches any pinholes. If yes, no rule matching is done and the packet is allowed.
- Stateful Firewall ruledef matching is done. If a rule matches, the packet is allowed or dropped as per the firewall priority configuration.
- If no Stateful Firewall ruledef matches, the packet is allowed or dropped as per the no-ruledef-matches configuration.

For a packet dropped due to Stateful Firewall ruledef match or no match (first packet of a flow), the charging action applied is the one configured in the firewall priority or the firewall no-ruledef-matches command respectively.

In StarOS 8.1, in the case of Policy-based Stateful Firewall, the charging action applied is the one configured in the access-rule priority or the access-rule no-ruledef-matches command respectively.

For action on packets dropped due to any error condition after data session is created, the charging action must be configured in the flow any-error charging-action command.

**Example**

The following command configures Stateful Firewall to permit downlink packets with no ruledef matches:

```
firewall no-ruledef-matches downlink action permit
```
**firewall policy**

This command allows you to enable/disable Stateful Firewall support for all subscribers using the current rulebase.

**Important:** In StarOS 8.0, this command is available in the APN/Subscriber Configuration Mode. In StarOS 8.1 and StarOS 8.3, use this command for Rulebase-based Firewall-and-NAT configuration. In StarOS 8.1 and StarOS 9.0 and later releases, for Policy-based Firewall-and-NAT configuration, this command is available in the Firewall-and-NAT Policy Configuration Mode.

**Product**
PSF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Rulebase Configuration

```
active-charging service service_name > rulebase rulebase_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

**Syntax**

```
firewall policy firewall-required
{ default | no } firewall policy
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Configures this command with its default setting. Default: Stateful Firewall support is disabled for all subscribers using the current rulebase.</td>
</tr>
<tr>
<td>no</td>
<td>If previously enabled, disables Stateful Firewall support for all subscribers using the current rulebase.</td>
</tr>
</tbody>
</table>

**Usage**

Use this command to enable/disable Stateful Firewall support for all subscribers using the current rulebase.

**Example**

The following command enables Stateful Firewall support:

```
firewall policy firewall-required
```

The following command disables Stateful Firewall support:

```
no firewall policy
```
**firewall priority**

This command allows you to add and specify the priority and type of a Stateful Firewall ruledef in the current rulebase, and allows you to configure a single or range of ports to be allowed on the server for auxiliary/data connections.

**Important:** In StarOS 8.1 and StarOS 9.0 and later releases, for Policy-based Firewall-and-NAT configuration, use the `access-rule priority` command available in the Firewall-and-NAT Policy Configuration Mode.

**Product**
- PSF
- NAT

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > ACS Configuration > Rulebase Configuration
- `active-charging service service_name > rulebase rulebase_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

**Syntax**

```
firewall priority priority [ dynamic-only | static-and-dynamic ] firewall-ruledef
firewall_ruledef_name { { deny [ charging-action charging_action_name ] } | { permit [ natrealm nat_realm_name | { trigger open-port { aux_port_number | range start_port_number to end_port_number } direction { both | reverse | same } ] } ] } }

no firewall priority priority
```

**no**

If previously configured, deletes the specified Stateful Firewall ruledef priority configuration from the current rulebase.

**priority**

Specifies the Stateful Firewall ruledef’s priority in the current rulebase.  
*priority* must be a unique value in the current rulebase, and must be an integer from 1 through 65535.

```
[ dynamic-only | static-and-dynamic ] firewall-ruledef firewall_ruledef_name
```

Specifies the Stateful Firewall ruledef to add to the rulebase. Optionally, the Stateful Firewall ruledef type can be specified.

- **dynamic-only:** Firewall Dynamic Ruledef—Predefined ruledef that can be enabled/disabled by the policy server, and is disabled by default.

- **static-and-dynamic:** Firewall Static and Dynamic Ruledef—Predefined ruledef that can be disabled/enabled by the policy server, and is enabled by default.

- **firewall_ruledef_name** must be the name of a Stateful Firewall ruledef, and must be an alphanumeric string of 1 through 63 characters.
deny [ charging-action charging_action_name ]

Denies packets if the rule is matched. An optional charging action can be specified. If a packet matches the deny rule, action is taken as configured in the charging action. For Stateful Firewall ruledefs, only the terminate-flow action is applicable, if configured in the specified charging action.  
charging_action_name must be the name of a charging action, and must be an alphanumeric string of 1 through 63 characters.

permit [ nat-realm nat_realm_name | [ bypass-nat ] [ trigger open-port { aux_port_number | range start_port_number to end_port_number } ] ]

Permits packets.

- **nat-realm nat_realm_name**: Specifies the NAT realm to be used for performing NAT on subscriber packets matching the Stateful Firewall ruledef.

  If the NAT realm is not specified, then NAT will be bypassed. That is, NAT will not be applied on subscriber packets that are matching a Stateful Firewall ruledef with no NAT realm name configured.

  nat_realm_name must be the name of a NAT realm, and must be an alphanumeric string of 1 through 31 characters.

- **bypass-nat**: Specifies that packets bypass NAT.

  Important: If the nat-realm is not configured, NAT is performed if the nat policy nat-required CLI command is configured with the default-nat-realm option.

- **trigger open-port { aux_port_number | range start_port_number to end_port_number }**: Permits packets if the rule is matched, and allows the creation of data flows for Stateful Firewall. Optionally a port trigger can be specified to be used for this rule to limit the range of auxiliary data connections (a single or range of port numbers) for protocols having control and data connections (like FTP). The trigger port will be the destination port of an association which matches a rule.

  - **aux_port_number**: Specifies the number of auxiliary ports to open for traffic, and must be an integer from 1 through 65535.

  - **range start_port_number to end_port_number**: Specifies the range of ports to open for subscriber traffic.

    - **start_port_number** must be an integer from 1 through 65535. This is the start of the port range and must be less than **end_port_number**.

    - **end_port_number** must be an integer from 1 through 65535. This is the end of the port range and must be greater than **start_port_number**.

**direction { both | reverse | same }

Specifies the direction from which the auxiliary connection is initiated. This direction can be same as the direction of control connection, or the reverse of the control connection direction, or in both directions.

- **both**: Provides the trigger to open port for traffic in either direction of the control connection.

- **reverse**: Provides the trigger to open port for traffic in the reverse direction of the control connection (from where the connection is initiated).

- **same**: Provides the trigger to open port for traffic in the same direction of the control connection (from where the connection is initiated).
Usage

Use this command to add Stateful Firewall ruledefs to the rulebase and configure the priority, type, and port triggers. Port trigger configuration is optional. Port trigger can be configured only if a rule action is permit. The rulebase specifies the Stateful Firewall rules to be applied on the calls. The ruledefs within a rulebase have priorities, based on which priority matching is done. Once a rule is matched and the rule action is permit, if the trigger is configured, the appropriate check is made. The trigger port will be the destination port of an association which matches the rule.

Multiple triggers can be defined for the same port number to permit multiple auxiliary ports for subscriber traffic.

Once a rule is matched and if the rule action is deny, the action taken depends on what is configured in the specified charging action. If the flow exists, flow statistics are updated and action is taken as configured in the charging action:

- If the billing action is configured as EDR enabled, an EDR is generated.
- If the content ID is configured, UDR information is updated.
- If the flow action is configured as “terminate-flow”, the flow is terminated instead of just discarding the packet.

If the billing action, content ID, and flow action are not configured, no action is taken on the dropped packets.

Important: For Stateful Firewall ruledefs, only the terminate-flow action is applicable if configured in the specified charging action.

For a packet dropped due to Stateful Firewall ruledef match or no match (first packet of a flow), the charging action applied is the one configured in the firewall priority or the firewall no-ruledef-matches command respectively.

In StarOS 8.1, in the case of Policy-based Firewall, the charging action applied is the one configured in the access-rule priority or the access-rule no-ruledef-matches command respectively.

For action on packets dropped due to any error condition after data session is created, the charging action must be configured in the flow any-error charging-action command.

The GGSN can dynamically activate/deactivate dynamic Stateful Firewall ruledefs for a subscriber based on the rule name received from a policy server. At rule match, if a rule in the rulebase is a dynamic rule, and if the rule is enabled for the particular subscriber, rule matching is done for the rule. If the rule is disabled for the particular subscriber, rule matching is not done for the rule.

Example

The following command assigns a priority of 10 to the Stateful Firewall ruledef fw_rule1, adds it to the rulebase, and permits port trigger to be used for the rule to open ports in the range of 100 to 200 in either direction of the control connection:

```
firewall priority 10 firewall-ruledef fw_rule1 permit trigger open-port range 100 to 200 direction both
```

The following command configures the Stateful Firewall ruledef fw_rule2 as a dynamic ruledef:

```
firewall priority 7 dynamic-only firewall-ruledef fw_rule2 deny
```
firewall tcp-first-packet-non-syn

This command allows you to configure the action to take on TCP flows starting with a non-syn packet.

**Important:** In StarOS 8.1 and StarOS 8.3, use this command for Rulebase-based Firewall-and-NAT configuration. In StarOS 8.1 and StarOS 9.0 and later releases, for Policy-based Firewall-and-NAT configuration, this command is available in the Firewall-and-NAT Policy Configuration Mode.

**Syntax**

```
firewall tcp-first-packet-non-syn { drop | reset }
```

**default firewall tcp-first-packet-non-syn**

```
drop
```

Specifies to drop the packet or session.

```
reset
```

Specifies to send reset.

**Usage**

Use this command to configure action to take on TCP flow starting with a non-syn packet.

**Example**

The following command configures action to take on TCP flow starting with a non-syn packet to drop:

```
firewall tcp-first-packet-non-syn drop
```
**firewall tcp-idle-timeout-action**

This command allows you to configure the Stateful Firewall action to be taken on TCP idle timeout expiry.

**Important:** In StarOS 8.1 and StarOS 8.3, use this command for Rulebase-based Firewall-and-NAT configuration. In StarOS 8.1 and StarOS 9.0 and later releases, for Policy-based Firewall-and-NAT configuration, this command is available in the Firewall-and-NAT Policy Configuration Mode.

**Product**
- PSF

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > ACS Configuration > Rulebase Configuration

```
active-charging service service_name > rulebase rulebase_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

**Syntax**

```
firewall tcp-idle-timeout-action { drop | reset }
```

**default firewall tcp-idle-timeout-action**

```
default
Configures this command with its default setting.
Default: reset
```

```
drop
Specifies to drop the packet or session on TCP timeout expiry.
```

```
reset
Specifies to send reset on TCP timeout expiry.
```

**Usage**

Use this command to configure action to take on TCP idle timeout expiry.

**Example**

The following command configures action to take on TCP idle timeout expiry to drop:

```
firware tcp-idle-timeout-action drop
```
firewall tcp-reset-message-threshold

This command allows you to configure a threshold on the number of TCP reset messages sent by the subscriber for a particular data flow. After this threshold is reached, further downlink traffic to the subscriber on the unwanted flow is blocked.

**Important:** This command is only available in StarOS 8.3 and later releases. In StarOS 8.3, use this command for Rulebase-based Firewall-and-NAT configuration. In StarOS 9.0 and later releases, for Policy-based Firewall-and-NAT configuration, this command is available in the Firewall-and-NAT Policy Configuration Mode.

### Syntax

```
firewall tcp-reset-message-threshold messages then-block-server

{ default | no } firewall tcp-reset-message-threshold
```

- `default` Configures this command with its default setting. Default: `no firewall tcp-reset-message-threshold`
- `no` If previously configured, deletes the firewall tcp-reset-message-threshold configuration from the current rulebase.
- `messages` Specifies the threshold on the number of TCP reset messages sent by the subscriber for a particular data flow. `messages` must be an integer from 1 through 100.

### Usage

Use this command to configure a threshold on the number of TCP reset messages sent by the subscriber for a particular data flow. After the threshold is reached, assuming the server is not reacting properly to the reset messages further downlink traffic to the subscriber on the unwanted flow is blocked. This configuration enables QCHAT noise suppression for TCP.

### Example

The following command sets the threshold on the number of TCP reset messages to 10:

```
firewall tcp-reset-message-threshold messages 10
```
firewall tcp-reset-message-threshold 10 then-block-server
firewall tcp-syn-flood-intercept

This command allows you to configure the TCP intercept parameters to prevent TCP SYN flooding attacks by intercepting and validating TCP connection requests for DoS protection mechanism configured with the dos-protection command.

**Important:** In StarOS 8.0, this command is available in the ACS Configuration Mode. In StarOS 8.1 and StarOS 8.3, use this command for Rulebase-based Firewall-and-NAT configuration. In StarOS 8.1 and StarOS 9.0 and later releases, for Policy-based Firewall-and-NAT configuration, this command is available in the Firewall-and-NAT Policy Configuration Mode.

**Product**
PSF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Rulebase Configuration

```
active-charging service service_name > rulebase rulebase_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

**Syntax**

```
firewall tcp-syn-flood-intercept { mode { none | watch [ aggressive ] } | watch-timeout intercept_watch_timeout }

default firewall tcp-syn-flood-intercept { mode | watch-timeout }
```

---

**default**

Sets the default values of TCP intercept parameters for SYN Flood DoS protection.

**mode { none | watch [ aggressive ] }**

Specifies the TCP SYN flood intercept mode:

- **none**: Disables TCP SYN flood intercept feature.
- **watch**: Configures TCP SYN flood intercept feature in watch mode. Stateful Firewall passively watches to see if TCP connections become established within a configurable interval. If connections are not established within the timeout period, Stateful Firewall clears the half-open connections by sending RST to TCP client and server. The default watch-timeout for connection establishment is 30 seconds.
- **aggressive**: Configures TCP SYN flood Intercept or Watch feature for aggressive behavior. Each new connection request causes the oldest incomplete connection to be deleted. When operating in watch mode, the watch timeout is reduced by half. If the watch-timeout is 30 seconds, under aggressive conditions it becomes 15 seconds. When operating in intercept mode, the retransmit timeout is reduced by half (i.e. if the timeout is 60 seconds, it is reduced to 30 seconds). Thus the amount of time waiting for connections to be established is reduced by half (i.e. it is reduced to 150 seconds from 300 seconds under aggressive conditions).
Default: none

watch-timeout intercept_watch_timeout

Specifies the TCP intercept watch timeout, in seconds. 
intercept_watch_timeout must be an integer from 5 through 30.
Default: 30

Usage
This TCP intercept functionality provides protection against TCP SYN Flooding attacks. 
The system captures TCP SYN requests and responds with TCP SYN-ACKs. If a connection initiator 
completes the handshake with a TCP ACK, the TCP connection request is considered as valid by system and 
system forwards the initial TCP SYN to the valid target which triggers the target to send a TCP SYN-ACK. 
Now system intercepts with TCP SYN-ACK and sends the TCP ACK to complete the TCP handshake. Any 
TCP packet received before the handshake completion will be discarded.

Example
The following command sets the TCP intercept watch timeout setting to 5 seconds:

```
firewall tcp-syn-flood-intercept watch-timeout 5
```
flow any-error

This command allows you to specify the charging action to be used for packets dropped by Stateful Firewall due to any error conditions.

Product
PSF

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Rulebase Configuration

Syntax

```
flow any-error charging-action charging_action_name

default flow any-error
```

**default**

Configures the default action for packets dropped by Stateful Firewall due to any errors.
Default: Update the flow statistics if flow is available

```
charging_action_name
```

Specifies the charging action based on which accounting action is taken on packets dropped by Stateful Firewall due to any errors.
`charging_action_name` must be the name of a charging action, and must be an alphanumeric string of 1 through 63 characters.

**Important:** The charging action specified here should preferably not be used for action on packets dropped due to Stateful Firewall ruledef match or no-match (in the `firewall priority` and `firewall no-ruledef-matches` commands) and the content ID within the charging action must be unique so that dropped counts will not interfere with other content IDs.

**Usage**

Use this command to configure the charging action for packets dropped by Stateful Firewall due to any error conditions, such as, a packet being inappropriate based on the state of the protocol of the packet's session, or DoS protection causing the packet to be discarded, and so on.

For a packet dropped due to Stateful Firewall ruledef match or no match (first packet of a flow), the charging action applied is the one configured in the `firewall priority` or the `firewall no-ruledef-matches` command respectively.

In StarOS 8.1, in the case of Policy-based Firewall, the charging action applied is the one configured in the `access-rule priority` or the `access-rule no-ruledef-matches` command respectively.
For a packet dropped due to any error condition after data session is created, the charging action used is the one configured in the `flow any-error charging-action` command.

If the charging action applied on a packet is the one specified in the `flow any-error charging-action` command, flow statistics are updated and action is taken as configured in the charging action:

- If the billing action is configured as EDR enabled, an Event Data Record (EDR) is generated.
- If the content ID is configured, Usage Data Record (UDR) information is updated.
- If the flow action is configured as “terminate-flow”, the flow is terminated instead of just discarding the packet.

If the billing action, content ID, and flow action are not configured, no action is taken on the dropped packets.

Example

The following command specifies the charging action `test2` for accounting action on packets dropped/discarded by Stateful Firewall due to any error:

```
flow any-error charging-action test2
```
**flow control-handshaking**

This command allows you to specify how to charge for the control traffic associated with an application.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Rulebase Configuration

`active-charging service service_name > rulebase rulebase_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

**Syntax**

```
flow control-handshaking { charge-to-application { [ all-packets ] [ initial-packets ] [ mid-session-packets ] [ tear-down-packets ] } | charge-separate-from-application }

default flow control-handshaking

no flow control-handshaking [ charge-to-application ]
```

**default flow control-handshaking**

Configures this command with its default setting.
Default: Same as `no flow control-handshaking`

**no flow control-handshaking [ charge-to-application ]**

If previously configured, deletes the flow control-handshaking configuration from the current rulebase. The control packets will use whatever content-id is determined by the normal use of the `action` commands. In this command, the optional keyword `charge-to-application` is deprecated and has no effect.

**charge-to-application { [ all-packets ] [ initial-packets ] [ mid-session-packets ] [ tear-down-packets ] }**

Configures the charging action to include the flow control packets either during initial handshaking only or specified control packets during session for charging.

- **all-packets**: Specifies that the initial setup packets will wait until the application has been determined before assigning the content-id, and all mid-session ACK packets as well as the final tear-down packets will use that content-id.

- **initial-packets**: Specifies that only the initial setup packets will wait for content-id assignment.

- **mid-session-packets**: Specifies that the ACK packets after the initial setup will use the application's or content-id assignment.

- **tear-down-packets**: Specifies that the final tear-down packets (TCP or WAP) will use the application's or content-id assignment.
charge-separate-from-application

Configures the charging action to separate the charging of the initial control packets or all subsequent control packets from regular charging.

Usage

Use this command to configure how to charge for the control traffic associated with an application ruledef. Applications like HTTP use TCP to set up and tear down connections before the HTTP application starts. This command controls whether the packets that set up and tear down the connections should use the same content ID as the application's flow.

In normal mode 3-way handshake TCP packets (SYN, SYN-ACK, and ACK) and closing or intermittent packets (FIN, RST, etc.) directed and charged based on configured matched rules. This command makes the system to wait for the start and stop of layer 7 packet flow and content ID and charge the initial, intermittent, and closing TCP packets as configured to the same matching rules and content ID as of the flow.

This command also affects applications that do not use TCP but use other methods for control packets, for example WAP, where WTP/UDP may be used to set up and tear down connection-oriented WSP.

Example

Following command enables the charging for initial TCP handshaking control packets and wait for content-id of data traffic flow:

```
flow control-handshaking charge-to-application initial-packets
```

The following command enables charging all mid-session ACKs as well as tear-down packets to application:

```
flow control-handshaking charge-to-application mid-session-packets tear-down-packets
```
flow end-condition

This command allows you to configure the end condition of the session flows related to a user session and triggers EDR generation.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Rulebase Configuration

`active-charging service service_name > rulebase rulebase_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

**Syntax**

In StarOS 12.2 and later releases:

```
flow end-condition { content-filtering | hagr | handoff | normal-end-signaling | session-end | url-blacklisting | timeout } [ flow-overflow ] + { charging-edr charging_edr_format_name | reporting-edr reporting_edr_format_name }
```

```
no flow end-condition
```

In StarOS 12.1 and earlier releases:

```
flow end-condition { { content-filtering | normal-end-signaling | timeout + } | { hagr | handoff | session-end } [ flow-overflow ] + } [ url-blacklisting ] } edr edr_format_name
```

```
no flow end-condition
```

**no**
If previously configured, deletes the flow end-condition configuration from the current rulebase.

**content-filtering**
Creates an EDR with the specified EDR format whenever a flow ends due to Category-based Content Filtering in-line service action. Possible actions include redirect-url, terminate-flow, content-insert.

**hagr**
Creates an EDR with the specified EDR format whenever a flow is terminated due to Inter-chassis Session Recovery action.

**handoff**
Creates an EDR with the specified EDR format whenever a flow ends due to hand-off. Whenever a handoff occurs, ACS closes the EDRs for all current flows using the specified EDR format, and begins new statistics collection for the flows for the EDRs that will be generated when the flows actually end.
normal-end-signaling
Creates an EDR with the specified EDR format whenever flow end is signaled normally, for example like detecting FIN and ACK for a TCP flow, or a WSP-DISCONNECT terminating a connection-oriented WSP flow over UDP) and create an EDR for the flow using the specified EDR format.

session-end
Creates an EDR with the specified EDR format whenever a subscriber session ends. By this option ACS creates an EDR with the specified format name for every flow that has had any activity since last EDR was created for the flow on session end.

url-blacklisting
Creates an EDR with the specified EDR format whenever flow ends due to URL Blacklisting action.

timeout
Creates an EDR with the specified EDR format whenever a flow ends due to a timeout condition.

flow-overflow

**Important:** This keyword is only available in StarOS 8.3 and later releases. And, is only applicable when used with the `hagr`, `handoff`, and `session-end` keywords.

Important: This keyword is only available in StarOS 8.3 and later releases. And, is only applicable when used with the `hagr`, `handoff`, and `session-end` keywords.

Creates an EDR with the specified EDR format whenever there is a flow-overflow condition. If any of the specified end-conditions that affect subscriber information stored at ACS (such as call line) is configured, the “flow-overflow” EDR is generated.

+ Indicates that more than one of the keywords can be entered within a single command.

edr edr_format_name

**Important:** This option is available only in the 12.1 and earlier releases. In 12.2 and later releases, this option is deprecated and is replaced by the `charging-edr` option.

Specifies the EDR format to record EDR for specified flow end condition.
`edr_format_name` must be the name of an EDR format, and must be a unique alphanumeric string of 1 through 63 characters.

charging-edr charging_edr_format_name

**Important:** This option is available only in 12.2 and later releases.

Specifies the charging EDR format.
`charging_edr_format_name` must be the name of a charging EDR format, and must be an alphanumeric string of 1 through 63 characters.
**flow end-condition**

```
reporting-edr  reporting_edr_format_name
```

**Important:** This option is available only in 12.2 and later releases.

Specifications the reporting EDR format.

*reporting_edr_format_name* must be the name of a reporting EDR format, and must be a unique alphanumeric string of 1 through 63 characters.

**Usage**

Use this command to enable or disable the capturing of EDRs based on flow end condition.

**Example**

In 12.1 and earlier releases, the following command configures the flow end condition as “handoff” and creates a charging EDR with format named *EDR_format1*:

```
flow end-condition handoff edr-format EDR_format1
```

In 12.2 and later releases, the following command configures the flow end condition as *handoff* and creates a charging EDR with format named *EDR_format1*:

```
flow end-condition handoff charging-edr EDR_format1
```
flow limit-across-applications

This command allows you to limit the total number of simultaneous flows per Subscriber/APN sent to a rulebase regardless of the flow type, or limit flows based on the protocol type under the Session Control feature.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Rulebase Configuration

active-charging service service_name > rulebase rulebase_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-rule-base)#

Syntax

flow limit-across-applications { limit | non-tcp limit | tcp limit }

no flow limit-across-applications [ non-tcp | tcp ]

no
If previously configured, deletes the flow limit-across-applications configuration from the current rulebase.

flow limit-across-applications limit
Specifies the maximum number of flows across all applications for the rulebase.
limit must be an integer from 1 through 4000000000.
Default: No limits

non-tcp limit
Specifies the maximum limit of non-TCP type flows.
limit must be an integer from 1 through 4000000000.
Default: No limits

tcp limit
Specifies the maximum limit of TCP flows.
limit must be an integer from 1 through 4000000000.
Default: No limits

Usage
Use this command to limit the total number of flows allowed for a rulebase regardless of flow type, or limit flows based on the protocol—non-TCP (connection-less) or TCP (connection-oriented).
If a subscriber attempts to exceed these limits system discards the packets of new flow. This limit processing of this command has following aspects for UDP, TCP, ICMP and some of the exempted flows:
• UDP/ICMP: System waits for the flow timeout before updating the counter and removing it from the count of number of flows.
• TCP: After a TCP flow ends, system waits for a short period of time to accommodate the retransmission of any missed packet from one end. TCP flows those are ended, but are still in wait period for timeout are exempted for this limit processing.

• Exempted flows: System exempts all the other flows specified with the flow limit-for-flow-type command in the ACS Charging Action Configuration Mode set to no.

Example

The following command defines the maximum number of 200000 flows for the rulebase:

```
flow limit-across-applications 200000
```
flow rtsp-all-pkts

This command allows you to delay charge packets in an RTSP flow.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Rulebase Configuration

active-charging service service_name > rulebase rulebase_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-rule-base)#

Syntax

[ no | default ] flow rtsp-all-pkts charge-to-application

no
If previously configured, deletes the flow rtsp-all-pkts configuration from the current rulebase.

default
Configures this command with its default setting.
Default: Same as no flow rtsp-all-pkts charge-to-application.

flow rtsp-all-pkts charge-to-application

Configures delay charging for RTSP traffic. When this configuration is enabled, all packets (TCP control packets and RTSP packets) prior to the first SETUP will be charged to application as per the application ruledef. In other words, they will be charged to the content-id established by the first SETUP of the RTSP flow.

Usage

Use this command to delay charge packets in a RTSP flow. All initial packets (TCP control packets (all packets including initial, mid-session, end-session) and RTSP packets prior to the first SETUP) can be delay charged. Apart from the initial packets, all intermittent TCP control packets are also charged to the last matched Ruledef for the given RTSP flow. This command is used in conjunction with the rtsp initial-bytes-limit RTSP_bytes command.

The following command enables the RTSP flow’s delay charging:

flow rtsp-all-pkts charge-to-application
fw-and-nat default-policy

This command allows you to configure the default Firewall-and-NAT policy for the current rulebase. This command must be used to configure the Policy-based Firewall-and-NAT feature.

**Important:** This command is only available in StarOS 8.1 and StarOS 9.0 and later releases.

**Product**
PSF
NAT

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Rulebase Configuration

```
active-charging service service_name > rulebase rulebase_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

**Syntax**

```
fw-and-nat default-policy fw_nat_policy_name

no fw-and-nat default-policy
```

- **no**
  If previously configured, deletes the Firewall-and-NAT default policy configuration from the current rulebase.

- **fw_nat_policy_name**
  Specifies the default Firewall-and-NAT policy for the current rulebase. `fw_nat_policy_name` must be the name of a Firewall-and-NAT policy, and must be an alphanumeric string of 1 through 63 characters.

**Usage**

Use this command to configure the default Firewall-and-NAT policy for a rulebase.
For subscribers using the current rulebase, the default Firewall-and-NAT policy will be used if in the APN/subscriber profile the `default fw-and-nat policy` command is configured, and a policy to use is not received from the AAA/OCS.
For more information, see the *Personal Stateful Firewall Administration Guide*.

**Example**

The following command configures a Firewall-and-NAT policy named `standard` to the rulebase:

```
fw-and-nat default-policy standard
```
http header-parse-limit

This command allows you to configure the HTTP header parse limit, on exceeding which the flow is marked as permanent failure and is matched and charged against http error = TRUE ruledef.

⚠️ Important: This command is customer specific. For more information contact your Cisco account representative.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Rulebase Configuration

active-charging service service_name > rulebase rulebase_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-rule-base)#

Syntax

http header-parse-limit parse_limit_bytes

{ default | no } http header-parse-limit

default
Configures the default setting for this command.
Default: 12000 bytes

no
If enabled, disables the header-parse-limit configuration in the current rulebase.

⚠️ Important: Disabling header parse limit may lead to uncharged bytes (due to no rule-matching until header is complete) if header is not correctly terminated.

parse_limit_bytes
Specifies the header-parse-limit, number of bytes.
parse_limit_bytes must be an integer from 1 through 256000.

Usage
If a user sends HTTP LF terminated traffic instead of the usual HTTP CRLF terminated traffic, and similarly the server is responding with LF terminated traffic, the traffic does not result in any rule match, and rule match happens only at flow idle or at call clear when the quota for the same is not requested/updated. This results in a revenue hole for prepaid subscribers.
For operators who have Stateful Firewall in-line service enabled, and are okay if packets are dropped, a workaround is to configure the `firewall mime-flood` command in the ACS Configuration Mode, which enables to configure the maximum number of headers allowed in an HTTP packet and the maximum header field size allowed in the HTTP header (in bytes). However, a limitation of this workaround is that Stateful Firewall supports MIME flood detection only in the downlink direction.

The support for LF termination has been added in StarOS 14.0 and later releases. For this release, with the help of configurable maximum header length support, HTTP analyzer would be allowing such LF terminated HTTP request/responses to pass through without rule matching only until the configured maximum header length is reached. When this threshold is reached, immediately the analyzer marks such HTTP session as failure and rule match would occur for `http error = TRUE` for the current packet as well as for all the previous packets that passed through unmatched. At this point, the quota for all such packets will be requested and reported.

**Example**

The following command sets the HTTP header parse limit to 10000 bytes:

```
http header-parse-limit 10000
```
ip reassembly-timeout

This command allows you to configure how long to hold onto IP fragments for reassembly, while waiting for the complete packet to arrive.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Rulebase Configuration
active-charging service service_name > rulebase rulebase_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-rule-base)#

Syntax

ip reassembly-timeout timeout_duration

default ip reassembly-timeout

default
 Configures the default setting for this command.
Default: 5000 milliseconds

timeout_duration
 Specifies the timeout duration, in milliseconds, to hold fragmented packets before reassembly.
timeout_duration must be an integer from 100 through 30000.

Usage
Use this command to configure duration for timeout timer to hold IP fragmented packets before reassembly is needed.
IP fragmented packet are retained, until either all fragmented packets have been received or the configured timeout has expired for the oldest fragment. If all fragments have been received, a temporary complete packet is reconstructed for analysis. Then all fragments are forwarded in order from first to last. If all fragments are not received, the fragments will be forwarded without being passed through the protocol analyzers, except for the IP analyzer.

Example
The following command sets the timeout timer to 15000 milliseconds:

ip reassembly-timeout 15000
ip reset-tos

This command allows you to reset the IP Type of Service (ToS) value of incoming packets to the default QCI value, before proceeding with the rest of ACS processing.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Rulebase Configuration
active-charging service service_name > rulebase rulebase_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-rule-base)#

Syntax

[ default | no ] ip reset-tos

default

Configures this command with its default setting.
Default: Disabled

no

If previously configured, deletes the IP reset-tos configuration from the current rulebase.

Usage

Use this command to reset the ToS field of any packet after it reaches ACS, or to broaden the range of values that are used in the ToS field in the IP header of any packet.
nat binding-record

This command allows you to configure NAT Binding Record (NBR) generation.

**Important:** This command is only available in StarOS 8.3. In StarOS 9.0 and later releases this command is available in the Firewall-and-NAT Policy Configuration Mode.

<table>
<thead>
<tr>
<th>Product</th>
<th>NAT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privilege</td>
<td>Security Administrator, Administrator</td>
</tr>
<tr>
<td>Mode</td>
<td>Exec &gt; ACS Configuration &gt; Rulebase Configuration</td>
</tr>
</tbody>
</table>

active-charging service service_name > rulebase rulebase_name

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

**Syntax**

```plaintext
nat binding-record edr-format edr_format_name [ port-chunk-allocation ] [ port-chunk-release ] +

{ default | no } nat binding-record
```

- **default**
  - Configures this command with its default setting.
  - Default: `port-chunk-release`

- **no**
  - If previously configured, deletes the configuration from the current rulebase.

- **edr-format edr_format_name**
  - Specifies the EDR format.
  - `edr_format_name` must be the name of an EDR format, and must be an alphanumeric string of 1 through 63 characters.

- **port-chunk-allocation**
  - Specifies generating NBR when a port chunk is allocated.

- **port-chunk-release**
  - Specifies generating NBR when a port chunk is released.
Indicates that more than one of the previous keywords can be entered within a single command.

**Usage**

Use this command to configure NBR generation.

**Example**

The following command configures an EDR format named `test123` and specifies generating NBR when a port chunk is allocated, and when a port chunk is released:

```
  nat binding-record edr-format test123 port-chunk-allocation port-chunk-release
```
## nat policy

This command allows you to enable/disable Network Address Translation (NAT) processing for all subscribers using the current rulebase.

**Important:** In StarOS 8.1 and StarOS 9.0 and later releases, for Policy-based Firewall-and-NAT, this command is available in the Firewall-and-NAT Policy Configuration Mode.

**Important:** Before enabling NAT processing for a subscriber, Stateful Firewall must be enabled for the subscriber. See the `firewall policy` CLI command.

### Product
NAT

### Privilege
Security Administrator, Administrator

### Mode
Exec > ACS Configuration > Rulebase Configuration

`active-charging service service_name > rulebase rulebase_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

### Syntax

```
nat policy nat-required [ default-nat-realm nat_realm_name ]

{ default | no } nat policy
```

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>default</code></td>
<td>Configures this command with its default setting. Default: NAT processing is disabled for all subscribers using the current rulebase.</td>
</tr>
<tr>
<td><code>no</code></td>
<td>If previously enabled, disables NAT processing for all subscribers using the current rulebase.</td>
</tr>
</tbody>
</table>

**Important:** This keyword is only available in StarOS 8.3 and later releases.

### Syntax

```
nat policy nat-required
```

Enables NAT processing for all subscribers using the current rulebase.

```
default-nat-realm nat_realm_name
```

Specifies the default NAT realm to be used if one is not already configured. `nat_realm_name` must be the name of a NAT realm, and must be an alphanumeric string of 1 through 31 characters.
**Important:** Including the default NAT realm, a maximum of three NAT realms are supported.

**Usage**

Use this command to enable/disable NAT processing for all subscribers using the current rulebase. After NAT is enabled for a subscriber, the NAT IP address to be used is chosen from the NAT realms defined in the rule priority lines within the rulebase. See the `firewall priority` CLI command.

NAT enable/disable status in the rulebase can be changed any time, however the changed NAT status will not be applied for active calls using the rulebase. The new NAT status is only applied to new calls.

**Example**

The following command enables NAT processing:

```
nat policy nat
```

The following command disables NAT processing:

```
no nat policy
```
nat suppress-aaa-update call-termination

This command allows you to suppress sending NAT Bind Updates (NBU) to the AAA server when a call gets terminated.

Important: This command is customer-specific. For more information please contact your Cisco account representative. In release 9.0, this command is available in the Firewall-and-NAT Policy Configuration Mode.

Product
NAT

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Rulebase Configuration

active-charging service service_name > rulebase rulebase_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-rule-base)#

Syntax

nat suppress-aaa-update call-termination

default nat suppress-aaa-update

default

Configures this command with its default setting.
Default: Disabled. No suppression of AAA updates.

Usage

Use this command to suppress the sending of NAT Bind Updates (NBU) to the AAA server when the call gets terminated, as these NBUs would be cleared at the AAA after receiving the accounting-stop. This enables to minimize the number of messages between the chassis and AAA server. When not configured, NBUs are sent to the AAA server whenever a port chunk is allocated, de-allocated, or the call is cleared (PPP disconnect).

Example

The following command suppresses the sending of NBU to the AAA server when PPP disconnect happens:

nat suppress-aaa-update call-termination
p2p dynamic-flow-detection

This command allows you to enable/disable the P2P analyzer to detect peer-to-peer (P2P) applications.

Product
ADC

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Rulebase Configuration

`active-charging service service_name > rulebase rulebase_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax

```
[ default | no ] p2p dynamic-flow-detection
```

- **default**
  - Configures this command with its default setting.
  - Default: Disabled

- **no**
  - If previously enabled, disables P2P dynamic flow detection in the current rulebase.

- **p2p dynamic-flow-detection**
  - Enables dynamic P2P flow detection.

Usage

Use this command to enable dynamic-flow detection. This allows the P2P analyzer to detect the P2P applications configured for the ACS.
**pcp service**

This command allows you to configure the PCP service for the current rulebase.

**Important:** This command is customer specific. Contact your Cisco account representative for more information.

**Product**
NAT
PSF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Rulebase Configuration

```
active-charging service service_name > rulebase rulebase_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

**Syntax**

```
pcp service pcp_service_name

no pcp service
```

If previously configured, deletes the PCP service configuration from the current rulebase. This service is disabled by default.

```
no pcp_service_name
```

Specifies the PCP service name for the current rulebase.

**Usage**

Use this command to configure the PCP service for the current rulebase.

**Example**

The following command configures a PCP service named *pcp1* for the rulebase:

```
pcp service pcp1
```
post-processing dynamic

This command allows you to specify rules as dynamic post-processing rules. This allows the system to differentiate normal post-processing rules from preconfigured ones. By default, this configuration is disabled.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Rulebase Configuration

active-charging service service_name > rulebase rulebase_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-rule-base)#

Syntax

post-processing dynamic { group-of-ruledefs ruledefs_group_name | ruledef ruledef_name }
charging-action charging_action_name [ description description ]

no post-processing dynamic { group-of-ruledefs ruledefs_group_name | ruledef ruledef_name }

If previously configured, deletes the specified configuration from the current rulebase.

group-of-ruledefs ruledefs_group_name

Adds the specified group-of-ruledefs to the current rulebase.

ruledefs_group_name must be the name of a group-of-ruledefs, and must be an alphanumeric string of 1 through 63 characters.

ruledef ruledef_name

Adds the specified ruledef to the current rulebase.

ruledef_name must be the name of a ruledef, and must be an alphanumeric string of 1 through 63 characters.

charging-action charging_action_name

Specifies the charging action.

charging_action_name must be the name of a charging action, and must be an alphanumeric string of 1 through 63 characters.

description description

Specifies an optional description for this configuration.

description must be an alphanumeric string of 1 through 31 characters.
Usage

Use this command to configure specific ruledefs/group-of-ruledefs as dynamic post-processing ruledefs/group-of-ruledefs. This allows the system to differentiate normal post-processing rules from the preconfigured ones. This makes possible enabling/disabling ruledefs/groups-of-ruledefs entry from an external server.

Example

The following command specifies the ruledef named test_rule as a dynamic post-processing ruledef configured with the charging action ca13 and a description of testing:

```
post-processing dynamic ruledef test_rule charging-action ca13
description testing
```
post-processing policy

This command allows you to specify the post-processing policy to be applied on Limit-Reached packets.

Product
- GGSN
- PDSN
- P-GW
- SAEGW

Privilege
- Security Administrator, Administrator

Mode
- Exec > ACS Configuration > Rulebase Configuration

active-charging service service_name > rulebase rulebase_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-rule-base)#

Syntax

post-processing policy { always | not-for-dynamic-discard }

default post-processing policy

default

Configures this command with its default setting.
Default: not-for-dynamic-discard

always

Specifies to apply post-processing even if the Credit Control Application (CCA) decides to discard packets due to limit-reached condition. If there are post-processing priority-based rules, CCA will check for any redirection rules. Otherwise, by default, CCA will discard the packets. No other post-processing actions like forward, next-hop, or xheader-insertion will be applied on the limit-reached packets.

not-for-dynamic-discard

Specifies to apply post-processing only if CCA decides not to discard packet. Will directly discard the limit-reached context and will not apply post-processing priority based rules.

Usage

This command allows to enable post-processing priority based rules for content in blacklisted state. Whenever RADIUS/Diameter prepay server blacklists content the packets are generally discarded. To enable redirection of such content, post-processing should be enabled on the blacklisted content. With this command, RADIUS/Diameter Credit-Control application will decide whether to allow post-processing to be enabled or not for the blacklisted content.

The following is a sample configuration:
configure
active-charging service service1
ruledef http_low
http any-match = TRUE
cca quota-state = limit-reached
rule-application post-processing
#exit
ruledef httpany
http any-match = TRUE
#exit
charging-action standard1
content-id 1
cca charging credit
#exit
charging-action redirect
flow action redirect-url http://aoc.com
#exit
rulebase base1
action priority 30 ruledef httpany charging-action standard1
post-processing policy always
post-processing priority 1 ruledef http_low charging-action redirect
#exit
end

Example

The following command will enable post processing on Limit-Reached packets:

post-processing policy always
post-processing priority

This command allows you to configure the post-processing priority and action to be taken on specific ruledef in the current rulebase.

ℹ️ **Important:** This command is only available in StarOS 8.3 and later releases.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Rulebase Configuration

```bash
active-charging service service_name > rulebase rulebase_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

**Syntax**

```bash
post-processing priority priority { group-of-ruledefs ruledefs_group_name | ruledef ruledef_name } charging-action charging_action_name [ description description ]
```

```bash
no post-processing priority priority
```

- **no**
  If previously configured, deletes the specified post-processing priority configuration from the current rulebase.

```bash
priority priority
```

- **priority priority**
  Specifies priority for the ruledef/group-of-ruledefs in the current rulebase.
  `priority` must be a unique value in the current rulebase, and must be an integer from 1 through 65535.

```bash
group-of-ruledefs ruledefs_group_name
```

- **group-of-ruledefs ruledefs_group_name**
  Specifies the group-of-ruledefs.
  `ruledefs_group_name` must be the name of a group-of-ruledefs, and must be an alphanumeric string of 1 through 63 characters.

ℹ️ **Important:** The group-of-ruledefs specified must be configured for post-processing. See the `group-of-ruledefs-application` command in the ACS Group-of-Ruledefs Configuration mode.

```bash
ruledef ruledef_name
```

- **ruledef ruledef_name**
  Specifies the ruledef.
  `ruledef_name` must be the name of a ruledef, and must be an alphanumeric string of 1 through 63 characters.
**Important:** The ruledef specified must be configured for post-processing. See the `rule-application` command in the *ACS Ruledef Configuration Mode Commands* chapter.

```
charging-action charging_action_name
```

Specifies the charging action.

*charging_action_name* must be the name of a charging action, and must be an alphanumeric string of 1 through 63 characters.

```
description description
```

Specifies an optional description for this configuration.

*description* must be an alphanumeric string of 1 through 31 characters.

**Usage**

Use this command to configure the post-processing priority and action to be taken on a ruledef in the rulebase.

**Example**

The following command configures the ruledef named *test_ruledef* with a priority of 10, and the charging action named *test_ca* for post processing:

```
post-processing priority 10 ruledef test_ruledef charging-action test_ca
```
**qos-renegotiate timeout**

This command allows you to configure the timeout setting for the Quality of Service (QoS) Renegotiation feature.

---

**Important:** This command is license dependent. For more information contact your Cisco account representative.

---

**Product**

All

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > ACS Configuration > Rulebase Configuration

```active-charging service service_name > rulebase rulebase_name```

Entering the above command sequence results in the following prompt:

```[local]host_name(config-rule-base)#```

**Syntax**

```qos-renegotiate timeout timeout```

```no qos-renegotiate timeout```

---

**timeout**

If previously configured, deletes the qos-renegotiate timeout configuration from the current rulebase.

---

**timeout**

Specifies the timeout period for the QoS Renegotiation feature in the current rulebase.

`timeout` is the timeout period in seconds, and must be an integer from 0 through 4294967295. If set to 0, `timeout` is disabled.

---

**Usage**

Use this command to configure timeout setting for the QoS Renegotiation feature.

---

**Example**

The following command sets the QoS renegotiate timeout period to 1000 seconds:

```qos-renegotiate timeout 1000```
radius threshold

This command allows you to configure the interval and volume thresholds to generate interim RADIUS Charging Data Records (CDRs) and write them to CDR file for ACS postpaid billing.

Product

HA
PDSN

Privilege

Security Administrator, Administrator

Mode

Exec > ACS Configuration > Rulebase Configuration

`active-charging service service_name > rulebase rulebase_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax

```
radius threshold { interval interval | volume total volume }
{ default | no } radius threshold { interval | volume total }
```

- **no**
  If previously configured, deletes the RADIUS threshold configuration from the current rulebase.

- **default**
  Configures this command with the default settings.
  Default: Disabled

- **interval interval**
  Specifies the time interval, in seconds, for generating RADIUS interim accounting requests.
  `interval` must be an integer from 60 through 40000000.
  Default: Disabled

- **volume total volume**
  Specifies the limit for the total number of octets (uplink+downlink) after which a stop-start pair will be sent to RADIUS.
  `volume` must be an integer from 100000 through 4000000000.
  Default: Disabled

Usage

Use this command to specify a time interval threshold to generate interim RADIUS CDRs and write it to RADIUS CDR file for postpaid billing.

Example

The following command configures a time threshold interval of 600 seconds for RADIUS CDRs:
radius threshold interval 600
**ran bandwidth optimize**

This command is used to enable optimized calculation of [MBR, GBR] when a subscriber (voice) call is put on hold in case of VoLTE.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > ACS Configuration > Rulebase Configuration

`active-charging service service_name > rulebase rulebase_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

**Syntax**

```
[ default | no ] ran-bandwidth optimize
```

`no`

If previously configured, disables the optimization feature for calculating [MBR, GBR] values based on Flow-Status AVP value.

**Usage**

Use this command to enable optimized calculation of [MBR, GBR] values when a subscriber (voice) call is put on hold in case of VoLTE.

When the rule is installed and active, the system uses the GBR/MBR assigned in the rule for calculating the GBR/MBR values towards the bearers created. When more than one rule is installed, P-GW adds the GBR/MBR values from all the active and installed rules even if the flow of a certain rule is marked as disabled. This current behavior is in accordance with 3GPP TS standard specification 29.212, and this might result in RAN bandwidth wastage. To avoid this wastage, some optimization is done while calculating MBR and GBR for GBR bearer.

This optimization feature provides the ability to configure a list of APNs, for which the optimized calculation of MBR, GBR can be enabled. By default, this optimized calculation should be enabled only for the IMS APN.

This feature further helps optimize the logic of aggregating MBR and GBR values, based on “Flow-Status” AVP value received in the rule definition through RAR.

During session setup, when a CCA-I is received, and if `ran bandwidth optimize` is configured for the associated rulebase, the system will aggregate [MBR, GBR] of only the rules which have flow-status='ENABLED'. This information will subsequently be sent to UE.

**Important:** The last used [MBR, GBR] for GBR bearer needs to be recovered in the event of a session manager or chassis switchover. Failure to do so can result in miscalculation of [MBR, GBR] after recovery.
By default, this CLI will be disabled. Any change in this configuration will not affect existing calls on the system. Optimized bandwidth calculation will be done only for the new calls established after enabling this CLI command.
route priority

This command allows you to configure the routing of packets to protocol analyzers.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Rulebase Configuration
active-charging service service_name > rulebase rulebase_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-rule-base)#

Syntax


no route priority route_priority

If previously configured, deletes the specified route priority configuration from the current rulebase.

route priority route_priority

Specifies the route priority for the specified ruledef in the current rulebase.
route_priority must be an integer from 1 through 65535.
Lower numbered priorities are examined first. Up to 1024 instances can be configured across all rulebases.

ruledef ruledef_name

Specifies the ruledef to evaluate packets to determine analyzer.
ruledef_name specifies the name of the ruledef configured for the route application using the rule-
application command in the ACS Ruledef Configuration Mode.
ruledef_name must be the name of a ruledef, and must be an alphanumeric string of 1 through 63
characters.

Analyzer

Specifies the analyzer for the ruledef, and must be one of the following:
• dns: Route to DNS protocol analyzer.
• file-transfer: Route to file analyzer.
• ftp-control: Route to FTP control protocol analyzer.
• ftp-data: Route to FTP data protocol analyzer.
**route priority**

- **h323**: Route to H323 protocol analyzer.
- **http**: Route to HTTP protocol analyzer.
- **imap**: Route to IMAP protocol analyzer.
- **mms**: Route to MMS protocol analyzer.
- **pop3**: Route to POP3 protocol analyzer.
- **pptp**: Route to PPTP protocol analyzer.
- **radius**: Route to RADIUS protocol analyzer.
- **rtcp**: Route to RTCP protocol analyzer.
- **rtp**: Route to RTP protocol analyzer.
- **rtsp**: Route to RTSP protocol analyzer.
- **sdp**: Route to SDP protocol analyzer.
- **secure-http**: Route to secure HTTP protocol analyzer.
- **sip [ advanced | basic-and-advanced ]**: Route to SIP protocol analyzer.
  - **advanced**: For SIP calls to work with NAT/Stateful Firewall, a SIP Application-Level Gateway (ALG) is required to do payload translation of SIP packets and pin-hole (dynamic flow) creation for media packets. A SIP routing rule must be configured for routing the packets to the SIP ALG for processing. If the keyword advanced is configured, the packets matching the routing rule will be routed to SIP ALG for processing and not to ACS SIP analyzer. If not configured, then packets will not be routed to SIP ALG and will be routed to ACS SIP analyzer for processing.
  - Also, see **firewall nat-alg** CLI command in the ACS Configuration Mode.
  - **basic-and-advanced**: For SIP ALG to co-exist with SIP Analyzer, the packets are routed through ACS SIP Analyzer and SIP ALG. The SIP packets can pass through ACS functionality (by ACS SIP Analyzer processing) and at the same time payload translation/pinhole-creation can happen successfully (by SIP ALG processing). If basic-and-advanced is configured, then the packets matching the routing rule will be routed through the SIP Analyzer and then through SIP ALG for processing.

- **tftp**: Route to TFTP protocol analyzer.
- **smtp**: Route to SMTP protocol analyzer.
- **wsp-connection-less**: Route to WSP connection-less protocol analyzer.
- **wsp-connection-oriented**: Route to WSP connection-oriented protocol analyzer.

**Important**: To route packets to the P2P analyzer, the ruledef should have rules to match all IP packets. Otherwise, the analyzer may not detect all P2P traffic.

**Important**: Use the **show active-charging analyzer statistics** command in the Exec Mode to see the list of supported analyzers.

**description**

Enables to add a description to the rule and action for later reference in saved configuration file. **description** must be an alphanumeric string of 1 through 63 characters.
Usage

Instances of this CLI command control which packets are routed to which protocol analyzers. Packets sent to ACS are always passed through the IP protocol analyzer. This CLI command controls which higher layer analyzers are also invoked.

<table>
<thead>
<tr>
<th>Analyzer</th>
<th>Common ways to route to the analyzer</th>
</tr>
</thead>
<tbody>
<tr>
<td>dns</td>
<td>UDP destination port or source port is DNS (53).</td>
</tr>
<tr>
<td>file-transfer</td>
<td>FTP and the command name is retr or stor; or, HTTP and the request method is get or post.</td>
</tr>
<tr>
<td>ftp</td>
<td>TCP destination port or source port is FTP control (21) or FTP data (20); or, ftp analyzer (for FTP control packets) dynamically detected an FTP data flow over TCP (tcp dynamic-flow = ftp-data).</td>
</tr>
<tr>
<td>http</td>
<td>TCP destination port or source port is HTTP (80).</td>
</tr>
<tr>
<td>icmp</td>
<td>All IPv4 packets with IP protocol = ICMP (1) are automatically routed here.</td>
</tr>
<tr>
<td>imap</td>
<td>TCP destination port or source port is IMAP (143).</td>
</tr>
<tr>
<td>ip</td>
<td>All IPv4 packets are automatically routed here.</td>
</tr>
<tr>
<td>mms</td>
<td>WSP content type is application/vnd.wap.mms-message; or, WSP uri contains “mms”; or, HTTP content type is application/vnd.wap.mms-message; or, HTTP uri contains “mms”.</td>
</tr>
<tr>
<td>p2p</td>
<td>Use the p2p dynamic-flow-detection CLI command to enable detection of the different P2P applications specified by the p2p application CLI command; that will cause every TCP or UDP packet to be automatically routed here</td>
</tr>
<tr>
<td>pop3</td>
<td>TCP destination port or source port is POP3 (110).</td>
</tr>
<tr>
<td>radius</td>
<td>UDP source or destination port 1812 to be used.</td>
</tr>
<tr>
<td>rtp and rtcp</td>
<td>RTSP has embedded RTP/RTCP payloads (you need to enable RTP dynamic flow detection to catch those flows); or, RTSP or SDP (for SDP within SIP) creates an RTP/RTCP flow over UDP (in addition to enabling the aforementioned dynamic flow detection, you must make sure that UDP packets are routed to the UDP analyzer) or, RTP/RTCP uses predefined UDP port numbers (e.g. default UDP port numbers of 5004/5005).</td>
</tr>
<tr>
<td>rtsp</td>
<td>TCP destination port or source port is RTSP (554).</td>
</tr>
<tr>
<td>sdp</td>
<td>RTSP or SIP content type is application/sdp</td>
</tr>
<tr>
<td>secure-http</td>
<td>TCP destination port or source port is HTTPS (443). Note that HTTP may use the CONNECT method (see RFC 2817), in which case, the subscriber will be upgraded with transport layer security, but the traffic to/from the chassis will still be HTTP and be passed through the http rather than the secure-http analyzer (assuming that routing to the http analyzer has been configured).</td>
</tr>
<tr>
<td>sip</td>
<td>UDP destination port or source port is SIP (5060).</td>
</tr>
<tr>
<td>smtp</td>
<td>TCP destination port or source port is SMTP (25).</td>
</tr>
<tr>
<td>tcp</td>
<td>All IPv4 packets with IP protocol = TCP (6) are automatically routed here.</td>
</tr>
<tr>
<td>udp</td>
<td>All IPv4 packets with IP protocol = UDP (17) are automatically routed here.</td>
</tr>
<tr>
<td>wap2</td>
<td>TCP destination port or source port of the carrier-specific port number for WAP-2 (e.g. one carrier uses 8799); or, send all HTTP traffic to the wap2 analyzer if the carrier does not use a special port number.</td>
</tr>
<tr>
<td>wsp</td>
<td>UDP destination port or source port is connection-less WSP (9200) or connection-oriented WSP (9201).</td>
</tr>
<tr>
<td>wtp</td>
<td>Packets are automatically routed here, if you specified “wsp-connection-oriented” as described above.</td>
</tr>
</tbody>
</table>
Example

The following command assigns a route and rule action with the route priority of 23, a ruledef named `test`, and an analyzer `test_analyzer` with description as `route_test1` to the current rulebase:

```
route priority 23 ruledef test analyzer test_analyzer description route_test1
```
**rtp dynamic-flow-detection**

This command allows you to enable/disable the Real Time Streaming Protocol (RTSP) and Session Description Protocol (SDP) analyzers to detect the start/stop of RTP and RTCP flows.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > ACS Configuration > Rulebase Configuration

```
active-charging service service_name > rulebase rulebase_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

**Syntax**

```
[ default | no ] rtp dynamic-flow-detection
```

**default**

Confirms this command with its default setting.
Default: Disabled; same as `no rtp dynamic-flow-detection`.

**no**

If previously configured, deletes this configuration from the current rulebase.

**Usage**

Use this command to enable the RTSP and SDP analyzer to detect the start/stop of RTP and RTCP flows. This command is used in conjunction with the `route priority` command.

**Example**

The following command enables RTP dynamic flow detection:

```
rtp dynamic-flow-detection
```
rtsp initial-bytes-limit

This command allows to set the maximum number of uplink and downlink bytes, added together to accumulate, while rule matching and charging is being delayed for RTSP flows. The limit is per RTSP flow.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Rulebase Configuration

`active-charging service service_name > rulebase rulebase_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

Syntax

```
rtsp initial-bytes-limit rtsp_bytes

default rtsp initial-bytes-limit
```

---

**default**

Configures the RTSP initial packets limit to 6000 bytes.

**RTSP_bytes**

Specifies the maximum number of uplink and downlink bytes limit. `rtsp_bytes` must be an integer from 1 through 256000.

---

Usage

Use this command to configure the maximum number of uplink and downlink bytes per RTSP flow that can be accumulated before the first SETUP request. The accumulated bytes include both TCP-control packets as well as RTSP packets. Once this limit is reached, rule matching occurs and charging is enforced on the flow. This command is used in conjunction with the `flow rtsp-all-pkts charge-to-application` command.

Example

The following command sets the RTSP initial bytes limit to 9000 bytes:

```
rtsp initial-bytes-limit 9000
```
**ruledef-parsing**

This command allows you to configure whether to consider or ignore the port number embedded in the application header (for example, the ":80" in www.star.com:80) when comparing the ruledef expressions to the packet contents.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Rulebase Configuration

```
active-charging service service_name > rulebase rulebase_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

**Syntax**

```
[ no ] ruledef-parsing ignore-port-numbers-embedded-in-application-headers analyzers { http rtsp sip wsp }
```

**Usage**

If previously configured, deletes the ruledef-parsing configuration from the current rulebase.

```
default ruledef-parsing
```

**Example**

Use this command to make the HTTP, RTSP, SIP, and WSP analyzer ignore port numbers embedded in application headers.

The following command makes the HTTP analyzer in the current rulebase ignore port numbers embedded in application headers:

```
ruledef-parsing ignore-port-numbers-embedded-in-application-headers analyzers http
```
tcp 2msl-timeout

This command allows you to configure how long to retain the TCP flow after the FIN has been acknowledged.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Rulebase Configuration

```
active-charging service service_name > rulebase rulebase_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

**Syntax**

```
tcp 2msl-timeout 2msl_timeout [port-reuse ]

{ default | no } tcp 2msl-timeout
```

- **default**
  Configures this command with its default setting.
  Default: 2 seconds

- **no**
  Disables the timeout and sets the system to delete the flow immediately upon seeing the FIN acknowledged.

```
tcp 2msl-timeout 2msl_timeout
```

Specifies the duration to keep the TCP flow.

2msl_timeout specifies the timeout duration, in seconds, and must be an integer from 1 through 20.

```
port-reuse
```

Allows the source port reuse to reopen the TCP flow in 2msl timeout.

**Usage**

Use this command to configure how long to retain the TCP flow after the FIN has been acknowledged. Acknowledgment to the FIN is not guaranteed to be received by the destination, then the FIN could be resent and re-acknowledged. In this scenario, it is desirable to still have the flow, so that the re-sends do not create a new flow.

**Example**

The following command sets the timeout to 4 seconds:

```
tcp 2msl-timeout 4 port-reuse
```
**tcp check-window-size**

This command allows you to enable/disable TCP window-size checking.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Rulebase Configuration

`active-charging service service_name > rulebase rulebase_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

**Syntax**

```
[ default | no ] tcp check-window-size
```

- **default**
  Configures this command with its default setting.
  Default: Enabled (packets after the erroneous packet (with size greater than the receiver’s window size) will hit tcp-error ruledef).

- **no**
  Disables the window-size check and continues with normal L7 parsing.

- **tcp check-window-size**
  Enables the window-size check and continues with normal L7 parsing.

**Usage**
Use this command to enable/disable TCP window-size check for packets out of TCP window.

**Example**
The following command enables TCP window-size check:

```
tcp check-window-size
```
**tcp mss**

This command allows you to configure the TCP Maximum Segment Size (MSS) in TCP SYN packets.

---

**Important:** This command is only available in StarOS 8.1 and later releases.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Rulebase Configuration

```
active-charging service service_name > rulebase rulebase_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-rule-base)#
```

**Syntax**

```
tcp mss tcp_mss { add-if-not-present | limit-if-present } +
{ default | no } tcp mss
```

- **default**
  Configures this command with its default setting.
  Default: Disabled

- **no**
  If previously configured, deletes the TCP MSS configuration from the current rulebase.

```
tcp_mss tcp_mss
```

Specifies the TCP MSS.

- **tcp_mss**
  must be an integer from 496 through 65535.

- **add-if-not-present**
  Specifies to add the TCP MSS if not present in the packet.

- **limit-if-present**
  Specifies to limit the TCP MSS if present in the packet.

**Usage**

Using this command, TCP MSS can be limited if already present in the TCP SYN packets. If there are no errors detected in IP header/TCP mandatory header and there are no memory allocation failures, TCP
optional header is parsed. If TCP MSS is present in the optional header and its value is greater than the configured MSS value, the value present in the TCP packet is replaced with the configured one. If the TCP optional header is not present in the SYN packet and there are no errors in already present TCP header, the TCP MSS value configured will be inserted while sending the current packet out.

**Example**

The following command limits the TCP maximum segment size to 3000, and if not present adds it to the packets:

```
tcp mss 3000 limit-if-present add-if-not-present
```
tcp out-of-order-timeout

**Description** This command has been deprecated, and is replaced by the tcp packets-out-of-order command.
tcp packets-out-of-order

This command allows you to configure processing of TCP packets that are out of order, while waiting for the earlier packet(s) to arrive.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Rulebase Configuration

active-charging service service_name > rulebase rulebase_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-rule-base)#

Syntax

tcp packets-out-of-order { timeout timeout_duration | transmit [ after-reordering | immediately ] }

default tcp packets-out-of-order { timeout | transmit }

default

Configures this command with its default setting.

*timeout: 5000 milliseconds

*transmit: immediately

timeout timeout_duration

Specifies the timeout duration for re-assembly of TCP out-of-order packets.

timeout_duration is the timeout duration, in milliseconds, and must be an integer from 100 through 30000.

Default: 5000 milliseconds

transmit [ after-reordering | immediately ]

Configures the TCP out-of-order segment behavior after buffering a copy.

*after-reordering: Delivers the TCP out-of-order segments in-sequence to the ECS analyzer after all packets are received and successfully reordered. The 'after-reordering' feature is doing this by buffering out-of-order packets, and only releasing them after the missing out-of-order packets are received (or after OOO timeout).

When the missing packet is received, complete deep packet inspection of all the packets and all relevant in-line services is done, and then the last packet is forwarded (as the latest). If reordering is not successful within the specified OOO timeout, all the subsequent received packets in that TCP flow are forwarded without being passed through the analysers (except the L3/L4 analyzer). As a consequence only L3/L4 rule matching will take place. If memory allocation fails or the received packet is partial retransmitted data, the packet will also be forwarded immediately without being passed through the protocol analyzers, except for the L3/L4 analyzers.
**Important:** On the outgoing interface, no in-sequence delivery is guaranteed. This feature is intended to: - deliver the TCP segments in-order to the ECS analysers - buffer the original packets during OOO conditions, such that application-based flow actions (ex: Header insertion) can still take place on the actual data packets - it is not intended to put the packets in-sequence on the outgoing interface (although some improvement can be seen there as well) - the cost of this feature is additional delay for OOO packets (up to a maximum of the OOO timeout).

- **Immediately:** Delivers the TCP out-of-order segments in-sequence to the ECS analyzer after all packets are received and successfully reordered. The 'immediately' feature is accomplishing this by making a copy of out-of-order packets, and buffering those, while transmitting the original data packets through the outgoing interface immediately. When the missing packet is received, complete deep packet inspection of all the packets and all relevant in-line services is done, and then the last packet is forwarded.

If reordering of the buffered packets is not successful within the specified OOO timeout, all the subsequent received packets in that TCP flow are forwarded without being passed through the analysers (except the L3/L4 analyzer). As a consequence only L3/L4 rule matching will take place.

If memory allocation fails or the received packet is partial retransmitted data, the packet will also be forwarded immediately without being passed through the protocol analyzers, except for the L3/L4 analysers.

**Important:** This feature is not changing anything on the sequencing of the packets - this feature has the consequence that during OOO conditions, certain application-based flow actions (ex: Header insertion) could not take place as the original packets are already sent out by the time the ECS analyzer receives the (copies of) in-sequence packets.

Default: **immediately**

**Usage**

Use this command to configure how to process TCP packets that are out of order, while waiting for the earlier packet(s) to arrive.

**Example**

The following command sets the timeout timer to 10000 milliseconds:

```
tcp packets-out-of-order timeout 10000
```
tcp proxy-mode

This command allows you to enable/disable TCP Proxy mode for all subscribers using the current rulebase.

Product
ACS
CF
MVG

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Rulebase Configuration
active-charging service service_name > rulebase rulebase_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-rule-base)#

Syntax

tcp proxy-mode { dynamic { all | content-filtering | dcca | ip-readdressing | nexthop-readdressing | xheader-insert } + | static [ port [ port_number [ to port_number ] ] ] }

default tcp proxy-mode

no tcp proxy-mode { dynamic { content-filtering | dcca | ip-readdressing | nexthop-readdressing | xheader-insert } + | static [ port [ port_number [ to port_number ] ] ] }

default

Configures this command with its default setting.
Default: Disabled

no

If previously enabled, disables TCP Proxy mode.
Optionally, TCP Proxy can be disabled for specific options that were previously enabled.

dynamic { all | content-filtering | dcca | ip-readdressing | nexthop-readdressing | xheader-insert } +

Enables TCP proxy for subscriber-initiated TCP flows under the specified condition(s).

- **all**: Specifies that subscriber-initiated TCP flows be proxied if all/any of the following conditions are satisfied.

- **content-filtering**: Specifies that subscriber-initiated TCP flows be proxied if a URL is requested, and that URL is checked because Category-based Content Filtering is enabled in the rulebase.

- **dcca**: Specifies that subscriber-initiated TCP flows be proxied if DCCA is enabled in the charging action.

- **ip-readdressing**: Specifies that subscriber-initiated TCP flows be proxied if IP Readdressing feature is enabled in the charging action.
• **nexthop-readdressing**: Specifies that subscriber-initiated TCP flows be proxied if Nexthop Readdressing feature is enabled in the charging action.

• **xheader-insert**: Specifies that subscriber-initiated TCP flows be proxied if x-Header Insertion feature is enabled in the charging action.

```
static [ port [ port_number [ to port_number ] ] ]
```

Enables static TCP proxy for every subscriber-initiated TCP flow, unless specific ports are specified.

```
port [ port_number [ to port_number ] ]
```

Specifies port numbers and/or range of port numbers.

`port_number` must be an integer from 1 through 65535.

**Important**: Up to 32 port numbers and eight port ranges can be specified.

**Usage**

**Important**: In release 11.0, TCP Proxy functions only in Static mode. Dynamic TCP Proxy mode is supported only in 12.0 and later releases.

Use this command to enable/disable TCP Proxy mode for all subscribers using this ACS rulebase. Optionally, TCP Proxy can be enabled/disabled for specific ACS features. Note that enabling/disabling the TCP Proxy feature for any of the optional ACS features, does not affect that feature.

Note that the last command overwrites any previous configuration. For example, when the following commands are applied in sequence:

```
tcp proxy-mode dynamic nexthop-readdressing
tcp proxy-mode dynamic xheader-insert
```

The `nexthop` configuration is overwritten by the `x-header` configuration.

**Example**

The following command enables TCP proxy for subscriber-initiated TCP flows whenever next-hop-forwarding-address is configured in the charging action:

```
tcp proxy-mode dynamic nexthop-readdressing
```
tethering-detection

This command allows you to enable/disable the Tethering Detection feature for the current rulebase, and specifies the database to use.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Rulebase Configuration

```
active-charging service service_name > rulebase rulebase_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

**Syntax**

```
tethering-detection { os-db-only | ua-db-only }

{ default | no } tethering-detection
```

---

**default**

Configures this command with its default setting.

Default: By default, the Tethering Detection feature is disabled. When enabled, unless a specific database is specified to be used, by default tethering detection will make use of both the databases.

---

**no**

If previously configured, deletes the tethering detection configuration from the current rulebase.

---

**os-db-only**

Specifies to perform tethering detection using only the OS signature database.

---

**ua-db-only**

Specifies to perform tethering detection using only the UA signature database.

---

**Usage**

Use this command to enable/disable the Tethering Detection feature for a rulebase, and configures the database to use.

Changing the configuration does not affect existing flows of the subscriber. If Tethering Detection was disabled and is turned enabled, it will be applied only to new flows of subscribers using the rulebase.

---

**Important:** IPv6 Tethering Detection is supported only with TTL and UA signatures, and not supported for OS signatures.

Also, see the `tethering-database` command in the *ACS Configuration Mode Commands* chapter.
Example

The following command enables the Tethering Detection feature in the rulebase, and specifies to use only the OS database:

```
tethering-detection os-db-only
```
tft-notify-ue-def-bearer

This command allows you to control whether TFT updates are sent to UE or not for default bearer for the specified rulebase.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Rulebase Configuration
```
active-charging service service_name > rulebase rulebase_name
```

Entering the above command sequence results in the following prompt:
```
[local]host_name(config-rule-base)#
```

**Syntax**
```
{ default | no } tft-notify-ue-def-bearer
```

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>The default behavior is to send the TFT updates of default bearer for the specified APN to UE.</td>
</tr>
<tr>
<td>no</td>
<td>This keyword controls the TFT updates of default bearer for the APN attached to the chassis, from being sent to the UE.</td>
</tr>
</tbody>
</table>

**Usage**
Use this command at the rulebase level to control whether TFT updates are sent to UE or not for default bearer for the specified rulebase.

This feature provides the operator the flexibility to configure this per Rulebase and also configure to suppress TFT updates only. The CLI command allows sending other QoS updates to the UE and controls only the TFT related updates. This CLI is supported only for default bearer.

In releases prior to 15.0, the "no policy-control update-default-bearer" CLI command is used to suppress all the TFT updates to the UE on the default bearer including the initial TFTs sent in the Create Session Response. Also, this configuration is available for the entire system and not per rulebase.

Additionally, this CLI command suppresses all the QoS related updates (including change in bit rate) to the UE.
timestamp rounding

This command allows you to enable/disable timestamp rounding in EDRs or eG-CDRs.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Rulebase Configuration

active-charging service service_name > rulebase rulebase_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-rule-base)#

Syntax

timestamp rounding { edr | egcdr } { ceiling | floor | round-off }

{ default | no } timestamp rounding { edr | egcdr }

default
Configures this command with its default setting.
Default: round-off

no
Disables timestamp rounding.

edr
Enables timestamp rounding for EDRs.

ecdr
Enables timestamp rounding for eG-CDRs.

ceiling
If the fractional part of the seconds is greater than 0, adds 1 to the number of seconds and discards the fraction.

floor
Discards the fractional part of the second.

round-off
Sets the fractional part of the seconds to nearest integer value. If the fractional value is greater than or equal to 0.5, it adds 1 to the number of seconds and discards the fractional part of second.
### Usage

Use this command to configure the timestamp rounding setting. The specified rounding will be performed before system attempts any calculation. For example using round-off, if the start time is 1.4, and the end time is 1.6, then the calculated duration will be 1 (for example, 2 – 1 = 1).

This command may be repeated for each type of EDR or eG-CDR.

### Example

The following command sets the EDR timestamp to nearest integer value second; for example, 34:12.23 to 34:12.00:

```
timestamp rounding edr round-off
```
tpo default-policy

The Traffic Performance Optimization (TPO) in-line service is not supported in this release.
**transactional-rule-matching**

This command allows you to enable or disable transactional rule matching (TRM) which allows the Enhanced Charging Service (ECS) to bypass per-packet rule matching on a transaction once the transaction is fully classified.

**Product**
- ACS
- ADC

**Privilege**
- Security Administrator, Administrator

**Mode**
- `Exec > ACS Configuration > Rulebase Configuration`

**Syntax**

```plaintext
transactional-rule-matching
[ default | no ] transactional-rule-matching
```

**Usage**

Use this command to enable or disable transactional rule matching. This allows the Enhanced Charging Service (ECS) to bypass per-packet rule matching on a transaction once the transaction is fully classified. A transaction for TRM can be defined as the entire UDP flow, the ACK of the 3-way handshake to the FIN/RST of a TCP flow, or the HTTP request to the next HTTP request, or HTTP request to the FIN/RST for the final request of the flow. Rule matching can be performed on IP L4 rules (UDP, TCP), HTTP, and HTTPS.

**Example**

The following command enables transactional rule matching:

```plaintext
transactional-rule-matching
```
transport-layer-checksum

This command allows you to enable/disable checksum verification for TCP and UDP packets.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Rulebase Configuration
active-charging service service_name > rulebase rulebase_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-rule-base)#

Syntax

[ no ] transport-layer-checksum verify-during-packet-inspection [ tcp | udp ]
default transport-layer-checksum

no
Disables the checksum calculation for the specified packet type.

default
Configures this command with its default setting.
Default: Same as transport-layer-checksum verify-during-packet-inspection—to perform the checksum verification calculation on all TCP and UDP packets.

[ tcp | udp ]
Specifies that either TCP or UDP packets should be verified/not verified.
If neither of these keywords is specified the command applies to both TCP and UDP packets.

Usage
Use this command to disable or enable performing checksum verification calculations on TCP or UDP packets.
If the checksum is not verified, the packets will go through the TCP/UDP analyzers (and deeper analyzers, if so configured via the route command) regardless of the value of the TCP/UDP checksum.
If the checksum is verified, only packets with good checksums will go through the TCP/UDP analyzers (and deeper analyzers, if so configured).

Example
The following command disables checksum verification calculations on all TCP and UDP packets:

no transport-layer-checksum verify-during-packet-inspection
udsr threshold

This command allows you to configure the threshold limit to generate Usage Data Records (UDRs) that provide Comma Separated Value (CSV) records written periodically in a fixed schema designed to reflect a total billable quantity.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Rulebase Configuration

active-charging service service_name > rulebase rulebase_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-rule-base)#

Syntax

udr threshold { interval interval | volume { downlink bytes [ uplink bytes ] | total bytes | downlink bytes [ uplink bytes ] } }

default udr threshold { interval | volume }

no udr threshold { interval | volume { downlink [ uplink ] | total | uplink [ downlink ] } }

---

no

If previously configured, deletes the UDR threshold configuration from the current rulebase.

---

default

Configures this command with its default setting.
Default: Disabled; same as no udr threshold interval and no udr threshold volume.

---

interval interval

Specifies the time interval, in seconds, for closing the UDR if the minimum time duration thresholds are satisfied. By default, this option is disabled.
interval must be an integer from 60 through 40000000.
Default: 0 (Disabled)

---

volume

Specifies uplink/downlink volume octet counts for the generation of interim UDRs.

•downlink bytes: Specifies the limit for the number of downlink octets after which the UDR is closed.

bytes must be an integer from 100000 through 4000000000.
Default: 4000000000

•total bytes: Specifies the limit for the total number of octets (uplink+downlink) after which the UDR is closed.
udr threshold

- **bytes** must be an integer from 100000 through 4000000000.
  
  Default: Disabled

- **uplink bytes**: Specifies the limit for the number of uplink octets after which the UDR is closed.
  
  bytes must be an integer from 100000 through 4000000000.
  
  Default: 4000000000

UDR records are generated whenever either threshold is reached.

**Usage**

Use this command to enable thresholds for generation of UDRs.

**Example**

The following command specifies that UDR records should be generated every 10 minutes (600 seconds):

```plaintext
udr threshold interval 600
```
udr trigger

This command allows you to configure additional triggers for generating UDRs.

**Important:** This command is only available in StarOS 8.3 and later releases.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Rulebase Configuration

`active-charging service service_name > rulebase rulebase_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-rule-base)#
```

**Syntax**

```
udr trigger first-hit-content-id | tariff-time minute minutes hour hours

no udr trigger first-hit-content-id | tariff-time

default udr trigger
```

**udr trigger**

- **no**
  Disables first-hit-content-id UDR trigger.

- **default**
  Configures this command with its default setting.
  Default: Disabled; no additional triggers.

- **first-hit-content-id**
  Specifies to generate interim UDR on first packet hit per rating group/content ID.

- **tariff-time minute minutes hour hours**
  This keyword allows to configure tariff time trigger to close ongoing UDR buckets and save all data traffic up to tariff time in a single UDR file. By default, this CLI keyword is disabled.
  Configuring this keyword enables the PDSN/PCEF to generate content base UDR record for each concurrent online subscriber in each of day cross and place them in a single UDR file. The charging records include content based service (by duration and by volume).
  Tariff time is stored at rulebase level. Therefore if the tariff time is updated while there are ongoing calls in the network, the old tariff time will be ignored and the new tariff time will be applied to the existing as well as upcoming calls.
  At the end of the “Tariff Time” period, the UDR files are created and the next set of records are stored in a new UDR file.
Usage
This command enables to assign first packet trigger to interim UDRs—for generating UDR for first packet hit per rating group/content ID. The first-hit-content-id trigger when configured causes an UDR to be generated as soon as a packet hits a Charging Action with a content ID. UDR generation will be triggered when this command is configured and present in the rulebase.

Example
The following command assigns first packet trigger to interim UDRs, for generating UDR for first packet hit per rating group/content ID:

```
udr trigger first-hit-content-id
```
url-blacklisting action

This command allows you to enable/disable URL Blacklisting functionality for the current rulebase, and configures the action to be taken when there is a URL match.

Product
CF

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Rulebase Configuration

active-charging service service_name > rulebase rulebase_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-rule-base)#

Syntax

url-blacklisting action { discard | redirect-url url | terminate-flow | www-reply-code-and-terminate-flow reply_code } [ content-id content_id ]

{ default | no } url-blacklisting action

---

default
Disables URL Blacklisting in the current rulebase.

---

no
If previously configured, deletes the URL Blacklisting action configuration from the current rulebase.

---

discard
Configures URL Blacklisting “discard” action.

---

redirect-url url
Configures URL Blacklisting “redirect-url” action.

url specifies the redirect URL/URI, which must be a fully qualified URL/URI, and must be an alphanumeric string of 1 through 1023 characters.

---

terminate-flow
Configures URL Blacklisting “terminate-flow” action.

---

www-reply-code-and-terminate-flow reply_code
Configures URL Blacklisting “terminate-flow” action with reply code.

reply_code specifies the reply code, and must be an integer from 100 through 599.
url-blacklisting action

content-id content_id

Usage
Use this command to enable/disable URL Blacklisting at the rulebase level, and configure the action to be taken.

Example
The following command enables URL Blacklisting in the rulebase, and configures the terminate-flow action with reply code 300:

```
url-blacklisting action www-reply-code-and-terminate-flow 300
```

The following command disables URL Blacklisting feature in the rulebase:

```
no url-blacklisting action
```
url-preprocessing

This command allows you to enable/disable a group-of-prefixed-urls for preprocessing of embedded URLs.

**Important:** This command is customer specific. For more information, please contact your Cisco account representative.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Rulebase Configuration

*active-charging service service_name > rulebase rulebase_name*

Entering the above command sequence results in the following prompt:

[local]host_name(config-rule-base)#

**Syntax**

```
[ no ] url-preprocessing bypass group-of-prefixed-urls prefixed_urls_group_name
```

- **no**
  
  If previously configured, deletes the URL-preprocessing bypass configuration from the current rulebase.

- **group-of-prefixed-urls prefixed_urls_group_name**
  
  Specifies the group-of-prefixed-urls. 
  
  *prefixed_urls_group_name* must be the name of a group-of-prefixed-urls, and must be an alphanumeric string of 1 through 63 characters.

**Usage**

Use this command to enable/disable a group-of-prefixed-urls for preprocessing of embedded URLs. This command can be issued multiple times to enable multiple groups. If an embedded URL begins with the string specified within any of the groups, that prefix text will be removed from the URL.

**Example**

The following command enables looking for prefixed URLs of the group-of-prefixed-urls named *test5*:

```
url-preprocessing bypass group-of-prefixed-urls test5
```
video optimization-preprocessing cae-readdressing

This command allows you to enable/disable CAE readdressing at the rulebase level.

**Product**

ACS
MVG

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > ACS Configuration > Rulebase Configuration

```plaintext
active-charging service service_name > rulebase rulebase_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-rule-base)#
```

**Syntax**

```plaintext
video optimization-preprocessing cae-readdressing
[ default | no ] video optimization-preprocessing
```

- **default**
  
  Configures this command with its default setting.

- **no**
  
  If already configured, disables CAE readdressing.

**Usage**

Use this command to configure ACS to readdress the flows to CAE.
wtp out-of-order-timeout

**Description** This command has been deprecated, and is replaced by the `wtp packets-out-of-order` command.
wtp packets-out-of-order

This command allows you to configure how to process Wireless Transaction Protocol (WTP) packets that are out of order, while waiting for the earlier packet(s) to arrive.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Rulebase Configuration

active-charging service service_name > rulebase rulebase_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-rule-base)#

Syntax

wtp packets-out-of-order { out-of-order-timeout timeout | transmit [ after-reordering | immediately ] }

default wtp packets-out-of-order { out-of-order-timeout | transmit }

default

Configures this command with its default setting.

*out-of-order-timeout: 5000 milliseconds

*transmit: immediately

out-of-order-timeout timeout

Specifies the maximum duration for which WTP out-of-order packets are retained, before reassembly is needed.

timeout is the timeout duration, in milliseconds, and must be an integer from 100 through 30000.

Default: 5000 milliseconds

transmit [ after-reordering | immediately ]

Specifies the WTP out-of-order segment behavior after buffering a copy:

*after-reordering: Sends WTP out-of-order segment after it becomes ordered

*immediately: Sends WTP out-of-order segment immediately after buffering a copy

Default: immediately

Usage

Use this command to configure TCP out-of-order segment options.

If out-of-order-timeout is specified, out-of-order packets are retained, until either all packets have been received or the configured timeout has expired for the oldest packet. If all packets have been received, a temporary complete packet is reconstructed for analysis. Then all packets are forwarded in order from first to
last. If all packets are not received, the packets will be forwarded without being passed through the protocol analyzers, except for the IP analyzer.

If `after-reordering` transmitting is specified, the packets are held onto and reordered. After successfully reordering the packets, they are processed in the proper order. If reordering is not successful due to timeout (wtp out-of-order-timeout), the received packets are forwarded without being passed through the protocol analyzers.

If `immediately` is specified, the packets are transmitted as they are received without any in-line services or Charging Action processing, however a copy of each packet is retained. When the missing packet is received, complete deep packet inspection of all the packets and all relevant in-line services is undertaken, and then the last packet is forward (unless otherwise configured by the in-line services or Charging Action).

**Example**

The following command sets the timeout timer to 10000 milliseconds:

```
    wtp out-of-order-timeout 10000
```
xheader-encryption

This command allows you to configure X-Header Encryption feature’s parameters.

⚠ Important: This command is license dependent. For more information please contact your Cisco account representative.

Product

ACS

Privilege

Security Administrator, Administrator

Mode

Exec > ACS Configuration > Rulebase Configuration

active-charging service service_name > rulebase rulebase_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-rule-base)#

Syntax

xheader-encryption { certificate-name certificate_name | re-encryption period period }

default xheader-encryption re-encryption period

no xheader-encryption { certificate-name | re-encryption }

default

Configures this command with its default setting.

Default: Disabled

no

If previously configured, deletes the configuration from the current rulebase.

certificate-name certificate_name

Specifies the encryption certificate to use for the X-Header Encryption feature.

certificate_name must be the name of an encryption certificate, and must be an alphanumeric string of 1 through 63 characters.

Default: Disabled; no encryption certificate

re-encryption period period

Specifies how often to re-generate the encryption keys.

period specifies the re-encryption time period in minutes, and must be an integer from 1 through 10000.

Default: Disabled; no re-encryption
Usage

Use this command to configure the X-Header Encryption feature’s certificate and re-encryption parameters.

Example

The following command configures the X-Header Encryption feature to use the certificate named testcert:

```
xheader-encryption certificate-name testcert
```
Chapter 19
ACS Ruledef Configuration Mode Commands

The ACS Ruledef Configuration Mode is used to create and manage rule expressions in individual rule definitions (ruledefs).

**Important**: In 14.1 and earlier releases, up to 10 rule expressions can be configured in one ruledef. In 15.0 and later releases, up to 32 rule expressions can be configured in one ruledef.

**Mode**

Exec > ACS Configuration > Ruledef Configuration

`active-charging service service_name > ruledef ruledef_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Important**: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
bearer 3gpp apn

This command allows you to define rule expressions to match Access Point Name (APN) of the bearer flow.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] bearer 3gpp apn [ case-sensitive ] operator apn_name
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **case-sensitive**
  Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

- **operator**
  Specifies how to match.
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `!contains`: Does not contain
  - `!ends-with`: Does not end with
  - `!starts-with`: Does not start with
  - `=`: Equals
  - `contains`: Contains
  - `ends-with`: Ends with
  - `starts-with`: Starts with

- **apn_name**
  Specifies name of the APN to match.
  `apn_name` must be an alphanumeric string of 1 through 62 characters and may contain punctuation characters.
Usage
Use this command to define rule expressions to match an APN in the bearer flow.

Example
The following command defines a rule expression to match user traffic based on APN named *apn12*:

```
bearer 3gpp = apn12
```
bearer 3gpp imsi

This command allows you to define rule expressions to match International Mobile Station Identification (IMSI) number in the bearer flow.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local] host_name(config-acs-ruledef)#

Syntax

[ no ] bearer 3gpp imsi { operator imsi | { !range | range } imsi_pool imsi_pool_name }

- no
  If previously configured, deletes the specified rule expression from the current ruledef.

- operator
  Specifies how to match.
  operator must be one of the following:
  - !=: Does not equal
  - ==: Equals

- imsi
  Specifies the IMSI number to match.

- !range | range
  !range | range: Specifies the range criteria:
  - !=range: Not in the range of
  - ==range: In the range of

- imsi_pool imsi_pool_name
  Specifies the IMSI pool.
  imsi_pool_name must be the name of an IMSI pool, and must be an alphanumeric string of 1 through 63 characters.

Usage
Use this command to define rule expressions to match an IMSI.

Example
The following command defines a rule expression to analyze user traffic for the IMSI number 9198838330912:

`bearer 3gpp imsi = 9198838330912`
bearer 3gpp rat-type

This command allows you to define rule expressions to match Radio Access Technology (RAT) in the bearer flow.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] bearer 3gpp rat-type operator rat_type

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be one of the following:
• !=: Does not equal
• ==: Equals

rat_type
Specifies the RAT type to match.
rat_type must be one of the following:
• geran: GSM EDGE Radio Access Network type
• utran: UMTS Terrestrial Radio Access Network type
• wlan: Wireless LAN type

Usage
Use this command to define rule expressions to match a RAT type.

Example
The following command defines a rule expression to match user traffic based on RAT type wlan:

    bearer 3gpp rat-type = wlan
bearer 3gpp sgsn-address

This command allows you to define rule expressions to match SGSN address associated in the bearer flow.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration
active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax
[ no ] bearer 3gpp sgsn-address operator ipv4/ipv6_address

- **no**
  - If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  - Specifies how to match.
  - *operator* must be one of the following:
    - !=: Does not equal
    - ==: Equals

- **ipv4/ipv6_address**
  - Specifies the SGSN IP address to match.
  - *ipv4/ipv6_address* must be in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

Usage
Use this command to define rule expressions to match IP address of an SGSN node. This command replaces the **bearer sgsn-address** command.

Example
The following command defines a rule expression to analyze user traffic for an SGSN node with IP address 10.1.1.1:

```
bearer 3gpp sgsn-address = 10.1.1.1
```
bearer 3gpp2 bsid

This command allows you to define rule expressions to match Base Station Identifier (BSID) associated with the bearer.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] bearer 3gpp2 bsid [ case-sensitive ] [ use-group-of-objects ] operator string
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **case-sensitive**
  Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

- **use-group-of-objects**
  Specifies using a group-of-objects as a qualifier to match this rule.

- **operator**
  Specifies how to match.
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `!contains`: Does not contain
  - `!ends-with`: Does not end with
  - `!starts-with`: Does not start with
  - `=`: Equals
  - `contains`: Contains
  - `ends-with`: Ends with
  - `starts-with`: Starts with

- **string**
  Specifies the name of a group-of-objects to match.
  If the `use-group-of-objects` keyword is not included in the command, `string` specifies name of the matching 3GPP2 service Base Station ID (BSID) in bearer flow.
If the `use-group-of-objects` keyword is included in the command, `string` must be the name of the group-of-objects to use. In this case, it is checked if the rule is satisfied for either one or none of the objects in the group-of-objects depending upon the operator used. For example, if the `operator` is `contains`, the expression would be true if any of the objects in the specified object group is contained in the BSID. If the `operator` is `!contains`, then the expression would be true if none of the objects in the object group is contained in the BSID.

`string` must be an alphanumeric string of 1 through 16 characters, and may contain punctuation characters.

**Usage**

Use this command to define rule expressions to match a 3GPP2 Base Station Identifier (BSID).

**Example**

The following command defines a rule expression to analyze user traffic for 3GPP2 BSID named `bs001_xyz`:

```
bearer 3gpp2 bsid = bs001_xyz
```
bearer 3gpp2 service-option

This command allows you to define rule expressions to match 3GPP2 service with service options associated with the bearer.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] bearer 3gpp2 service-option operator service_option_code

- **no**
  - If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  - Specifies how to match.
  - **operator** must be one of the following:
    - !=: Does not equal
    - <=: Lesser than or equals
    - =: Equals
    - >=: Greater than or equals

- **service_option_code**
  - Specifies the 3GPP2 service option code to match.
  - **service_option_code** must be an integer from 0 through 1000.

Usage

Use this command to define rule expressions to match a 3GPP2 service’s service option code.

Example

The following command defines a rule expression to analyze user traffic for a 3GPP2 service’s service option matching 1034:

```
bearer 3gpp2 service-option = 1034
```
bearer apn

This command allows you to define rule expressions to match the APN used for the subscriber session.

‼️Important: In 8.1 and later releases, this command is deprecated and is replaced by the bearer 3gpp apn command.

Product
GGSN

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

Syntax

```
[ no ] bearer apn [ case-sensitive ] operator apn_name
```

no
If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive
Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator
Specifies how to match.

- `!=`: Does not equal
- `!contains`: Does not contain
- `!ends-with`: Does not end with
- `!starts-with`: Does not start with
- `=`: Equals
- `contains`: Contains
- `ends-with`: Ends with
- `starts-with`: Starts with

apn_name
Specifies the APN to match.
**Usage**

Use this command to define rule expressions to match APN used for subscriber session.

**Example**

The following command defines a rule expression to match user traffic based on APN name `apn12`:

```
bearer apn = apn12
```
**bearer imsi**

This command allows you to define rule expressions to match IMSI number of the subscriber.

**Important:** In 8.1 and later releases, this command is deprecated and is replaced by the `bearer 3gpp imsi` command.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**
```
[ no ] bearer imsi { operator imsi | { !range | range } imsi_pool imsi_pool_name }
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `==`: Equals

- **imsi**
  Specifies the IMSI number to match.

- **!range | range**
  Specifies the range criteria:
  - `!range`: Not in the range of
  - `range`: In the range of

- **imsi_pool imsi_pool_name**
  Specifies an IMSI pool.
  `imsi_pool_name` must be the name of an IMSI pool, and must be an alphanumeric string of 1 through 63 characters.
Usage
Use this command to define rule expressions to match IMSI number of subscriber.

Example
The following command defines a rule expression to match user traffic based on IMSI number 9198838330912:

```
bearer imsi = 9198838330912
```
bears rat-type

This command allows you to define rule expressions to match Radio Access Technology (RAT) in the bearer flow.

**Important:** In 8.1 and later releases, this command is deprecated and is replaced by the `bearer 3gpp rat-type` command.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

`active-charging service service_name > ruledef ruledef_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] bearer rat-type operator rat_type
```

- **no**
  - If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  - Specifies how to match.
    - `operator` must be one of the following:
      - `!=`: Does not equal
      - `=`: Equals

- **rat_type**
  - Specifies the RAT type to match.
    - `rat_type` must be one of the following:
      - `geran`: GSM EDGE Radio Access Network type
      - `utran`: UMTS Terrestrial Radio Access Network type
      - `wlan`: Wireless LAN type

**Usage**

Use this command to define rule expressions to match a RAT type.

**Example**

The following command defines a rule expression to match user traffic based on RAT type `wlan`:

```
bearer rat-type = wlan
```
bearer sgsn-address

This command allows you to define rule expressions to match IP address of the SGSN (in acting as GGSN) / P-GW (if acting as S-GW) in the bearer flow.

**Important:** In 8.1 and later releases, this command is deprecated and is replaced by the `bearer 3gpp sgsn-address` command.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs-ruledef) #
```

**Syntax**

```
[ no ] bearer sgsn-address operator ipv4/ipv6_address
```

- `no`
  If previously configured, deletes the specified rule expression from the current ruledef.

- `operator`
  Specifies how to match.
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `==`: Equals

- `ipv4/ipv6_address`
  Specifies the SGSN IP address to match.
  `ipv4/ipv6_address` must be in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

**Usage**

Use this command to define rule expressions to match IP address of the SGSN (in acting as GGSN) / P-GW (if acting as S-GW).

**Example**

The following command defines a rule expression to match user traffic based on SGSN node IP address `10.1.1.1`:

```
bearer sgsn-address = 10.1.1.1
```
bearer traffic-group

This command allows you to define rule expressions to match traffic group number associated with the subscriber session.

**Important**: This functionality is available only if the Content Access Control license has been installed on the chassis.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

**Syntax**

```
[ no ] bearer traffic-group operator group_number
```

- **no**
  
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  
  Specifies how to match.
  
  `operator` must be one of the following:
  
  - `!=`: Does not equal
  - `<=`: Lesser than or equals
  - `=`: Equals
  - `>=`: Greater than or equals

- **group_number**
  
  Specifies the traffic group number to match.
  
  `group_number` must be an integer from 1 through 255.

**Usage**

Use this command to define rule expressions to match traffic group of the subscriber session. See the `fa-ha-spi` command in the HA Service Configuration Mode Commands chapter for more information.

**Example**

The following command defines a rule expression to analyze all traffic groups assigned a value greater or equal to 23:
bearer traffic-group

bearer traffic-group >= 23
**cca quota-state**

Specifies the quota state of a subscriber for prepaid credit control service. In release 12.0 and later, this command should be used as a post-processing rule. For more information on post-processing policy command, refer to the ACS Rulebase Configuration Mode Commands chapter in this guide.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] cca quota-state operator { limit-reached | lower-bandwidth }
```

- **no**
  Disables the configured credit control quota state.

- **operator**
  Specifies how to match.
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `<=`: Lesser than or equals
  - `=`: Equals
  - `>=`: Greater than or equals

- **limit-reached**
  This state matches an affirmative end-of-quota indication for the current ruledef from the prepay server.

- **lower-bandwidth**
  This state matches the lower-bandwidth quota state of a rating group.

**Usage**

This command supports URL redirection and creates a rule for subscriber prepaid quota state as exhausted or not exhausted.

If a subscriber has exhausted the quota but has not exhausted the qualified period, a different charging-action can be applied via the `cca quota-state` command.

**Example**
The following command defines a rule expression to match user traffic based on the Credit-Control Application (CCA) quota state `limit-reached`:

```
cca quota-state = limit-reached
```
cca redirect-indicator

This command allows you to define rule expressions to match redirect-indicator state of the Credit Control Application. In release 12.0 and later, this command should be used as a post-processing rule. For more information on post-processing policy command, refer to ACS Rulebase Configuration Mode Commands chapter in this reference.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] cca redirect-indicator operator redirect_indicator

no
Disables the configured CCA redirect-indicator in the current ruledef.

operator
Specifies how to match.
operator must be one of the following:
• !=: Does not equal
• <=: Lesser than or equals
• >=: Greater than or equals

redirect_indicator
Specifies the redirect indicator for the AVP used for redirection of the URL in the RADIUS dictionary for prepaid service. It must be an integer from 0 through 4294967295.

Important: For the RADIUS server configured with different values to return for this AVP, the ACS requires ruledefs to match the different values for system to associate with charging actions that have different redirect URLs configured.

Usage

This command is used to configure an AVP to be used from a dictionary that defines the AVP for the redirect-indicator.
For example, a RADIUS dictionary specifies the 3gpp2-release-indicator to be used for the redirect indicator when RADIUS is used as the Credit-Control Application. In this case, the value for 3gpp2-release-indicator
that is returned by the RADIUS prepaid server for a quota request for a given content ID is retained by system and associated with the flow.

**Example**

The following command defines a rule expression to match redirect indicator 1234 for the URL Redirect AVP:

```
cca redirect-indicator = 1234
```
copy-packet-to-log

This command allows you to print every packet that hits the current ruledef to a log statement.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] copy-packet-to-log
```

- **no**
  - Disables the copy-packet-to-log feature.

- **copy-packet-to-log**
  - Specifies to print packets hitting the current ruledef to a log.

**Usage**

Use this command to print every packet that hits a ruledef to a log statement. This facilitates debugging.
**dns answer-name**

This command allows you to define rule expressions to match answer name in the answer section of DNS response messages.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

`active-charging service service_name > ruledef ruledef_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] dns answer-name [ case-sensitive ] operator value
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **case-sensitive**
  Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

- **operator**
  Specifies how to match.

  `operator` must be one of the following:
  - `!=`: Does not equal
  - `!contains`: Does not contain
  - `!ends-with`: Does not end with
  - `!starts-with`: Does not start with
  - `=`: Equals
  - `contains`: Contains
  - `ends-with`: Ends with
  - `starts-with`: Starts with

- **value**
  Specifies the value to match.

  `value` must be an alphanumeric string of 1 through 255 characters and may contain punctuation characters.
Usage

Use this command to define rule expressions to match an answer name from the answer section of DNS response messages.

The answer section of a DNS response may contain more than one answer. A maximum of seven answers from the response packet are parsed. For the equality expressions (=, contains, starts-with, ends-with) a match is sought from any of the answers in the packet (up to the first seven answers). For the inequality expressions (!=, !contains, !starts-with, !ends-with), a non-match is sought from all answers (up to the first seven answers).

Example

The following command defines a rule expression to match user traffic for answer name `test`:

```
dns answer-name = test
```
dns any-match

This command allows you to define rule expressions to match all DNS packets.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

`active-charging service service_name > ruledef ruledef_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] dns any-match operator condition
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  `operator` must be one of the following:
  - !=: Does not equal
  - ==: Equals

- **condition**
  Specifies the condition to match.
  `condition` must be one of the following:
  - FALSE
  - TRUE

**Usage**

Use this command to define an any-match rule expression to match all DNS packets.

**Example**

The following command defines an any-match rule expression to match all DNS packets:

```
dns any-match = TRUE
```
dns previous-state

This command allows you to define rule expressions to match previous state of the DNS FSM.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```bash
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] dns previous-state operator dns_previous_state
```

- `no`
  - If previously configured, deletes the specified rule expression from the current ruledef.

- `operator`
  - Specifies how to match.
  - `operator` must be one of the following:
    - `!=`: Does not equal
    - `=`: Equals

- `dns_previous_state`
  - Specifies the previous state to match.
  - `dns_previous_state` must be one of the following:
    - `dns-timeout`
    - `init`
    - `req-sent`
    - `resp-error`
    - `resp-success`

**Usage**
Use this command to define rule expressions to match previous state of DNS FSM.

**Example**
The following command defines a rule expression to match the DNS FSM previous state `req-sent`:

```
dns previous-state = req-sent
```
**dns query-name**

This command allows you to define rule expressions to match query name in DNS request messages.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] dns query-name [ case-sensitive ] operator query_name
```

- **no**
  
  If previously configured, deletes the specified rule expression from the current ruledef.

- **case-sensitive**
  
  Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

- **operator**
  
  Specifies how to match.
  
  `operator` must be one of the following:
  
  - `!=`: Does not equal
  - `!contains`: Does not contain
  - `!ends-with`: Does not end with
  - `!starts-with`: Does not start with
  - `=`: Equals
  - `contains`: Contains
  - `ends-with`: Ends with
  - `starts-with`: Starts with

- **query_name**
  
  Specifies the query name to match.
  
  `query_name` must be an alphanumeric string of 1 through 255 characters and may contain punctuation characters.
Usage
Use this command to define rule expressions to match query name in DNS request messages.

Example
The following command defines a rule expression to match DNS query name test:

```
    dns query-name = test
```
**dns return-code**

This command allows you to define rule expressions to match response code in DNS response messages.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

`active-charging service service_name > ruledef ruledef_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] dns return-code operator return_code
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `=`: Equals

- **return_code**
  Specifies the response code to match.
  `return_code` must be one of the following:
  - `format-error`
  - `name-error`
  - `no-error`
  - `not-implemented`
  - `refused`
  - `server-failure`

**Usage**
Use this command to define rule expressions to match response code in DNS response messages.

**Example**
The following command defines a rule expression to match a DNS response code `refused`:

```
dns return-code = refused
```
dns state

This command allows you to define rule expressions to match current state of DNS FSM.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acsl-ruledef)#

Syntax

[ no ] dns state operator dns_current_state

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be one of the following:
• !=: Does not equal
• ==: Equals

dns_current_state
Specifies the current state to match.
dns_current_state must be one of the following:
• dns-timeout
• init
• req-sent
• resp-error
• resp-success

Usage
Use this command to define rule expressions to match DNS FSM current state.

Example
The following command defines a rule expression to match DNS FSM current state of req-sent:

dns state = req-sent
**dns tid**

This command allows you to define rule expressions to match Transaction Identifier (TID) field in DNS messages.

**Product**  
ACS

**Privilege**  
Security Administrator, Administrator

**Mode**  
Exec > ACS Configuration > Ruledef Configuration

**Syntax**

```
[ no ] dns tid operator tid_value
```

- **no**  
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**  
  Specifies how to match.  
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `<=`: Lesser than or equals
  - `==`: Equals
  - `>=`: Greater than or equals

- **tid_value**  
  Specifies the DNS transaction identifier to match.  
  `tid_value` must be an integer from 1 through 65535.

**Usage**  
Use this command to define rule expressions to match a TID field of DNS messages.

**Example**

The following command defines a rule expression to match DNS TID field value of `test`:

```
dns tid = test
```
email

This command allows you to define rule expressions to match generic e-mail message parameters. These expressions will be applicable for IMAP, MMS, POP3, and SMTP protocols.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

`active-charging service service_name > ruledef ruledef_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acp-ruledef)#
```

**Syntax**

```
[ no ] email { cc | content { class | type } | from | size | subject | to } [ case-sensitive ] operator value
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **cc**
  Specifies to match the “cc” field of standard e-mail message.

- **content { class | type }**
  Specifies to match the “content-type” or “content-class” field of standard e-mail message.

- **from**
  Specifies to match the “from” field of standard e-mail message.

- **subject**
  Specifies to match the “subject” field of standard e-mail message.

- **to**
  Specifies to match the “to” field of standard e-mail message.

- **size**
  Specifies to match with the total size of e-mail message specified in bytes.

- **case-sensitive**
  Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.
email

operator

Specifies how to match.
operator must be one of the following except for size:

- !=: Does not equal
- !contains: Does not contain
- !ends-with: Does not end with
- !starts-with: Does not start with
- =: Equals
- contains: Contains
- ends-with: Ends with
- starts-with: Starts with

operator must be one of the following for size:

- !=: Does not equal
- <=: Lesser than or equals
- =: Equals
- >=: Greater than or equals

value

Specifies the value to match.
value must be an alphanumeric string and can contain punctuation characters.

- cc: A string of 1 through 512 characters
- content: A string of 1 through 128 characters
- from: A string of 1 through 64 characters
- size: A range of bytes from 1 through 4000000000 bytes
- subject: A string of 1 through 128 characters
- to: A string of 1 through 512 characters

Usage

Use this command to define rule expressions to match different fields/parameters within standard e-mail messages.

Example

The following command defines a rule expression to analyze user traffic for the occurrence of triangle in the “cc” field of e-mail messages:

```sql
email cc contains triangle@xyz.com
```
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Use this command to return to the parent configuration mode.
file-transfer any-match

This command allows you to define rule expressions to match all file-transfer packets. This expression applies to file transfers that use the FTP or HTTP protocols.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] file-transfer any-match operator condition

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be one of the following:
- !=: Does not equal
- ==: Equals

cconditio
Specifies the condition to match.
ccondition must be one of the following:
- FALSE
- TRUE

Usage
Use this command to define rule expressions to match all file-transfer packets. This expression applies to file transfers that use the FTP or HTTP protocols.

Example
The following command defines a rule expression to match all file-transfer packets:

    file-transfer any-match = TRUE
file-transfer chunk-number

This command allows you to define rule expressions to match the total number of chunks in an HTTP file as determined by the File Transfer analyzer.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] file-transfer chunk-number operator chunks_number
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  **operator** must be one of the following:
  - `!=`: Does not equal
  - `<=`: Lesser than or equals
  - `=`: Equals
  - `>=`: Greater than or equals

- **chunks_number**
  Specifies the number of chunks to match.
  **chunks_number** must be an integer from 1 through 65535.

**Usage**

Use this command to define rule expressions to match the total number of chunks in an HTTP file as determined by the File Transfer analyzer.

**Example**

The following command defines a rule expression to match 150 number of chunks:

```
file-transfer chunk-number = 150
```
file-transfer current-chunk-length

This command allows you to define rule expressions to match the length of an HTTP chunk currently in the File Transfer analyzer.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] file-transfer current-chunk-length operator current_chunk_length
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  - `!=`: Does not equal
  - `<=`: Lesser than or equals
  - `==`: Equals
  - `>=`: Greater than or equals

- **current_chunk_length**
  Specifies the current chunk length value (in bytes) to match.
  `current_chunk_length` must be an integer from 1 through 4000000.

**Usage**
Use this command to define rule expressions to match the length of an HTTP chunk currently in the File Transfer analyzer.

**Example**
The following command defines a rule expression to match length of current HTTP chunk as 1500000 bytes:

```
file-transfer current-chunk-length = 1500000
```
file-transfer declared-chunk-length

This command allows you to define rule expressions to match the declared length of an HTTP chunk currently in the File Transfer analyzer.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] file-transfer declared-chunk-length operator declared_chunk_length

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be one of the following:
- !=: Does not equal
- <=: Lesser than or equals
- ==: Equals
- >=: Greater than or equals

declared_chunk_length
Specifies the declared chunk length value (in bytes) to match.
declared_chunk_length must be an integer from 1 through 4000000.

Usage
Use this command to define rule expressions to match the declared length of an HTTP chunk currently in the File Transfer analyzer.

Example
The following command defines a rule expression to match declared length of the current HTTP chunk as 2500000 bytes:

file-transfer declared-chunk-length = 2500000
file-transfer declared-file-size

This command allows you to define rule expressions to match the declared file size by the File Transfer analyzer decoding the FTP handshake.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

Syntax

[ no ] file-transfer declared-file-size operator declared_file_size

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  - operator must be one of the following:
    - !=: Does not equal
    - <=: Lesser than or equals
    - ==: Equals
    - >=: Greater than or equals

- **declared_file_size**
  Specifies the declared file size (in bytes) to match.
  - declared_file_size must be an integer from 1 through 4000000.

Usage
Use this command to define rule expressions to match the declared file size by the File Transfer analyzer decoding the FTP handshake.

Example
The following command defines a rule expression to match declared file size as 2500000 bytes:

```
file-transfer declared-file-size = 2500000
```
file-transfer filename

This command allows you to define rule expressions to match file name.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

`active-charging service service_name > ruledef ruledef_name`

Entering the above command sequence results in the following prompt:

`[local]host_name(config-acs-ruledef)#`

**Syntax**

```
[ no ] file-transfer filename [ case-sensitive ] operator file_name
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **case-sensitive**
  Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

- **operator**
  Specifies how to match.
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `!contains`: Does not contain
  - `!ends-with`: Does not end with
  - `!starts-with`: Does not start with
  - `=`: Equals
  - `contains`: Contains
  - `ends-with`: Ends with
  - `starts-with`: Starts with

- **file_name**
  Specifies the file name to match.
  `file_name` must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters.
Usage
Use this command to define rule expressions to match file name in file-transfer.

Example
The following command defines a rule expression to match file name containing `star1`:

```
file-transfer filename contains star1
```
file-transfer previous-state

This command allows you to define rule expressions to match previous state of File Transfer FSM.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] file-transfer previous-state operator file_transfer_previous_state

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be one of the following:
• !=: Does not equal
• ==: Equals

file_transfer_previous_state
Specifies the previous state to match.
file_transfer_previous_state must be one of the following:
• init: Specifies previous state as initialization.
• request-sent: Specifies previous state as request sent.
• transfer-error: Specifies previous state as transfer error.
• transfer-ok: Specifies previous state as transfer ok.

Usage
Use this command to define rule expressions to match previous state of File Transfer FSM.

Example
The following command defines a rule expression to match previous state of init:

file-transfer previous-state = init
file-transfer state

This command allows you to define rule expressions to match the current state of File Transfer FSM.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] file-transfer state operator file_transfer_current_state

Syntax:

- `no` If previously configured, deletes the specified rule expression from the current ruledef.
- `operator` Specifies how to match. `operator` must be one of the following:
  - `!=`: Does not equal
  - `==`: Equals
- `file_transfer_current_state` Specifies the current state to match. `file_transfer_current_state` must be one of the following:
  - `init`: Specifies current state as initialization.
  - `request-sent`: Specifies current state as request sent.
  - `transfer-error`: Specifies current state as transfer error.
  - `transfer-ok`: Specifies current state as transfer ok.

Usage

Use this command to define rule expressions to match current state of File Transfer FSM.

The following table describes details of File Transfer FSM states with event:

<table>
<thead>
<tr>
<th>Event</th>
<th>init</th>
<th>request-sent</th>
<th>transfer-ok</th>
<th>transfer-err</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTP &quot;RETR&quot; command or HTTP &quot;GET&quot; request received with chunk encoding</td>
<td></td>
<td>request-sent</td>
<td>Discarded</td>
<td>Discarded</td>
</tr>
<tr>
<td>HTTP 2xx response received</td>
<td></td>
<td>transfer-ok</td>
<td>Discarded</td>
<td>Discarded</td>
</tr>
</tbody>
</table>
**file-transfer state**

<table>
<thead>
<tr>
<th>Event</th>
<th>init</th>
<th>request-sent</th>
<th>transfer-ok</th>
<th>transfer-err</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP 4xx or HTTP 5xx response received</td>
<td>transfer-error</td>
<td>Discarded</td>
<td>Discarded</td>
<td>Discarded</td>
</tr>
<tr>
<td>FTP reply received with reply status as file-transfer complete/successful</td>
<td>Discarded</td>
<td>transfer-ok</td>
<td>Discarded</td>
<td>Discarded</td>
</tr>
<tr>
<td>FTP reply received with reply status as file-transfer unsuccessful</td>
<td>Discarded</td>
<td>transfer-error</td>
<td>Discarded</td>
<td>Discarded</td>
</tr>
</tbody>
</table>

**Example**

The following command defines a rule expression to match file-transfer current state of `init`:

```
file-transfer state = init
```
file-transfer transferred-file-size

This command allows you to define rule expressions to match the size of a file that has been transferred so far, as detected by the File Transfer analyzer.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] file-transfer transferred-file-size operator transferred_file_size

<table>
<thead>
<tr>
<th>no</th>
</tr>
</thead>
<tbody>
<tr>
<td>If previously configured, deletes the specified rule expression from the current ruledef.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>operator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies how to match.</td>
</tr>
<tr>
<td>operator must be one of the following:</td>
</tr>
</tbody>
</table>

| • !=: Does not equal |
| • <=: Lesser than or equals |
| • :=: Equals |
| • =>: Greater than or equals |

<table>
<thead>
<tr>
<th>transferred_file_size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the transferred file size (in bytes) to match.</td>
</tr>
<tr>
<td>transferred_file_size must be an integer from 1 through 400000000.</td>
</tr>
</tbody>
</table>

Usage

Use this command to define rule expressions to match the size of the file that has been transferred so far, as detected by the File Transfer analyzer.

Example

The following command defines a rule expression to match file transferred size of 2500 bytes:

file-transfer transferred-file-size = 2500
ftp any-match

This command allows you to define rule expressions to match all FTP packets.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration
active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local] host_name(config-acs-ruledef) #

Syntax

[ no ] ftp any-match operator condition

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be one of the following:
- !=: Does not equal
- ==: Equals

condition
Specifies the condition to match.
condition must be one of the following:
- FALSE
- TRUE

Usage
Use this command to define a rule expression to match all FTP packets.

Example
The following command defines a rule expression to match all FTP packets:

ftp any-match = TRUE
**ftp client-ip-address**

This command allows you to define rule expressions to match IP address of the FTP client.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acis-ruledef)#
```

**Syntax**

```
[ no ] ftp client-ip-address operator ipv4/ipv6_address
```

<table>
<thead>
<tr>
<th><strong>no</strong></th>
<th>If previously configured, deletes the specified rule expression from the current ruledef.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>operator</strong></td>
<td>Specifies how to match. Developed as follows:</td>
</tr>
<tr>
<td></td>
<td>• !=: Does not equal</td>
</tr>
<tr>
<td></td>
<td>• &lt;=: Lesser than or equals</td>
</tr>
<tr>
<td></td>
<td>• ==: Equals</td>
</tr>
<tr>
<td></td>
<td>• &gt;=: Greater than or equals</td>
</tr>
</tbody>
</table>

| **ipv4/ipv6_address** | Specifies the FTP client IP address to match. IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation. |

**Usage**

Use this command to define rule expressions to match an FTP client IP address, which will be either the IP source address or the IP destination address, depending on the direction.

**Example**

The following command defines a rule expression to match client IP address 10.1.1.1:

```
ftp client-ip-address = 10.1.1.1
```
**ftp client-port**

This command allows you to define rule expressions to match port number of the FTP client.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```plaintext
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] ftp client-port operator port_number
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  ```plaintext
  operator must be one of the following:
  • !=: Does not equal
  • <=: Lesser than or equals
  • ==: Equals
  • >=: Greater than or equals
  ```

- **port_number**
  Specifies the client port number to match.
  ```plaintext
  port_number must be an integer from 1 through 65535.
  ```

**Usage**

Use this command to define rule expressions to match port number of the FTP client, which will be either the TCP source port or the TCP destination port, depending on the direction.

**Example**

The following command defines a rule expression to match FTP client port number 10:

```
ftp client-port = 10
```
ftp command args

This command allows you to define rule expressions to match arguments within an FTP command.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] ftp command args [ case-sensitive ] operator argument

---

no
If previously configured, deletes the specified rule expression from the current ruledef.

---

case-sensitive
Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

---

operator
Specifies how to match.
operator must be one of the following:

• !=: Does not equal
• !contains: Does not contain
• !ends-with: Does not end with
• !starts-with: Does not start with
• ==: Equals
• contains: Contains
• ends-with: Ends with
• starts-with: Starts with

---

argument
Specifies the argument to match.
argument must be an alphanumeric string of 1 through 127 characters.

---

Usage

Use this command to define rule expressions to match arguments within an FTP command.
Example

The following command defines a rule expression to match argument *ascii* within an FTP command:

```plaintext
ftp command args = ascii
```
**ftp command id**

This command allows you to define rule expressions to match FTP command ID.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
```
Exec > ACS Configuration > Ruledef Configuration
```

**active-charging service service_name > ruledef ruledef_name**

Entering the above command sequence results in the following prompt:
```
[local]host_name(config-acs-ruledef)#
```

**Syntax**
```
[ no ] ftp command id operator command_id
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  `operator` must be one of the following:
  - !=: Does not equal
  - <=: Lesser than or equals
  - ==: Equals
  - >=: Greater than or equals

- **command_id**
  Specifies the command identifier to match.
  In 8.3 and earlier releases, `command_id` must be an integer from 0 through 15.
  In 9.0 and later releases, `command_id` must be an integer from 0 through 18.

**Usage**
Use this command to define rule expressions to match FTP command ID.

**Example**
The following command defines a rule expression to match the FTP command ID 10:
```
ftp command id = 10
```
ftp command name

This command allows you to define rule expressions to match FTP command name.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] ftp command name operator command_name

- **no**
  - If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  - Specifies how to match.
  - **operator** must be one of the following:
    - !=: Does not equal
    - ==: Equals

- **command_name**
  - Specifies the command name to match.
  - **command_name** must be one of the following:
    - abor: Abort command
    - cwd: Current working directory command
    - eprt: eprt command
    - epsv: epsv command
    - list: List command
    - mode: Transfer mode command
    - pass: Password command
    - pasv: Passive command
    - port: Port command
    - quit: Quit command
    - rest: Restore command
    - retr: Retry command
 ACS Ruledef Configuration Mode Commands

ftp command name

- **stor**: Store command
- **stru**: File structure command
- **syst**: System command
- **type**: Type command
- **user**: User command

Usage
Use this command to define rule expressions to match FTP command name.

Example
The following command defines a rule expression to match FTP command name **list**:

```plaintext
ftp command name = list
```
ftp connection-type

This command allows you to define rule expressions to match FTP connection type.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] ftp connection-type operator connection_type

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be one of the following:

• !=: Does not equal
• <=: Lesser than or equals
• ==: Equals
• >=: Greater than or equals

connection_type
Specifies the connection type to match.
connection_type must be one of the following:

• 0: Unknown
• 1: Control connection
• 2: Data connection

Usage
Use this command to define rule expressions to match an FTP connection type.

Example

The following command defines a rule expression to match FTP connection type 1:

ftp connection-type = 1
**ftp data-any-match**

This command allows you to define rule expressions to match all FTP data packets.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

`active-charging service service_name > ruledef ruledef_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acruledef)#
```

**Syntax**

```
[ no ] ftp data-any-match operator condition
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `=`: Equals

- **condition**
  Specifies the condition to match.
  `condition` must be one of the following:
  - `FALSE`
  - `TRUE`

**Usage**
Use this command to define rule expressions to match all FTP data packets.

**Example**
The following command defines a rule expression to match all FTP data packets:

```
ftp data-any-match = TRUE
```
ftp filename

This command allows you to define rule expressions to match FTP file name.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

`active-charging service service_name > ruledef ruledef_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] ftp filename [ case-sensitive ] operator file_name
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **case-sensitive**
  Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

- **operator**
  Specifies how to match.
  `operator` must be one of the following:
  
  - `!=`: Does not equal
  - `!contains`: Does not contain
  - `!ends-with`: Does not end with
  - `!starts-with`: Does not start with
  - `=`: Equals
  - `contains`: Contains
  - `ends-with`: Ends with
  - `starts-with`: Starts with

- **file_name**
  Specifies the file name to match.
  `file_name` must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters.
Usage

Use this command to define rule expressions to match an FTP file name.

Example

The following command defines a rule expression to match a file named testtransfer:

```plaintext
ftp filename = testtransfer
```
**ftp pdu-length**

This command allows you to define rule expressions to match the length of a current FTP packet.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] ftp pdu-length operator pdu_length
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `<=`: Lesser than or equals
  - `==`: Equals
  - `>=`: Greater than or equals

- **pdu_length**
  Specifies the FTP PDU length (in bytes) to match.
  `pdu_length` must be an integer from 0 through 65535.

**Usage**

Use this command to define rule expressions to match the length of a current FTP packet, that is, FTP PDU length (FTP header + FTP payload).

**Example**

The following command defines a rule expression to match an FTP PDU length of 9647 bytes:

```
ftp pdu-length = 9647
```
**ftp pdu-type**

This command allows you to define rule expressions to match FTP Protocol Data Unit (PDU) type.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

`active-charging service service_name > ruledef ruledef_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] ftp pdu-type operator pdu_type
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `<=`: Lesser than or equals
  - `==`: Equals
  - `>=`: Greater than or equals

- **pdu_type**
  Specifies the PDU type to match.
  `pdu_type` must be one of the following:
  - `0`: Unknown
  - `1`: Command
  - `2`: Reply

**Usage**

Use this command to define rule expressions to match a PDU type of FTP packet.

**Example**

The following command defines a rule expression to match FTP PDU type 1:

```
ftp pdu-type = 1
```
ftp previous-state

This command allows you to define rule expressions to match previous state of FTP session.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] ftp previous-state operator ftp_previous_state

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be one of the following:
- !=: Does not equal
- ==: Equals

ftp_previous_state
Specifies the previous state to match.
ftp_previous_state must be one of the following:
- command-sent
- init
- response-error
- response-ok

Usage
Use this command to define rule expressions to match a previous state of FTP session.

Example
The following command defines a rule expression to match previous FTP state init:

ftp previous-state = init
**ftp reply code**

This command allows you to define rule expressions to match FTP reply code.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acd-ruledef)#
```

**Syntax**

```
[ no ] ftp reply code operator reply_code
```

- **no**
  - If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  - Specifies how to match.
  - `operator` must be one of the following:
    - `!=`: Does not equal
    - `<=`: Lesser than or equals
    - `=:` Equals
    - `>=`: Greater than or equals

- **reply_code**
  - Specifies the FTP reply code to match.
  - `reply_code` must be an integer from 100 through 599.

**Usage**

Use this command to define rule expressions to match an FTP reply code.

**Example**

The following command defines a rule expression to match FTP reply code 150:

```
ftp reply code = 150
```
**ftp server-ip-address**

This command allows you to define rule expressions to match FTP server IP address.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

`active-charging service service_name > ruledef ruledef_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] ftp server-ip-address operator ipv4/ipv6_address
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `<=`: Lesser than or equals
  - `==`: Equals
  - `>=`: Greater than or equals

- **ipv4/ipv6_address**
  Specifies IP address of the server to match
  `ipv4/ipv6_address` must be in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

**Usage**
Use this command to define rule expressions to match an FTP server IP address, which will be either the IP source address or the IP destination address, depending on the direction.

**Example**
The following command defines a rule expression to match the FTP server IP address `10.1.1.1`:

```
ftp server-ip-address = 10.1.1.1
```
ftp server-port

This command allows you to define rule expressions to match FTP server port number.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] ftp server-port operator port

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.

operator must be one of the following:

- !=: Does not equal
- <=: Lesser than or equals
- =: Equals
- >=: Greater than or equals

port

Specifies the FTP server port number to match.

port must be an integer from 1 through 65535.

Usage

Use this command to define rule expressions to match an FTP server port number, which will be either the TCP source port or the TCP destination port, depending on the direction.

Example

The following command defines a rule expression to analyze user traffic for FTP server port 21:

    ftp server-port = 21
**ftp session-length**

This command allows you to define rule expressions to match the total number of bytes sent on an FTP control connection.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] ftp session-length operator session_length
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  **operator** must be one of the following:
  - !=: Does not equal
  - <=: Lesser than or equals
  - =: Equals
  - >=: Greater than or equals

- **session_length**
  Specifies the FTP session length (in bytes) to match.
  **session_length** must be an integer from 1 through 400000000.

**Usage**
Use this command to define rule expressions to match the total number of bytes sent on an FTP control connection.

**Example**

The following command defines a rule expression to match FTP session length of 40000 bytes:

```
ftp session-length = 40000
```
**ftp state**

This command allows you to define rule expressions to match the current state of an FTP session.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] ftp state operator ftp_state
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `==`: Equals

- **ftp_state**
  Specifies the FTP state to match.
  `ftp_state` must be one of the following:
  - `close`: FTP transmissions that are in closed state.
  - `command-sent`: FTP transmissions that are in command-sent state.
  - `response-error`: FTP transmissions that are in response-error state.
  - `response-ok`: FTP transmissions that are in response-ok state.

**Usage**

Use this command to define rule expressions to match the current state of an FTP session.

**Example**

The following command defines a rule expression to match FTP current state `close`:

```
ftp state = close
```
ftp url

This command allows you to define rule expressions to match the FTP URL/path of a file being transferred.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] ftp url [ case-sensitive ] operator url

no
If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive
Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator
Specifies how to match.
operator must be one of the following:
• !=: Does not equal
• !contains: Does not contain
• !ends-with: Does not end with
• !starts-with: Does not start with
• =: Equals
• contains: Contains
• ends-with: Ends with
• starts-with: Starts with

url
Specifies the URL to match.
url must be an alphanumeric string of 1 through 127 characters.

Usage
Use this command to define rule expressions to match the FTP URL/path of a file being transferred.
Example

The following command defines a rule expression to match the URL ftp://rfc.ietf.org/rfc/rfc1738.txt:

    ftp url = ftp://rfc.ietf.org/rfc/rfc1738.txt
**ftp user**

This command allows you to define rule expressions to match the user name FTP command packet.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```cisco
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] ftp user [ case-sensitive ] operator ftp_user
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **case-sensitive**
  Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

- **operator**
  Specifies how to match.
  ```
  operator must be one of the following:
  • !=: Does not equal
  • !=contains: Does not contain
  • !=ends-with: Does not end with
  • !=starts-with: Does not start with
  • =: Equals
  • contains: Contains
  • ends-with: Ends with
  • starts-with: Starts with
  ```

- **ftp_user**
  Specifies the FTP user name to match.
  ```
  ftp_user must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters.
  ```
Usage
Use this command to define rule expressions to match a user name FTP command.

Example
The following command defines a rule expression to match FTP user name user1:

```
ftp user = user1
```
http any-match

This command allows you to define rule expressions to match all HTTP and HTTPS Connect Method packets.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

Example
The following command defines a rule expression to match all HTTP packets:

    http any-match = TRUE

Syntax

[ no ] http any-match operator condition

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  * operator must be one of the following:
    - !=: Does not equal
    - =: Equals

- **condition**
  Specifies the condition to match.
  * condition must be one of the following:
    - FALSE
    - TRUE

Usage
Use this command to define rule expressions to match all HTTP packets.
http attribute-in-data

This command allows you to define rule expressions to match any arbitrary attribute in the payload following the HTTP headers.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **attribute**
  *attribute* must be an alphanumeric string of 1 through 31 characters.

- **case-sensitive**
  Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

- **operator**
  Specifies how to match.
  *operator* must be one of the following:
  - !=: Does not equal
  - !contains: Does not contain
  - !ends-with: Does not end with
  - !starts-with: Does not start with
  - ==: Equals
  - contains: Contains
  - ends-with: Ends with
  - starts-with: Starts with

- **value**
  Specifies the value as an alphanumeric string of 1 through 127 characters.
Usage

Use this command to define rule expressions to match arbitrary attribute in the payload following the HTTP headers.
In 14.0 and later releases, the ECS HTTP analyzer supports both CRLF and LF as valid terminators for HTTP header fields.
http attribute-in-url

This command allows you to define rule expressions to match arbitrary attribute in the combined Host+URI HTTP headers.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax


<table>
<thead>
<tr>
<th>no</th>
</tr>
</thead>
<tbody>
<tr>
<td>If previously configured, deletes the specified rule expression from the current ruledef.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>attribute must be an alphanumeric string of 1 through 31 characters.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>case-sensitive</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>operator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies how to match. operator must be one of the following:</td>
</tr>
<tr>
<td>• !=: Does not equal</td>
</tr>
<tr>
<td>• !contains: Does not contain</td>
</tr>
<tr>
<td>• !ends-with: Does not end with</td>
</tr>
<tr>
<td>• !starts-with: Does not start with</td>
</tr>
<tr>
<td>• =: Equals</td>
</tr>
<tr>
<td>• contains: Contains</td>
</tr>
<tr>
<td>• ends-with: Ends with</td>
</tr>
<tr>
<td>• starts-with: Starts with</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the value as an alphanumeric string of 1 through 127 characters.</td>
</tr>
</tbody>
</table>
**http attribute-in-url**

**Usage**

Use this command to configure rule expression to match an arbitrary attribute in the combined Host+URI HTTP headers.

In 14.0 and later releases, the ECS HTTP analyzer supports both CRLF and LF as valid terminators for HTTP header fields.
http content disposition

This command allows you to define rule expressions to match optional content-disposition field of HTTP entity header.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] http content disposition [ case-sensitive ] operator content_disposition
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **case-sensitive**
  Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

- **operator**
  Specifies how to match.
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `!contains`: Does not contain
  - `!ends-with`: Does not end with
  - `!starts-with`: Does not start with
  - `=`: Equals
  - `contains`: Contains
  - `ends-with`: Ends with
  - `starts-with`: Starts with

- **content_disposition**
  This field offers a mechanism for the sender to transmit presentational information to the recipient, allowing each component of a message to be tagged with an indication of its desired presentation semantics.
  `content_disposition` must be an alphanumerics string of 1 through 127 characters, and may contain punctuation characters.
Usage

Use this command to define rule expressions to match optional content-disposition field of HTTP entity header. This feature supports RFC 2616 for HTTP and RFC 1806 for Content Disposition.
In 14.0 and later releases, the ECS HTTP analyzer supports both CRLF and LF as valid terminators for HTTP header fields.

Example

The following command defines a rule expression to match content disposition `successful`:

```
http content disposition = successful
```
http content length

This command allows you to define rule expressions to match the value in HTTP Content-Length entity-header field.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] http content length operator content_length

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be one of the following:

• !=: Does not equal
• <=: Lesser than or equals
• ==: Equals
• >=: Greater than or equals

content_length
Specifies the HTTP body length (in bytes) to match.
content_length must be an integer from 1 through 4000000000.

Usage
Use this command to define rule expressions to match value in HTTP Content-Length entity-header field.
In 14.0 and later releases, the ECS HTTP analyzer supports both CRLF and LF as valid terminators for HTTP header fields.

Example
The following command defines a rule expression to match value of 10000 bytes in HTTP Content-Length entity-header field:

http content length = 10000
**http content type**

This command allows you to define rule expressions to match value in HTTP Content-Type entity-header field.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] http content type [ case-sensitive ] operator content_type
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **case-sensitive**
  Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

- **operator**
  Specifies how to match.

  - **operator** must be one of the following:
    - `!=`: Does not equal
    - `!contains`: Does not contain
    - `!ends-with`: Does not end with
    - `!starts-with`: Does not start with
    - `=`: Equals
    - `contains`: Contains
    - `ends-with`: Ends with
    - `starts-with`: Starts with

- **content_type**
  Specifies the content type to match.

  - **content_type** must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters.
Usage
Use this command to define rule expressions to match value in HTTP Content-Type entity-header field. In 14.0 and later releases, the ECS HTTP analyzer supports both CRLF and LF as valid terminators for HTTP header fields.

Example
The following command defines a rule expression to match abc100 in HTTP Content-Type entity-header field:

```
http content type = abc100
```
http cookie

This command allows you to define rule expressions to match strings in the HTTP cookie header.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] http cookie [ case-sensitive ] operator cookie_string

no

If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator

Specifies how to match.
operator must be one of the following:
- !=: Does not equal
- !contains: Does not contain
- !ends-with: Does not end with
- !starts-with: Does not start with
- =: Equals
- contains: Contains
- ends-with: Ends with
- starts-with: Starts with

cookie_string

Specifies the string to match in the HTTP cookie header.
cookie_string must be an alphanumeric string of 1 through 127 characters.

Usage

Use this command to define rule expressions to match strings in an HTTP cookie header.
The cookie match ruleline can be combined with other rulelines having different match criteria. Multiple line cookie header strings can be combined together using a comma (,) separator.

**Important:** The HTTP parser can parse up to a maximum of 4096 bytes in the cookie header. In the case of multiple line cookie headers, the maximum of 4096 bytes includes the total size of all cookie header values, and the separators added to combine them.

**Example**

The following command defines a rule expression to match the HTTP cookie header with the string `tollfree`:

```
http cookie = tollfree
```
**http domain**

This command allows you to define rule expressions to match the domain portion of URIs in HTTP packets.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] http domain [ case-sensitive ] operator domain
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **case-sensitive**
  Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

- **operator**
  Specifies how to match.
  - operator must be one of the following:
    - !=: Does not equal
    - !contains: Does not contain
    - !ends-with: Does not end with
    - !starts-with: Does not start with
    - ==: Equals
    - contains: Contains
    - ends-with: Ends with
    - starts-with: Starts with

- **domain**
  Specifies the domain to match.
  - domain must be an alphanumeric string of 1 through 127 characters.

**Usage**

Use this command to define rule expressions to match the domain portion of URIs in HTTP packets.
From the URL, after http:// (if present) is removed, everything until the first "/" is the domain.

The following command defines a rule expression to match user traffic based on domain name testdomain:

```
http domain = testdomain
```
http error

This command allows you to define rule expressions to match for errors in HTTP packets (for example, invalid HTTP header) and errors in the HTTP analyzer FSM (Finite State Machine) while parsing HTTP packets.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs-ruledef) #
```

**Syntax**

```
[ no ] http error operator condition
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `==`: Equals

- **condition**
  Specifies the condition to match.
  `condition` must be one of the following:
  - `FALSE`
  - `TRUE`

**Usage**

Use this command to define rule expressions to match for errors in HTTP packets and other errors in HTTP analyzer FSM while parsing HTTP packets. For example, FSM error, invalid header field values, ACS memory and buffer limit, packet related errors, and so on.

ACS supports pipelining of up to 32 HTTP requests on the same TCP connection. Pipeline overflow requests are not analyzed. Such overflow requests are treated as HTTP error. The billing system, based on this information, decides to charge or not charge, or refund the subscriber accordingly.

In 14.0 and later releases, the ECS HTTP analyzer supports both CRLF and LF as valid terminators for HTTP header fields.

**Example**

The following command defines a rule expression to match user traffic based on HTTP error status of `TRUE`:
http error = TRUE
http first-request-packet

This command allows you to define rule expressions to match the GET or POST request, if it is the first HTTP request for the subscriber's session.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] http first-request-packet operator condition
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  
  **operator** must be one of the following:
  - ```!=```: Does not equal
  - ```==```: Equals

- **condition**
  Specifies the condition to match.
  
  **condition** must be one of the following:
  - ```FALSE```
  - ```TRUE```

**Usage**

Use this command to define rule expressions to match the GET or POST request, if it is the first HTTP request for the subscriber's session.

This expression can be connected with a charging action, so the subscriber is redirected to a splash page for the first Web access attempted.

**Example**

The following command defines a rule expression to match first-request-packet:

```
http first-request-packet = TRUE
```
http header-length

This command allows you to define rule expressions to match HTTP header length.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] http header-length operator header_length

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:
• !=: Does not equal
• <=: Lesser than or equals
• =: Equals
• >=: Greater than or equals

header_length

Specifies the HTTP header length (in bytes) to match.
header_length must be an integer from 0 through 65535.

Usage

Use this command to define rule expressions to match the length of an HTTP header.
In 14.0 and later releases, the ECS HTTP analyzer supports both CRLF and LF as valid terminators for HTTP header fields.

Example

The following command defines a rule expression to match an HTTP header length of 8000:

    http header-length = 8000
http host

This command allows you to define rule expressions to match value in HTTP Host request-header field.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] http host [ case-sensitive ] operator host_name

---

no

If previously configured, deletes the specified rule expression from the current ruledef.

---

case-sensitive

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

---

operator

Specifies how to match.

operator must be one of the following:

• !=: Does not equal
• !contains: Does not contain
• !ends-with: Does not end with
• !starts-with: Does not start with
• ==: Equals
• contains: Contains
• ends-with: Ends with
• regex: Regular expression
• starts-with: Starts with

---

host_name

Specifies the host name to match.

host_name must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters.
**Usage**

Use this command to define rule expressions to match value in HTTP Host request-header field.

In 14.0 and later releases, the ECS HTTP analyzer supports both CRLF and LF as valid terminators for HTTP header fields.

The following table lists the special characters that you can use in regex rule expressions. For more information on regex support, refer to the *Enhanced Charging Service Administration Guide*.

<table>
<thead>
<tr>
<th>Regex Character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Zero or more characters</td>
</tr>
<tr>
<td>+</td>
<td>Zero or more repeated instances of the token preceding the +</td>
</tr>
<tr>
<td>?</td>
<td>Match zero or one character</td>
</tr>
</tbody>
</table>

**Important:** The CLI does not support configuring “?” directly, you must instead use “\077”.

For example, if you want to match the string “xyz<any one character>pqr”, you must configure it as:

```
http host regex "xyz\077pqr"
```

In another example, if you want to exactly match the string “url?resource=abc”, you must configure it as:

```
http uri regex "url\077resource=abc"
```

Where, the first “\” (backslash) is for the escaping of “?” and then “\077” for specifying “?” to the CLI.

<table>
<thead>
<tr>
<th>\character</th>
<th>Escaped character</th>
</tr>
</thead>
<tbody>
<tr>
<td>?</td>
<td>Match the question mark (&lt;ctrl-v&gt;?)</td>
</tr>
<tr>
<td>+</td>
<td>Match the plus character</td>
</tr>
<tr>
<td>*</td>
<td>Match the asterisk character</td>
</tr>
<tr>
<td>\a</td>
<td>Match the Alert (ASCII 7) character</td>
</tr>
<tr>
<td>\b</td>
<td>Match the Backspace (ASCII 8) character</td>
</tr>
<tr>
<td>\f</td>
<td>Match the Form-feed (ASCII 12) character</td>
</tr>
<tr>
<td>\n</td>
<td>Match the New line (ASCII 10) character</td>
</tr>
<tr>
<td>\r</td>
<td>Match the Carriage return (ASCII 13) character</td>
</tr>
<tr>
<td>\t</td>
<td>Match the Tab (ASCII 9) character</td>
</tr>
<tr>
<td>\v</td>
<td>Match the Vertical tab (ASCII 11) character</td>
</tr>
<tr>
<td>\0</td>
<td>Match the Null (ASCII 0) character</td>
</tr>
<tr>
<td>\</td>
<td>Match the backslash character</td>
</tr>
</tbody>
</table>
| [0-9]      | Bracketed range
| ^          | Do not match any in the range. All other characters represent themselves. |
### http host

<table>
<thead>
<tr>
<th>Regex Character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>\x##</td>
<td>Any ASCII character as specified in two-digit hex notation. For example, \x5A yields a “Z”.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Important**: When using the regex operator “|” in regex expressions, always wrap the string in double quotes.

For example, if you want to match the string "pqr" OR "xyz", you must configure it as:

```plaintext
http host regex "pqr|xyz"
```

### Example

The following command defines a rule expression to match `host1` in HTTP Host request-header field:

```plaintext
http host = host1
```

The following command defines a regex rule expression to match either of the following values in the HTTP Host request-header field: `host1`, `host23w01`.

```plaintext
http host regex "host1|host23w01"
```
http payload-length

This command allows you to define rule expressions to match HTTP payload length.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > ACS Configuration > Ruledef Configuration

`active-charging service service_name > ruledef ruledef_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] http payload-length operator payload_length
```

- **no**
  
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  
  Specifies how to match. `operator` must be one of the following:
  - `!=`: Does not equal
  - `<=`: Lesser than or equals
  - `=`: Equals
  - `>=`: Greater than or equals

- **payload_length**
  
  Specifies the HTTP payload (data) length (in bytes) to match. `payload_length` must be an integer from 1 through 400000000.

**Usage**

Use this command to define rule expressions to match HTTP payload (data) length (pdu-length - header-length).

**Example**

The following command defines a rule expression to match HTTP payload length of 100000 bytes:

```
http payload-length = 100000
```
**http pdu-length**

This command allows you to define rule expressions to match the total length of a single HTTP packet.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] http pdu-length operator pdu_length
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  `operator` must be one of the following:
  ```
  • !=: Does not equal
  • <=: Lesser than or equals
  • ==: Equals
  • >=: Greater than or equals
  ```

- **pdu_length**
  Specifies the HTTP PDU length (in bytes) to match.
  `pdu_length` must be an integer from 0 through 65535.

**Usage**

Use this command to define rule expressions to match the total length of a single HTTP packet. This will also match packets with partial HTTP message (due to fragmentation).

**Example**

The following command defines a rule expression to match an HTTP PDU length of 10000 bytes:

```
http pdu-length = 10000
```
http previous-state

This command allows you to define rule expressions to match previous state of HTTP sessions.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] http previous-state operator http_previous_state

- no
  If previously configured, deletes the specified rule expression from the current ruledef.

- operator
  Specifies how to match.
  operator must be one of the following:
  - !=: Does not equal
  - ==: Equals

- http_previous_state
  Specifies the previous state to match.
  http_previous_state must be one of the following:
  - init: Initialized state
  - response-error: Response error state
  - response-ok: Response ok state
  - waiting-for-response: Waiting for response state

Usage

Use this command to define rule expressions to match a previous state of HTTP sessions.

Example

The following command defines a rule expression to match HTTP previous state response-ok:

    http previous-state = response-ok
http referer

This command allows you to define rule expressions to match the value in the HTTP Referer request-header field.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] http referer [ case-sensitive ] operator referer_name

no
If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive
Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator
Specifies how to match.
operator must be one of the following:
- !: Does not equal
- !contains: Does not contain
- !ends-with: Does not end with
- !starts-with: Does not start with
- =: Equals
- contains: Contains
- ends-with: Ends with
- regex: Regular expression
- starts-with: Starts with

referer_name
Specifies the HTTP referer name to match.
referer_name must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters.
Usage

Use this command to define rule expressions to match value in HTTP Referer request-header field. This feature allows an operator to collect or track all URLs visited during a particular subscriber session. These URLs include the entire string of visited URLs, including all referral links. This information is output in an Event Data Record (EDR) format to support reporting or billing functions.

For example, if a subscriber begins a mobile web session and clicks on the “Sports” link from the home deck, and then selects ESPN and moves to an advertiser link, the operator can capture all URLs for that entire session. During this period ACS collects the URLs for a particular subscriber session; collection can be limited by time duration or number of URLs visited.

ACS generates EDRs that contain HTTP URL and the HTTP referer fields along with other fields. In 14.0 and later releases, the ECS HTTP analyzer supports both CRLF and LF as valid terminators for HTTP header fields.

The following table lists the special characters that you can use in regex rule expressions. For more information on regex support, refer to the Enhanced Charging Service Administration Guide.

<table>
<thead>
<tr>
<th>Regex Character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Zero or more characters</td>
</tr>
<tr>
<td>+</td>
<td>Zero or more repeated instances of the token preceding the +</td>
</tr>
<tr>
<td>?</td>
<td>Match zero or one character</td>
</tr>
</tbody>
</table>

**Important:** The CLI does not support configuring “?” directly, you must instead use “\077”.

For example, if you want to match the string “xyz<any one character>pqr”, you must configure it as:

```
http host regex "xyz\077pqr"
```

In another example, if you want to exactly match the string “url?resource=abc”, you must configure it as:

```
http uri regex "url\077resource=abc"
```

Where, the first “\” (backslash) is for the escaping of “?” and then “\077” for specifying “?” to the CLI.

<table>
<thead>
<tr>
<th>\character</th>
<th>Escaped character</th>
</tr>
</thead>
<tbody>
<tr>
<td>?</td>
<td>Match the question mark (&lt;ctrl-v&gt;?) character</td>
</tr>
<tr>
<td>+</td>
<td>Match the plus character</td>
</tr>
<tr>
<td>*</td>
<td>Match the asterisk character</td>
</tr>
<tr>
<td>\a</td>
<td>Match the Alert (ASCII 7) character</td>
</tr>
<tr>
<td>\b</td>
<td>Match the Backspace (ASCII 8) character</td>
</tr>
<tr>
<td>\f</td>
<td>Match the Form-feed (ASCII 12) character</td>
</tr>
<tr>
<td>\n</td>
<td>Match the New line (ASCII 10) character</td>
</tr>
<tr>
<td>\r</td>
<td>Match the Carriage return (ASCII 13) character</td>
</tr>
<tr>
<td>\t</td>
<td>Match the Tab (ASCII 9) character</td>
</tr>
<tr>
<td>\v</td>
<td>Match the Vertical tab (ASCII 11) character</td>
</tr>
<tr>
<td>\0</td>
<td>Match the Null (ASCII 0) character</td>
</tr>
</tbody>
</table>
## ACS Ruledef Configuration Mode Commands

### http referer

<table>
<thead>
<tr>
<th>Regex Character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>\</td>
<td>Match the backslash character</td>
</tr>
<tr>
<td>Bracketed range [0-9]</td>
<td>Match any single character from the range</td>
</tr>
<tr>
<td>A leading ^ in a range</td>
<td>Do not match any in the range. All other characters represent themselves.</td>
</tr>
<tr>
<td>\x##</td>
<td>Any ASCII character as specified in two-digit hex notation. For example, \x5A yields a “Z”.</td>
</tr>
<tr>
<td></td>
<td>Specify OR regular expression operator</td>
</tr>
</tbody>
</table>

**Important:** When using the regex operator “|” in regex expressions, always wrap the string in double quotes.

For example, if you want to match the string "pqr" OR “xyz”, you must configure it as:

```plaintext
http host regex "pqr|xyz".
```

### Example

The following command defines a rule expression to match the HTTP referer `cricket.espn.com`:

```plaintext
http referer = cricket.espn.com
```
http reply code

This command allows you to define rule expressions to match status code associated with HTTP response packets.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] http reply code operator reply_code
```

- **no**
  - If previously configured, deletes the specified rule expression from the current ruledef.
- **operator**
  - Specifies how to match.
  - `operator` must be one of the following:
    - `!=`: Does not equal
    - `<=`: Lesser than or equals
    - `==`: Equals
    - `>=`: Greater than or equals
- **reply_code**
  - Specifies the HTTP reply code to match.
  - `reply_code` must be an integer from 100 through 599.

**Usage**

Use this command to define rule expressions to match status code associated with HTTP response codes.

**Example**

The following command defines a rule expression to match HTTP response code 204:

```
http reply code = 204
```
http request method

This command allows you to define rule expressions to match HTTP request method.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] http request method operator request_method

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be one of the following:
• !=: Does not equal
• ==: Equals

request_method
Specifies the HTTP request method to match.
request_method must be one of the following:
• connect
• delete
• get
• head
• options
• post
• put
• trace

Usage
Use this command to define rule expressions to match an HTTP request method.

Example
The following command defines a rule expression to match user traffic based on HTTP request method `connect`:

```
http request method = connect
```
http session-length

This command allows you to define rule expressions to match HTTP session length.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```bash
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] http session-length operator session_length
```

- **no**
  - If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  - Specifies how to match.
  - `operator` must be one of the following:
    - `!=`: Does not equal
    - `<=`: Lesser than or equals
    - `==`: Equals
    - `>=`: Greater than or equals

- **session_length**
  - Specifies the HTTP total session length (in bytes) to match.
  - `session_length` must be an integer from 1 through 400000000.

**Usage**

Use this command to define rule expressions to match a total HTTP session length.

**Example**

The following command defines a rule expression to match an HTTP session length of **200000**:

```
http session-length = 200000
```
http state

This command allows you to define rule expressions to match current state of an HTTP session.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] http state operator current_state

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be one of the following:
• !=: Does not equal
• ==: Equals

current_state
Specifies the current state of HTTP session to match.
current_state must be one of the following:
• close: Closed state
• response-error: Response error state
• response-ok: Response ok state
• waiting-for-response: Waiting for response state

Usage
Use this command to define rule expressions to match a current state of an HTTP session.

Example
The following command defines a rule expression to match current state close:

http state = close
http transaction-length

This command allows you to define rule expressions to match HTTP transaction length (combined length of one HTTP GET Request message and its associated response messages).

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] http transaction-length { operator transaction_length | { range | !range } range_from to range_to } }

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be one of the following:
- !=: Does not equal
- <=: Lesser than or equals
- ==: Equals
- >=: Greater than or equals

transaction_length
Specifies the HTTP transaction length (in bytes) to match.
transaction_length must be an integer from 1 through 4000000000.

{ range | !range } range_from to range_to
Enables or disables the range criteria for length of transaction.
- range: Enables the range criteria for HTTP transaction length.
- !range: Disables the range criteria for HTTP transaction length.
- range_from: Specifies the start of range (in bytes) for HTTP transaction length.
- range_to: Specifies the end of range (in bytes) for HTTP transaction length.
Use this command to define rule expressions to match an HTTP transaction length [one HTTP GET Request message + associated response message(s)] in bytes.

Example

The following command defines a rule expression to match an HTTP transaction length of 10200 bytes:

```
http transaction-length = 10200
```
http transfer-encoding

This command allows you to define rule expressions to match the value in HTTP Transfer-Encoding general-header field.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[llocal]host_name(config-acs-ruledef)#

Syntax

[ no ] http transfer-encoding [ case-sensitive ] operator transfer_encoding

no
If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive
Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator
Specifies how to match.
operator must be one of the following:

- !=: Does not equal
- !contains: Does not contain
- !ends-with: Does not end with
- !starts-with: Does not start with
- =: Equals
- contains: Contains
- ends-with: Ends with
- starts-with: Starts with

transfer_encoding
Specifies the HTTP transfer encoding to match.
transfer_encoding must be an alphanumeric string of 1 through 127 characters, and may contain punctuation characters.
Usage

Use this command to define rule expressions to match the value in HTTP Transfer-Encoding general-header field.
In 14.0 and later releases, the ECS HTTP analyzer supports both CRLF and LF as valid terminators for HTTP header fields.

Example

The following command defines a rule expression to match the value \texttt{chunked} in HTTP Transfer-Encoding general-header field:

\texttt{http transfer-encoding = chunked}
http uri

This command allows you to define rule expressions to match HTTP URI.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > ACS Configuration > Ruledef Configuration

`active-charging service service_name > ruledef ruledef_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] http uri [ case-sensitive ] operator uri
```

---

**no**

If previously configured, deletes the specified rule expression from the current ruledef.

---

**case-sensitive**

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

---

**operator**

Specifies how to match.

- `operator` must be one of the following:
  - `!=`: Does not equal
  - `!contains`: Does not contain
  - `!ends-with`: Does not end with
  - `!starts-with`: Does not start with
  - `=`: Equals
  - `contains`: Contains
  - `ends-with`: Ends with
  - `regex`: Regular expression
  - `starts-with`: Starts with

---

**uri**

Specifies the HTTP URI to match.

- `uri` must be an alphanumeric string of 1 through 127 characters, and can contain punctuation characters, and excludes the “host” portion.
Usage

Use this command to define rule expressions to match an HTTP URI, excluding the host portion. The following table lists the special characters that you can use in regex rule expressions. For more information on regex support, refer to the Enhanced Charging Service Administration Guide.

<table>
<thead>
<tr>
<th>Regex Character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Zero or more characters</td>
</tr>
<tr>
<td>+</td>
<td>Zero or more repeated instances of the token preceding the +</td>
</tr>
<tr>
<td>?</td>
<td>Match zero or one character</td>
</tr>
</tbody>
</table>

**Important:** The CLI does not support configuring “?” directly, you must instead use “\077”.

For example, if you want to match the string “xyz<any one character>pqr”, you must configure it as:

```
http host regex "xyz\077pqr"
```

In another example, if you want to exactly match the string “url?resource=abc”, you must configure it as:

```
http uri regex "url\077resource=abc"
```

Where, the first “\" (backslash) is for the escaping of “?” and then “\077” for specifying “?” to the CLI.

<table>
<thead>
<tr>
<th>\character</th>
<th>Escaped character</th>
</tr>
</thead>
<tbody>
<tr>
<td>?</td>
<td>Match the question mark (&lt;ctrl-v&gt;?) character</td>
</tr>
<tr>
<td>+</td>
<td>Match the plus character</td>
</tr>
<tr>
<td>*</td>
<td>Match the asterisk character</td>
</tr>
<tr>
<td>\a</td>
<td>Match the Alert (ASCII 7) character</td>
</tr>
<tr>
<td>\b</td>
<td>Match the Backspace (ASCII 8) character</td>
</tr>
<tr>
<td>\f</td>
<td>Match the Form-feed (ASCII 12) character</td>
</tr>
<tr>
<td>\n</td>
<td>Match the New line (ASCII 10) character</td>
</tr>
<tr>
<td>\r</td>
<td>Match the Carriage return (ASCII 13) character</td>
</tr>
<tr>
<td>\t</td>
<td>Match the Tab (ASCII 9) character</td>
</tr>
<tr>
<td>\v</td>
<td>Match the Vertical tab (ASCII 11) character</td>
</tr>
<tr>
<td>\0</td>
<td>Match the Null (ASCII 0) character</td>
</tr>
<tr>
<td>\</td>
<td>Match the backslash character</td>
</tr>
</tbody>
</table>

Bracketed range [0-9] Match any single character from the range

A leading ^ in a range Do not match any in the range. All other characters represent themselves.

\x## Any ASCII character as specified in two-digit hex notation. For example, \x5A yields a “Z”.
### Regex Character | Description
---|---
| | Specify OR regular expression operator

**Important:** When using the regex operator “|” in regex expressions, always wrap the string in double quotes.

For example, if you want to match the string “pqr” OR “xyz”, you must configure it as: `http host regex "pqr|xyz"`.

### Example

The following command defines a rule expression to match the HTTP URI string `http://www.somehost.com`:

```plaintext
http uri = http://www.somehost.com
```

The following command defines a regex rule expression to match either of the following or similar values in the HTTP URI string: `http://server19.com/search?form=zip`, `http://server20.com/search?form=pdf`

```plaintext
```
http url

This command allows you to define rule expressions to match HTTP URL.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax


no
If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive
Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator
Specifies how to match.
operator must be one of the following:
- !=: Does not equal
- !contains: Does not contain
- !ends-with: Does not end with
- !starts-with: Does not start with
- =: Equals
- contains: Contains
- ends-with: Ends with
- regex: Regular expression
- starts-with: Starts with

url
Specifies the HTTP URL to match.
url must be an alphanumeric string of 1 through 127 characters, that allows punctuation characters and includes “host + URI” for HTTP PDUs.
For example, in case of the URL “http://www.google.fr/”, the host is “http://www.google.fr”, and the URI is “/”.

Hypertext Transfer Protocol

GET / HTTP/1.1
Request Method: GET
Request URI: /
Request Version: HTTP/1.1
Accept: */*
Accept-Language: fr
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)
Host: www.google.fr
Connection: Keep-Alive

Usage

Use this command to define rule expressions to match HTTP URL. The following table lists the special characters that you can use in regex rule expressions. For more information on regex support, refer to the Enhanced Charging Service Administration Guide.

<table>
<thead>
<tr>
<th>Regex Character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Zero or more characters</td>
</tr>
<tr>
<td>+</td>
<td>Zero or more repeated instances of the token preceding the +</td>
</tr>
<tr>
<td>?</td>
<td>Match zero or one character</td>
</tr>
</tbody>
</table>

**Important:** The CLI does not support configuring “?” directly, you must instead use “\077”. For example, if you want to match the string “xyz<any one character>pqr”, you must configure it as: `http host regex “xyz\077pqr”`. In another example, if you want to exactly match the string “url?resource=abc”, you must configure it as: `http uri regex “url\077resource=abc”`. Where, the first “\” (backslash) is for the escaping of “?” and then “\077” for specifying “?” to the CLI.

<table>
<thead>
<tr>
<th>\ character</th>
<th>Escaped character</th>
</tr>
</thead>
<tbody>
<tr>
<td>?</td>
<td>Match the question mark (&lt;ctrl-v&gt;?) character</td>
</tr>
<tr>
<td>+</td>
<td>Match the plus character</td>
</tr>
<tr>
<td>Regex Character</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------</td>
</tr>
<tr>
<td>*</td>
<td>Match the asterisk character</td>
</tr>
<tr>
<td>\a</td>
<td>Match the Alert (ASCII 7) character</td>
</tr>
<tr>
<td>\b</td>
<td>Match the Backspace (ASCII 8) character</td>
</tr>
<tr>
<td>\f</td>
<td>Match the Form-feed (ASCII 12) character</td>
</tr>
<tr>
<td>\n</td>
<td>Match the New line (ASCII 10) character</td>
</tr>
<tr>
<td>\r</td>
<td>Match the Carriage return (ASCII 13) character</td>
</tr>
<tr>
<td>\t</td>
<td>Match the Tab (ASCII 9) character</td>
</tr>
<tr>
<td>\v</td>
<td>Match the Vertical tab (ASCII 11) character</td>
</tr>
<tr>
<td>\0</td>
<td>Match the Null (ASCII 0) character</td>
</tr>
<tr>
<td>\</td>
<td>Match the backslash character</td>
</tr>
<tr>
<td>[0-9]</td>
<td>Match any single character from the range</td>
</tr>
<tr>
<td>^</td>
<td>Do not match any in the range. All other characters represent themselves.</td>
</tr>
<tr>
<td>\x##</td>
<td>Any ASCII character as specified in two-digit hex notation. For example, \x5A yields a “Z”.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Important:** When using the regex operator “|” in regex expressions, always wrap the string in double quotes.

For example, if you want to match the string "pqr" OR “xyz”, you must configure it as:

```
http host regex "pqr|xyz".
```

**Example**

The following command defines a rule expression to match the HTTP URL

```
http://rfc.ietf.org/rfc/rfc1738.txt:
```

```
http url = http://rfc.ietf.org/rfc/rfc1738.txt
```

The following command defines a regex rule expression to match either of the following or similar values in the HTTP URL string: http://yahoo.com, http://www.yahoo.co.in, http://yahoo.com/news.

```
http url regex "(http://|http://www).yahoo.(co.in|com)*"
```
**http user-agent**

This command allows you to define rule expressions to match the User-Agent request-header field of HTTP packets.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] http user-agent [ case-sensitive ] operator user_agent
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **case-sensitive**
  Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

- **operator**
  Specifies how to match.

  **operator** must be one of the following:

  - !=: Does not equal
  - !contains: Does not contain
  - !ends-with: Does not end with
  - !starts-with: Does not start with
  - =: Equals
  - contains: Contains
  - ends-with: Ends with
  - starts-with: Starts with

- **user_agent**
  Specifies the HTTP user agent value to match.

  **user_agent** must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters.
Usage

Use this command to define rule expressions to match value in HTTP user-agent header field. In 14.0 and later releases, the ECS HTTP analyzer supports both CRLF and LF as valid terminators for HTTP header fields.

Example

The following command defines a rule expression to match *xyz.123* in HTTP user-agent header field:

```
http user-agent = xyz.123
```
http version

This command allows you to define rule expressions to match version information in HTTP headers.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax


- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **case-sensitive**
  Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

- **operator**
  Specifies how to match.
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `!contains`: Does not contain
  - `!ends-with`: Does not end with
  - `!starts-with`: Does not start with
  - `=:`  Equals
  - `contains`: Contains
  - `ends-with`: Ends with
  - `starts-with`: Starts with

- **http_version**
  Specifies this HTTP version value to match.
  `http_version` must be an alphanumeric string of 1 through 127 characters, and may contain punctuation characters.
Usage
Use this command to define rule expressions to match HTTP version.

Example
The following command defines a rule expression to match HTTP version http4.2:

```plaintext
http version = http4.2
```
**http x-header**

This command allows you to define rule expressions to match specified field within extension-headers (x-headers).

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] http x-header field_name [ case-sensitive ] operator string
```

- **no**
  
  If previously configured, deletes the specified rule expression from the current ruledef.

- **field_name**
  
  `field_name` must be an alphanumeric string of 1 through 31 characters.

- **case-sensitive**
  
  Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

- **operator**
  
  Specifies how to match.

  - `operator` must be one of the following:
    
    - `!=`: Does not equal
    - `!contains`: Does not contain
    - `!ends-with`: Does not end with
    - `!starts-with`: Does not start with
    - `==`: Equals
    - `contains`: Contains
    - `ends-with`: Ends with
    - `starts-with`: Starts with

- **string**

  Specifies the HTTP x-header value to match.

  `string` must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters.
Usage

Use this command to define rule expressions to match specified fields within x-headers. The extension-header can be any header field not specified in RFCs.
All x-header fields must begin with “x-”.
In 14.0 and later releases, the ECS HTTP analyzer supports both CRLF and LF as valid terminators for HTTP header fields.

Example

The following command defines a rule expression to match the extension-header `test_field` for the value `test_string`:

```
http x-header test_field = test_string
```
icmp any-match

This command allows you to define rule expressions to match all ICMP packets.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

`active-charging service service_name > ruledef ruledef_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] icmp any-match operator condition
```

- **no**
  
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  
  Specifies how to match.

  **operator** must be one of the following:
  - !=: Does not equal
  - ==: Equals

- **condition**
  
  Specifies the condition to match.

  **condition** must be one of the following:
  - FALSE
  - TRUE

**Usage**

Use this command to define rule expressions to match all ICMP packets.

**Example**

The following command defines a rule expression to match all ICMP packets:

```
icmp any-match = TRUE
```
**icmp code**

This command allows you to define rule expressions to match value in the Code field of ICMP packets.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```plaintext
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acn-ruledef)#
```

**Syntax**

```
[ no ] icmp code operator code
```

- **no**
  
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**

  Specifies how to match.

  - `!=`: Does not equal
  - `<=`: Lesser than or equals
  - `=`: Equals
  - `>=`: Greater than or equals

- **code**

  Specifies the ICMP code to match.

  `code` must be an integer from 0 through 255.

**Usage**

Use this command to define rule expressions to match a code field of ICMP packets.

**Example**

The following command defines a rule expression to match ICMP code 11:

```
icmp code = 11
```
**icmp type**

This command allows you to define rule expressions to match value in Type field of ICMP packets.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] icmp type operator type
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `<=`: Lesser than or equals
  - `=`: Equals
  - `>=`: Greater than or equals

- **type**
  Specifies the ICMP type to match.
  `type` must be an integer from 0 through 255. For example, 0 for Echo Reply, 3 for Destination Unreachable, and 5 for Redirect.

**Usage**
Use this command to define rule expressions to match a type field of ICMP packets.

**Example**

The following command defines a rule expression to match user traffic based on ICMP type 3:

```
icmp type = 3
```
icmpv6 any-match

This command allows you to define rule expressions to match all ICMPv6 packets.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] icmpv6 any-match operator condition

- no
If previously configured, deletes the specified rule expression from the current ruledef.

- operator
Specifies how to match.
operator must be one of the following:
  • !=: Does not equal
  • ==: Equals

- condition
Specifies the condition to match.
condition must be one of the following:
  • FALSE
  • TRUE

Usage
Use this command to define rule expressions to match all ICMPv6 packets.

Example
The following command defines a rule expression to match all ICMPv6 packets:

    icmpv6 any-match = TRUE
**icmpv6 code**

This command allows you to define rule expressions to match value in Code field of ICMPv6 packets.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

**Syntax**

```
[ no ] icmpv6 code operator code
```

- **no**
  
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  
  Specifies how to match.
  
  `operator` must be one of the following:
  
  - `!=`: Does not equal
  - `<=`: Lesser than or equals
  - `==`: Equals
  - `>=`: Greater than or equals

- **code**
  
  Specifies the ICMPv6 code to match.
  
  `code` must be an integer from 0 through 255.

**Usage**

Use this command to define rule expressions to match a code field of ICMPv6 packets.

**Example**

The following command defines a rule expression to match ICMPv6 code 134:

```
icmpv6 code = 134
```
### icmpv6 type

This command allows you to define rule expressions to match type field of ICMPv6 packets.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > ACS Configuration > Ruledef Configuration

*active-charging service service_name > ruledef ruledef_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] icmpv6 type operator type
```

- **no**
  
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  
  Specifies how to match.
  
  *operator* must be one of the following:
  
  - !=: Does not equal
  - <=: Lesser than or equals
  - =: Equals
  - >=: Greater than or equals

- **type**
  
  Specifies the ICMPv6 type to match.
  
  *type* must be an integer from 0 through 255. For example, 129 for Echo Reply, 3 for Time Exceeded, and 137 for Redirect Message.

**Usage**

Use this command to define rule expressions to match type field of ICMPv6 packets.

**Example**

The following command defines a rule expression to match ICMPv6 type 133:

```
icmpv6 type = 133
```
if-protocol

This command allows you to associate different content IDs with the same ruledef, depending on the protocol being used.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

`active-charging service service_name > ruledef ruledef_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
if-protocol { http | wsp-connection-less | wsp-connection-oriented } content-id content_id

no if-protocol { http | wsp-connection-less | wsp-connection-oriented }
```

no

If previously configured, deletes the specified rule expression from the current ruledef.

**http**

Specifies HTTP protocol.
This is the same as the rule expression `http any-match = true`.

**wsp-connection-less**

Specifies WSP connection-less protocol.
This is the same as requiring “wsp any-match = true” but “wtp any-match = false” (that is, connection-less WAP1.x).

**wsp-connection-oriented**

Specifies WSP connection-oriented protocol.
This is the same as the combined rule expression “wsp any-match = true” and “wtp any-match = true” (that is, connection-oriented WAP1.x).

**content-id content_id**

Specifies the content ID for the specified protocol.
In 12.1 and earlier releases, `content_id` must be an integer from 1 through 65535.
In 12.2 and later releases, `content_id` must be an integer from 1 through 2147483647.
**Usage**

Use this command to associate different content IDs with the same ruledef, depending on the protocol being used.

This command is only effective for charging ruledefs. See the `rule-application` command for information on how to configure charging ruledefs.

If a particular ruledef should have three different values for content-id, depending on whether the traffic is connection-oriented WAP1.x, connection-less WAP1.x, or WAP2.0, within the ruledef we should have configuration similar to the following:

```plaintext
if-protocol wsp-connection-oriented content-id 1
if-protocol wsp-connection-less content-id 2
if-protocol http content-id 3
```

Presumably, the ruledef would have another configurable like “www url contains foo”, which would cause it to use different content IDs when "foo" was accessed, depending upon the protocol being used.

**Example**

The following command associates HTTP protocol and a content ID of 23:

```
if-protocol http content-id 23
```
imap any-match

This command allows you to define rule expressions to match all IMAP packets.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] imap any-match operator condition

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be one of the following:
- !=: Does not equal
- ==: Equals

condition
Specifies the condition to match.
condition must be one of the following:
- FALSE
- TRUE

Usage
Use this command to define rule expressions to match all IMAP packets.

Example
The following command defines a rule expression to match all IMAP packets:

imap any-match = TRUE
imap cc

This command allows you to define rule expressions to match recipient address in the Carbon Copy (cc) field of e-mails in IMAP messages.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] imap cc [ case-sensitive ] operator cc_address
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **case-sensitive**
  Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

- **operator**
  Specifies how to match.
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `!contains`: Does not contain
  - `!ends-with`: Does not end with
  - `!starts-with`: Does not start with
  - `=`: Equals
  - `contains`: Contains
  - `ends-with`: Ends with
  - `starts-with`: Starts with

- **cc_address**
  Specifies the e-mail “cc” address/name to match.
  `cc_address` must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters.
Usage

Use this command to define rule expressions to match recipient address in the “cc” field of e-mails in IMAP messages.

Example

The following command defines a rule expression to match recipient address `triangle@xyz.com` in the “cc” field of e-mails in IMAP messages:

```
imap cc contains triangle@xyz.com
```
imap command

This command allows you to define rule expressions to match embedded IMAP commands in IMAP messages.

**Product**  
ACS

**Privilege**  
Security Administrator, Administrator

**Mode**  
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] imap command operator command
```

- **no**  
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**  
  Specifies how to match.  
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `==`: Equals

- **command**  
  Specifies the command to match.  
  `command` must be one of the following:
  - `append`
  - `authenticate`
  - `capability`
  - `check`
  - `close`
  - `copy`
  - `create`
  - `delete`
  - `examine`
  - `expunge`
  - `fetch`
  - `list`
imap command

- login
- logout
- lsub
- noop
- rename
- search
- select
- starttls
- status
- store
- subscribe
- uid-copy
- uid-fetch
- uid-search
- uid-store
- unsubscribe

Usage

Use this command to define rule expressions to match an embedded command in the IMAP message.

Example

The following command defines a rule expression to match `close` command in IMAP messages:

    imap command = close
imap content class

This command allows you to define rule expressions to match the content-class field of e-mails in IMAP messages.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] imap content class [ case-sensitive ] operator content_class
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **case-sensitive**
  Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

- **operator**
  Specifies how to match.
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `!contains`: Does not contain
  - `!ends-with`: Does not end with
  - `!starts-with`: Does not start with
  - `=`: Equals
  - `contains`: Contains
  - `ends-with`: Ends with
  - `starts-with`: Starts with

- **content_class**
  Specifies the content class to match.
  `content_class` must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters.
Usage

Use this command to define rule expressions to match the content-class field of e-mails in IMAP messages.

Example

The following command defines a rule expression to analyze user traffic matching content class `javax.mail.internet.MimeMultipart` in the content-class field of e-mails in IMAP messages:

```
imap content class contains javax.mail.internet.MimeMultipart
```
imap content type

This command allows you to define rule expressions to match the content-type field of e-mails in IMAP messages.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] imap content type [ case-sensitive ] operator content_type

no
If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive
Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator
Specifies how to match.
operator must be one of the following:
• !=: Does not equal
• !contains: Does not contain
• !ends-with: Does not end with
• !starts-with: Does not start with
• ==: Equals
• contains: Contains
• ends-with: Ends with
• starts-with: Starts with

content_type
Specifies the content type field to match.
content_type must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters.
Usage
Use this command to define rule expressions to match the content-type field of e-mails in IMAP messages.

Example
The following command defines a rule expression to analyze user traffic matching content type "TEXT/plain; charset=iso-8859-1" in the content-type field of e-mails in IMAP messages:

`imap content type contains TEXT/plain; charset=iso-8859-1`
imap date

This command allows you to define rule expressions to match the Date field of e-mails in IMAP messages.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] imap date [ case-sensitive ] operator date

no
If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive
Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator
Specifies how to match.
operator must be one of the following:

• !=: Does not equal
• !contains: Does not contain
• !ends-with: Does not end with
• !starts-with: Does not start with
• ==: Equals
• contains: Contains
• ends-with: Ends with
• starts-with: Starts with

date
Specifies the date to match.
date must be an alphanumeric string of 1 through 127 characters that may include punctuation marks and spaces as shown in the example below.
Usage

Use this command to define rule expressions to match the date field of e-mails in IMAP messages.

Example

The following command defines a rule expression to analyze user traffic matching date Fri, 20 Jan 2012 11:00:00 -0600 in the “date” field of e-mails in IMAP messages:

imap date contains Fri, 21 Jan 2012 11:00:00 -0600
imap final-reply

This command allows you to define rule expressions to match final-reply value for the last IMAP final-reply message.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] imap final-reply operator final_reply
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `=`: Equals

- **final_reply**
  Specifies the “final-reply” condition to match.
  `final_reply` must be one of the following:
  - `bad`: Final reply is invalid or bad.
  - `no`: There is no final reply.
  - `ok`: Final reply is valid.

**Usage**

Use this command to define rule expressions to match a final-reply value for the last IMAP final-reply message.

**Example**

The following command defines a rule expression to analyze user traffic matching the final-reply condition `bad` in the last IMAP final-reply message:

```
imap final-reply = bad
```
imap from

This command allows you to define rule expressions to match the from field of e-mails in IMAP messages.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] imap from [ case-sensitive ] operator from_address

no
If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive
Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator
Specifies how to match.
operator must be one of the following:
• !=: Does not equal
• !contains: Does not contain
• !ends-with: Does not end with
• !starts-with: Does not start with
• =: Equals
• contains: Contains
• ends-with: Ends with
• starts-with: Starts with

from_address
Specifies the “from” address/value to match.
from_address must be an alphanumerical string of 1 through 127 characters.

Usage
Use this command to define rule expressions to match the from field of e-mails in IMAP messages.
Example

The following command defines a rule expression to analyze user traffic matching `triangle` in the “from” field of e-mails in the IMAP messages:

```
imap from contains triangle
```
imap mail-size

This command allows you to define rule expressions to match IMAP e-mail users that have e-mails of a specified size in their mailboxes.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] imap mail-size operator mail_size

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be one of the following:
- !=: Does not equal
- <=: Lesser than or equals
- =: Equals
- >=: Greater than or equals

mail_size
Specifies the total size of mail, in bytes, to match.
mail_size must be an integer from 0 through 400000000.

Usage
Use this command to define rule expressions to discover the number of IMAP e-mail users that have e-mails of a specified size in their mailboxes.

Example
The following command defines a rule expression to match users with e-mail size less than or equal to 23400 bytes:

imap mail-size <= 23400
imap mailbox-size

This command allows you to define rule expressions to match IMAP e-mail user having a specified number of messages in their mailboxes.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] imap mailbox-size operator number_of_email

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  operator must be one of the following:
  - !=: Does not equal
  - <=: Lesser than or equals
  - ==: Equals
  - >=: Greater than or equals

- **number_of_email**
  Specifies the total number of e-mail messages in mailbox of an IMAP user to match.
  number_of_email must be an integer from 0 through 65535.

Usage

Use this command to define rule expressions to match the number of IMAP e-mail users having a specified number of messages in their mailboxes.

Example

The following command defines a rule expression to match e-mail users having less than or equal to 1024 e-mail messages in their mailboxes:

    imap mailbox-size <= 1024
imap message-type

This command allows you to define rule expressions to match the type of IMAP packet.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

`active-charging service service_name > ruledef ruledef_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] imap message-type operator message_type
```

- **no**
  
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  
  Specifies how to match.
  
  `operator` must be one of the following:
  
  - `!=`: Does not equal
  - `=`: Equals

- **message_type**
  
  Specifies the IMAP packet message-type to match.
  
  `message_type` must be one of the following:
  
  - `command-continuation-reply`: Message with command-continuation-reply type.
  - `final-reply`: Message is of final reply type.
  - `request`: There is of request type.
  - `untagged-reply`: Message of reply type, but without any tag.

**Usage**

Use this command to define rule expressions to match the IMAP message type.

**Example**

The following command defines a rule expression to match IMAP sessions with message type `request`:

```
imap message-type = request
```
imap previous-state

This command allows you to define rule expressions to match the previous state of IMAP request sessions.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] imap previous-state operator imap_previous_state

<table>
<thead>
<tr>
<th>no</th>
</tr>
</thead>
<tbody>
<tr>
<td>If previously configured, deletes the specified rule expression from the current ruledef.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>operator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies how to match.</td>
</tr>
<tr>
<td>operator must be one of the following:</td>
</tr>
<tr>
<td>• !=: Does not equal</td>
</tr>
<tr>
<td>• ==: Equals</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>imap_previous_state</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the previous state to match.</td>
</tr>
<tr>
<td>imap_previous_state must be one of the following:</td>
</tr>
<tr>
<td>• init: Message in initialization state.</td>
</tr>
<tr>
<td>• request-sent: Message in request-sent state.</td>
</tr>
</tbody>
</table>

Usage
Use this command to define rule expressions to match previous state of IMAP request session.

Example
The following command defines a rule expression to match IMAP sessions with previous state init:

imap previous-state = init
imap session-length

This command allows you to define rule expressions to match the total length of an IMAP session.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] imap session-length operator session_length

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be one of the following:
  • !=: Does not equal
  • <=: Lesser than or equals
  • ==: Equals
  • >=: Greater than or equals

session_length
Specifies the total length of IMAP session (in bytes) to match.
session_length must be an integer from 1 through 4000000000.

Usage
Use this command to define rule expressions to match the total length of IMAP sessions.
The session length is calculated by adding together the IP payloads (that is, starting after the IP header) of all relevant IMAP session packets.

Example
The following command defines a rule expression to match IMAP sessions with length less than or equal to 4000 bytes:

imap session-length <= 4000
imap session-previous-state

This command allows you to define rule expressions to match the previous state of an IMAP session.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

Syntax

[ no ] imap session-previous-state operator imap_session_previous_state

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be one of the following:
• !=: Does not equal
• ==: Equals

imap_session_previous_state
Specifies the previous state of IMAP session to match.
imap_session_previous_state must be one of the following:
• authenticated: Session authenticated
• connected: Session connected
• init: Session initialized
• mailbox-selected: Mailbox selected

Usage
Use this command to define rule expressions to match the previous state of IMAP sessions.

Example
The following command defines a rule expression to match IMAP sessions with previous state init:

imap session-previous-state = init
**imap session-state**

This command allows you to define rule expressions to match the current state of IMAP sessions.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] imap session-state operator session_current_state
```

- **no**
  
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  
  Specifies how to match.
  
  `operator` must be one of the following:
  
  - `!=`: Does not equal
  - `==`: Equals

- **session_current_state**
  
  Specifies the current state to match.
  
  `session_current_state` must be one of the following:
  
  - `authenticated`: Session authenticating.
  - `connected`: Session connecting.
  - `logout`: Session logged out.
  - `mailbox-selected`: Mailbox selecting.

**Usage**

Use this command to define rule expressions to match the current state of IMAP sessions.

**Example**

The following command defines a rule expression to match IMAP sessions with current state `connected`:

```
imap session-state = connected
```
imap state

This command allows you to define rule expressions to match the current state of IMAP sessions.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] imap state operator current_state
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `==`: Equals

- **current_state**
  Specifies current state of IMAP session to match.
  `current_state` must be one of the following:
  - `request-sent`: Request message sent
  - `response-fail`: Request response failed
  - `response-ok`: Request response is good

**Usage**

Use this command to define rule expressions to match the current state of IMAP session.

**Example**

The following command defines a rule expression to match IMAP sessions with current state `response-fail`:

```
imap state = response-fail
```
imap subject

This command allows you to define rule expressions to match the subject field of e-mails in IMAP messages.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

`active-charging service service_name > ruledef ruledef_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] imap subject [ case-sensitive ] operator subject
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **case-sensitive**
  Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

- **operator**
  Specifies how to match.
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `!contains`: Does not contain
  - `!ends-with`: Does not end with
  - `!starts-with`: Does not start with
  - `=`: Equals
  - `contains`: Contains
  - `ends-with`: Ends with
  - `starts-with`: Starts with

- **subject**
  Specifies the “subject” to match.
  `subject` must be an alphanumeric string of 1 through 127 characters, and may contain punctuation characters and space as shown in the example below.
Usage

Use this command to define rule expressions to match “subject” field of e-mail in IMAP message.

Example

The following command defines rule expression to match occurrence of the string `My test` in the “subject” field of e-mails in IMAP message:

```
imap subject contains My test
```
imap to

This command allows you to define rule expressions to match the “to” field of e-mails in IMAP messages.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] imap to [ case-sensitive ] operator to

---

no

If previously configured, deletes the specified rule expression from the current ruledef.

---

case-sensitive

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

---

operator

Specifies how to match.

operator must be one of the following:

- !=: Does not equal
- !contains: Does not contain
- !ends-with: Does not end with
- !starts-with: Does not start with
- =: Equals
- contains: Contains
- ends-with: Ends with
- starts-with: Starts with

---

to

Specifies the “to” field value to match.
to must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters.

---

Usage

Use this command to define rule expressions to match “to” field of e-mails in IMAP messages.
Example

The following command defines a rule expression to analyze user traffic matching the occurrence `xyz.com` in the “to” field of e-mails in the IMAP message:

```
imap to contains xyz.com
```
**ip any-match**

This command allows you to define rule expressions to match all IPv4/IPv6 packets.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] ip any-match operator condition
```

- **no**
  
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  
  Specifies how to match.
  
  **operator** must be one of the following:
  
  - `!=`: Does not equal
  - `=`: Equals

- **condition**
  
  Specifies the condition to match.
  
  **condition** must be one of the following:
  
  - `FALSE`
  - `TRUE`

**Usage**

Use this command to define rule expressions to match IPv4/IPv6 packets.

**Example**

The following command defines a rule expression to match IPv4/IPv6 packets:

```
ip any-match = TRUE
```
ip dscp

This command enables you to configure a ruledef with the DSCP value and match it with the DSCP value in the incoming IP packets.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] ip dscp { operator } IPv4_ToS_value | IPv6_TC_value [ mask mask_value ]
```

- **no**
  If previously configured, removes the specified DSCP value and the mask from the configuration.

- **operator**
  Specifies how to match.
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `=`: Equals

- **IPv4_ToS_value | IPv6_TC_value**
  Specifies the DSCP value to match with the incoming IP packets.
  The `IPv4_ToS_value` or `IPv6_TC_value` must be an integer from 0 through 63.

- **mask mask_value**
  Specifies the mask for the number of bits in the DSCP value to be considered for matching.
  `mask_value` must be an integer from 0 through 63. The default mask value is 63.

**Usage**

Use this command to check if the DSCP value in the IPv4 ToS or IPv6 TC field of incoming IP packet matches with configured ToS/TC value.

**Example**

The following command will match all incoming packets which has DSCP value 20:

```
ip dscp = 20 mask 31
```
ip downlink

This command allows you to define rule expressions to match downlink (network to subscriber) packets.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

Syntax

[ no ] ip downlink operator condition

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be one of the following:
- !=: Does not equal
- ==: Equals

condition
Specifies the condition to match.
condition must be one of the following:
- FALSE
- TRUE

Usage
Use this command to define rule expressions to match downlink (to subscriber) IP packets.

Example
The following command defines a rule expression to match IP packet in downlink direction:

ip downlink = TRUE
**ip dst-address**

This command allows you to define rule expressions to match IP destination address field within IP headers.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```text
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```text
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```text
[ no ] ip dst-address { operator { ipv4/ipv6_address | ipv4/ipv6_address/mask } | { !range | range } host-pool host_pool_name }
```

- `operator`: Specifies how to match. `operator` must be one of the following:
  - `!=`: Does not equal
  - `<=`: Lesser than or equals
  - `==`: Equals
  - `>=`: Greater than or equals

- `ipv4/ipv6_address`: Specifies the IP address of the destination node for outgoing traffic. `ipv4/ipv6_address` must be an IP address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

- `ipv4/ipv6_address/mask`: Specifies the IP address of the destination node for outgoing traffic. `ipv4/ipv6_address/mask` must be an IP address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation with subnet mask bit. The mask bit is a numeric value which corresponding to the number of bits in the subnet mask.

- `{ !range | range } host-pool host_pool_name`: Specifies the name of the host pool. `host_pool_name` must be an alphanumeric string of 1 through 63 characters.
Usage

Use this command to define rule expressions to match the IP destination address field within IP headers.

Example

The following command defines a rule expression to match user traffic based on the IPv4 destination address 10.1.1.1:

```
ip dst-address = 10.1.1.1
```
ip error

This command allows you to define rule expressions to match user traffic for invalid IP packets and other errors, for example IP header error, while parsing IP packets.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] ip error operator condition

---

no
If previously configured, deletes the specified rule expression from the current ruledef.

---

operator
Specifies how to match.
operator must be one of the following:

- !=: Does not equal
- ==: Equals

---

condition
Specifies the condition to match.
condition must be one of the following:

- FALSE
- TRUE

---

Usage
Use this command to define rule expressions to match invalid IP packets and any other errors while parsing IP packets.

Example
The following command defines a rule expression to match user traffic for invalid IP packets and other errors:

   ip error = TRUE
**ip protocol**

This command allows you to define rule expressions to match the protocol field in IP headers.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > ACS Configuration > Ruledef Configuration

```
active charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] ip protocol operator { protocol_assignment_no | protocol }
```

- **no**
  
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  
  Specifies how to match.
  
  `operator` must be one of the following:
  
  - `!=`: Does not equal
  - `<=`: Lesser than or equals—available only in 8.1 and later releases
  - `=`: Equals
  - `>=`: Greater than or equals—available only in 8.1 and later releases

- **protocol_assignment_no**
  
  Specifies the protocol by assignment number.
  
  `protocol_assignment_no` must be an integer from 0 through 255.
  
  For example, 1 for ICMP, 6 for TCP, and 17 for UDP.

- **protocol**
  
  Specifies the protocol by name.
  
  `protocol` must be one of the following:
  
  - `ah`
  - `esp`
  - `gre`
  - `icmp`
  - `icmpv6`
  - `tcp`
ip protocol

• udp

Usage
Use this command to define rule expressions to match protocol field in IP packet headers.

Example
The following command defines a rule expression to match protocol assignment number 1:

\[
\text{ip protocol} = 1
\]
ip server-domain-name

This command allows you to define rule expressions to match host names (domain names).

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] ip server-domain-name operator domain_name

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be one of the following:
  ● =: Equals
  ● contains: Contains
  ● ends-with: Ends with
  ● starts-with: Starts with

domain_name
Specifies the domain name to match.
domain_name must be an alphanumeric string of 1 through 127 characters.

Usage
Use this command to define rule expressions to match full or partial host names (domain names).
The rule will be matched for the learnt IP addresses resolved from DNS queries to the specified domain names.
DNS responses for the specified domain names will be snooped and the learnt IP addresses stored.
Besides being used for standard rule matching, this command also enables the DNS Snooping feature if the rulebase references any ruledefs with this configuration. The DNS protocol analyzer must also be enabled in the rulebase.

Example
The following command defines a rule expression to match domain name values containing star:

ip server-domain-name contains star
**ip server-ip-address**

This command allows you to define rule expressions to match the IP address of the destination end of the connection.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] ip server-ip-address { operator { ipv4/ipv6_address | ipv4/ipv6_address/mask } | { !range | range } host-pool host_pool_name }
```

- **no**: If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**: Specifies how to match.
  - **operator** must be one of the following:
    - !: Does not equal
    - <=: Lesser than or equals
    - ==: Equals
    - >=: Greater than or equals

- **ipv4/ipv6_address**: Specifies the server IP address. For uplink packets (subscriber to network), this field matches the destination IP address in the IP header. For downlink packets (network to subscriber), this field matches the source IP address in the IP header. `ipv4/ipv6_address` must be an IP address in IPv4 dotted-decimal notation or IPv6 colon-separated-hexadecimal notation.

- **ipv4/ipv6_address/mask**: Specifies the server IP address with subnet mask bit. For uplink packets (subscriber to network), this field matches the destination IP address in the IP header. For downlink packets (network to subscriber), this field matches the source IP address in the IP header. `ipv4/ipv6_address/mask` must be an IP address in IPv4 dotted-decimal notation or IPv6 colon-separated-hexadecimal notation with subnet mask bit. The mask bit is a numeric value which is the number of bits in the subnet mask.

- **{ !range | range } host-pool host_pool_name**: Specifies the range criteria:
- \texttt{!range}: Not in the range of
- \texttt{range}: In the range of

\texttt{host-pool host\_pool\_name}: Specifies name of the host pool. \texttt{host\_pool\_name} must be an alphanumeric string of 1 through 63 characters.

\section*{Usage}

Use this command to define rule expressions to match the IP address of the destination end of the connection. For uplink packets, this field matches the destination IP address in the IP header. For downlink packets, this field matches the source IP address in the IP header.

\section*{Example}

The following command defines a rule expression to match user traffic based on IPv4 server address 10.1.1.1:

\begin{verbatim}
ip server-ip-address = 10.1.1.1
\end{verbatim}
ip src-address

This command allows you to define rule expressions to match the source IP address field within IP headers.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] ip src-address { operator { ipv4/ipv6_address | ipv4/ipv6_address/mask } | { !range | range } host-pool host_pool_name }
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  **operator** must be one of the following:
  - !=: Does not equal
  - <=: Lesser than or equals
  - =: Equals
  - >=: Greater than or equals

- **ipv4/ipv6_address**
  Specifies IP address of the source node for incoming traffic. **ipv4/ipv6_address** must be an IP address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

- **ipv4/ipv6_address/mask**
  Specifies the IP address of the source node for incoming traffic with subnet mask bit. **ipv4/ipv6_address/mask** must be an IP address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation with subnet mask bit. The mask bit is a numeric value which corresponds to the number of bits in the subnet mask.

- **{ !range | range } host-pool host_pool_name**
  **!range | range**: Specifies the range criteria:
  - !range: Not in the range of
  - range: In the range of
**host-pool**  *host_pool_name*: Specifies name of the host pool. *host_pool_name* must be a string of 1 through 63 characters.

---

**Usage**

Use this command to define rule expressions to match IP source address field within IP header.

**Example**

The following command defines a rule expression to match user traffic based on IPv4 source address 10.1.1.1:

```
ip src-address = 10.1.1.1
```
ip subscriber-ip-address

This command allows you to define rule expressions to match the IP address of the subscriber, which will be either the source or destination address depending on the direction.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] ip subscriber-ip-address { operator { ipv4/ipv6_address | ipv4/ipv6_address/mask } | { !range | range } host-pool host_pool_name }

<table>
<thead>
<tr>
<th>no</th>
</tr>
</thead>
</table>
| If previously configured, deletes the specified rule expression from the current ruledef.

<table>
<thead>
<tr>
<th>operator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies how to match.</td>
</tr>
<tr>
<td>operator must be one of the following:</td>
</tr>
<tr>
<td>• !=: Does not equal</td>
</tr>
<tr>
<td>• &lt;=: Lesser than or equals</td>
</tr>
<tr>
<td>• ==: Equals</td>
</tr>
<tr>
<td>• &gt;=: Greater than or equals</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ipv4/ipv6_address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the subscriber IP address. Depending on the direction of packet this IP address will be either the IP source address or the IP destination address. ipv4/ipv6_address must be an IP address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ipv4/ipv6_address/mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the subscriber IP address with subnet mask bit. Depending on the direction of packet this IP address will either be the IP source address or the IP destination address. ipv4/ipv6_address/mask must be an IP address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation with subnet mask bit. The mask bit is a numeric value which corresponds to the number of bits in the subnet mask.</td>
</tr>
</tbody>
</table>

| { !range | range } host-pool host_pool_name |
| --- |
| !range | range: Specifies the range criteria: |
| • !range: Not in the range of |
ip subscriber-ip-address

- **range**: In the range of

  `host-poll host_pool_name`: Specifies the name of the host pool. `host_pool_name` must be an alphanumeric string of 1 through 63 characters.

**Usage**

Use this command to define rule expressions to match the IP address of the subscriber, which will be either the source or destination address depending on the direction.

**Example**

The following command defines a rule expression to match user traffic based on subscriber IPv4 address 10.1.1.1:

```
ip subscriber-ip-address = 10.1.1.1
```
ip total-length

This command allows you to define rule expressions to match the total length field in IP headers.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration
active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] ip total-length operator total_length

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be one of the following:
• !=: Does not equal
• <=: Lesser than or equals
• ==: EQUALS
• >=: Greater than or equals

total_length
Specifies the total length of the IP packet (including payload) to match.
total_length must be an integer from 0 through 4096.

Usage
Use this command to define rule expressions to match the total length field in IP headers.

Example
The following command defines a rule expression to match user traffic based on IP total length of 2000 bytes:

ip total-length = 2000
ip uplink

This command allows you to define rule expressions to match uplink (subscriber to network) IP packets.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] ip uplink operator condition

---

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be one of the following:
- !=: Does not equal
- ==: Equals

condition
Specifies the condition to match.
condition must be one of the following:
- FALSE
- TRUE

Usage
Use this command to define rule expressions to match uplink (subscriber to network) IP packets.

Example
The following command defines a rule expression to match uplink packets:

    ip uplink = TRUE
ip version

This command allows you to define rule expressions to match the version number in IP headers.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

\[ active-charging service service_name > ruledef ruledef_name \]

Entering the above command sequence results in the following prompt:

\[ [local]host_name(config-acs-ruledef)# \]

**Syntax**

\[ [ no ] ip version operator ip_version \]

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  \textit{operator} \textbf{must} be \texttt{=} (equals).

- **ip_version**
  Specifies the IP version to match.
  \textit{ip_version} \textbf{must} be one of the following:
  - \texttt{ipv4}
  - \texttt{ipv6}

**Usage**
Use this command to define rule expressions to match version number in IP header.

**Example**
The following command defines a rule expression to match user traffic for the IP version \texttt{ipv6}:

\begin{verbatim}
ip version = ipv6
\end{verbatim}
**mms any-match**

This command allows you to define rule expressions to match all Multimedia Messenging Service (MMS) packets.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```bash
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] mms any-match operator condition
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `=`: Equals

- **condition**
  Specifies the condition to match.
  `condition` must be one of the following:
  - `FALSE`
  - `TRUE`

**Usage**

Use this command to define rule expressions to match all MMS packets.

**Example**

The following command defines a rule expression to match all MMS packets:

```
mms any-match = TRUE
```
**mms bcc**

This command allows you to define rule expressions to match recipient addresses in the bcc field of MMS messages.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] mms bcc [ case-sensitive ] operator bcc_address
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **case-sensitive**
  Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

- **operator**
  Specifies how to match.
  
  - !=: Does not equal
  - !contains: Does not contain
  - !ends-with: Does not end with
  - !starts-with: Does not start with
  - =: Equals
  - contains: Contains
  - ends-with: Ends with
  - starts-with: Starts with

- **bcc_address**
  Specifies the “bcc” address/value to match.
  
  - **bcc_address** must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters and space.
**Usage**

Use this command to define rule expressions to match recipient address in the “bcc” field of MMS messages.

**Example**

The following command defines a rule expression to match recipient address containing *test1* in “bcc” field of MMS messages:

```
mms bcc contains test1
```
mms cc

This command allows you to define rule expressions to match recipient addresses in the cc field of MMS messages.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] mms cc [ case-sensitive ] operator cc_address

- no
  If previously configured, deletes the specified rule expression from the current ruledef.

- case-sensitive
  Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

- operator
  Specifies how to match.
  operator must be one of the following:
  - !=: Does not equal
  - !contains: Does not contain
  - !ends-with: Does not end with
  - !starts-with: Does not start with
  - =: Equals
  - contains: Contains
  - ends-with: Ends with
  - starts-with: Starts with

- cc_address
  Specifies the “cc” address/value to match.
  cc_address must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters and space.
mms cc

Usage
Use this command to define rule expressions to match recipient addresses in “cc” field of MMS messages.

Example
The following command defines a rule expression to match recipient address containing test1 in the “cc” field of MMS messages:

```
    mms cc contains test1
```
**mms content location**

This command allows you to define rule expressions to match the content-location field of MMS messages.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

`active-charging service service_name > ruledef ruledef_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] mms content location [ case-sensitive ] operator string
```

- **no**
  
  If previously configured, deletes the specified rule expression from the current ruledef.

- **case-sensitive**
  
  Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

- **operator**
  
  Specifies how to match.

  - **operator** must be one of the following:

    - `!=`: Does not equal
    - `!contains`: Does not contain
    - `!ends-with`: Does not end with
    - `!starts-with`: Does not start with
    - `=`: Equals
    - `contains`: Contains
    - `ends-with`: Ends with
    - `starts-with`: Starts with

- **string**
  
  Specifies the value to match.

  - **string** must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters and space.
Usage
Use this command to define rule expressions to match the content-location field of MMS messages.

Example
The following command defines a rule expression to match `test1` in content-location field of MMS messages:

```
mms content location contains test1
```
mms content type

This command allows you to define rule expressions to match the content-type field of MMS messages.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] mms content type [ case-sensitive ] operator content_type
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **case-sensitive**
  Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

- **operator**
  Specifies how to match.

  - `!=`: Does not equal
  - `!contains`: Does not contain
  - `!ends-with`: Does not end with
  - `!starts-with`: Does not start with
  - `=`: Equals
  - `contains`: Contains
  - `ends-with`: Ends with
  - `starts-with`: Starts with

- **content_type**
  Specifies the MMS content type to match.

  - `content_type` must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters and space.
**Usage**

Use this command to define rule expressions to match content-type field of MMS messages.

**Example**

The following command defines a rule expression to match `image` in content-type field of MMS messages:

```
mms content type contains image
```
mms downlink

This command allows you to define rule expressions to match downlink (network to subscriber) MMS packets.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

`active-charging service service_name > ruledef ruledef_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acss-ruledef)#
```

**Syntax**

```
[ no ] mms downlink operator condition
```

- **no**
  
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  
  Specifies how to match.

  - `!=`: Does not equal
  - `=`: Equals

- **condition**
  
  Specifies the downlink (from the Mobile Node direction) status to match.

  - `FALSE`
  - `TRUE`

**Usage**

Use this command to define rule expressions to match downlink MMS packets.

**Example**

The following command defines a rule expression to match all downlink MMS packets:

```
mms downlink = TRUE
```
**mms from**

This command allows you to define rule expressions to match the “from” field in MMS messages.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] mms from [ case-sensitive ] operator from_address
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **case-sensitive**
  Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

- **operator**
  Specifies how to match.
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `!contains`: Does not contain
  - `!ends-with`: Does not end with
  - `!starts-with`: Does not start with
  - `=`: Equals
  - `contains`: Contains
  - `ends-with`: Ends with
  - `starts-with`: Starts with

- **from_address**
  Specifies the “from” address/value to match.
  `from_address` must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters and space.
Usage
Use this command to define rule expressions to match the “from” field of MMS messages.

Example
The following command defines a rule expression to match test1 in the “from” field of MMS messages:

```
        mms from contains test1
```
mms message-id

This command allows you to define rule expressions to match the message ID field of MMS messages.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] mms message-id [ case-sensitive ] operator message_id

no

If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator

Specifies how to match.

operator must be one of the following:

- !=: Does not equal
- !contains: Does not contain
- !ends-with: Does not end with
- !starts-with: Does not start with
- =: Equals
- contains: Contains
- ends-with: Ends with
- starts-with: Starts with

message_id

Specifies the MMS message ID to match.

message_id must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters.
Usage
Use this command to define rule expressions to match the “message ID” field of MMS messages.

Example
The following command defines a rule expression to match test1 in the “message ID” field of MMS messages:

```
  mms message-id contains test1
```
**mms pdu-type**

This command allows you to define rule expressions to match Protocol Data Unit (PDU) type in the current MMS packets.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] mms pdu-type operator pdu_type
```

- **no**
  - If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  - Specifies how to match.
    - `!=`: Does not equal
    - `=`: Equals

- **pdu_type**
  - Specifies the MMS PDU type to match.
    - `mms_pdu_type_m_acknowledge-ind`
    - `mms_pdu_type_m_delivery-ind`
    - `mms_pdu_type_m_http-get`
    - `mms_pdu_type_m_notification-ind`
    - `mms_pdu_type_m_notify-rsp-ind`
    - `mms_pdu_type_m_retrieve-conf`
    - `mms_pdu_type_m_send-conf`
    - `mms_pdu_type_m_send-request`
    - `mms_pdu_type_m_wsp-get`
    - `mms_pdu_type_response`: This option is deprecated. Use the `mms_pdu_type_m_retrieve_conf` option instead.
Usage
Use this command to define rule expressions to match the PDU type in the current MMS packet.

Example
The following command defines a rule expression to match PDU type `mms-pdu-type-m-http-get` in the current MMS packet:

```
mms pdu-type = mms-pdu-type-m-http-get
```
mms previous-state

This command allows you to define rule expressions to match the previous state of MMS sessions.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] mms previous-state operator mss_previous_state

<table>
<thead>
<tr>
<th>no</th>
</tr>
</thead>
<tbody>
<tr>
<td>If previously configured, deletes the specified rule expression from the current ruledef.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>operator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies how to match.</td>
</tr>
<tr>
<td>operator must be one of the following:</td>
</tr>
<tr>
<td>• !=: Does not equal</td>
</tr>
<tr>
<td>• ==: Equals</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>mms_previous_state</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the previous state to match.</td>
</tr>
<tr>
<td>mms_previous_state must be one of the following:</td>
</tr>
<tr>
<td>• delayed-ack-pending: This option is deprecated, use retrieve-conf-received.</td>
</tr>
<tr>
<td>• delayed-m-notify-rsp-sent: This option is deprecated, use notify-rsp-sent.</td>
</tr>
<tr>
<td>• delayed-retrieval-pending: This option is deprecated, use retrieval-pending.</td>
</tr>
<tr>
<td>• immediate-retrieval-pending: This option is deprecated, use retrieval-pending.</td>
</tr>
<tr>
<td>• init</td>
</tr>
<tr>
<td>• m-send-conf-rcvd: This option is deprecated, use send-success.</td>
</tr>
<tr>
<td>• m-send-req-sent</td>
</tr>
<tr>
<td>• notification-ind-rcvd</td>
</tr>
<tr>
<td>• notify-rsp-sent</td>
</tr>
<tr>
<td>• retrieval-pending</td>
</tr>
<tr>
<td>• retrieve-conf-received</td>
</tr>
<tr>
<td>• send-success</td>
</tr>
</tbody>
</table>
Usage
Use this command to define rule expressions to match the previous state of MMS sessions.

Example
The following command defines a rule expression to match user traffic based on MMS previous state of retrieval-pending:

```
mms previous-state = retrieval-pending
```
mms response status

This command allows you to define rule expressions to match the response status code of MMS messages.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

Syntax

[m no] mms response status operator status_code

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be one of the following:
  • !=: Does not equal
  • ==: Equals

status_code
Specifies the status code to match.
status_code must be an integer from 128 through 136.

Usage
Use this command to define rule expressions to match response status code of MMS messages.

Example
The following command defines a rule expression to match user traffic based on MMS response status code 129:

mms response status = 129
mms state

This command allows you to define rule expressions to match the current state of MMS sessions.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] mms state operator current_state

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be one of the following:
• !=: Does not equal
• ==: Equals

current_state
Specifies current state of MMS session to match.
current_state must be one of the following:
• delayed-ack-pending: This option is deprecated, use retrieve-conf-received.
• delayed-m-notify-rsp-sent: This option is deprecated, use notify-rsp-sent.
• delayed-retrieval-pending: This option is deprecated, use retrieval-pending.
• delivery-failed
• delivery-success
• immediate-retrieval-pending: This option is deprecated, use retrieval-pending.
• m-send-conf-rcvd: This option is deprecated, use send-success.
• m-send-req-sent
• notification-ind-rcvd
• notify-rsp-sent
• retrieval-failed
• retrieval-pending
ACS Ruledef Configuration Mode Commands

mms state

*retrieval-success
*retrieve-conf-received
*send-success

Usage

Use this command to define rule expressions to match the current state of MMS session.

Example

The following command defines a rule expression to match user traffic based on the current state of MMS session as retrieval-failed:

    mms state = retrieval-failed
mms status

This command allows you to define rule expressions to match the current status of MMS sessions.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active - charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] mms status operator status

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be one of the following:
  • !=: Does not equal
  • ==: Equals

status
Specifies the MMS status to match.
status must be an integer from 128 through 132.

Usage
Use this command to define rule expressions to match current status of MMS sessions.

Example
The following command defines a rule expression to match user traffic based on MMS current status 130:

mms status = 130
mms subject

This command allows you to define rule expressions to match the “subject” field of MMS messages.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] mms subject [ case-sensitive ] operator subject_string

---

no

If previously configured, deletes the specified rule expression from the current ruledef.

---

case-sensitive

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

---

operator

Specifies how to match.

operator must be one of the following:

- !=: Does not equal
- !contains: Does not contain
- !ends-with: Does not end with
- !starts-with: Does not start with
- =: Equals
- contains: Contains
- ends-with: Ends with
- starts-with: Starts with

---

subject_string

Specifies the value to match.

subject_string must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters and space.
Usage
Use this command to define rule expressions to match “subject” field of MMS messages.

Example
The following command defines a rule expression to match test1 in the “subject” field of MMS messages:

```
mms subject contains test1
```
**mms tid**

This command allows you to define rule expressions to match the “Transaction Identifier” (TID) field of MMS messages.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] mms tid [ case-sensitive ] operator transaction_id
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **case-sensitive**
  Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

- **operator**
  Specifies how to match.
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `!contains`: Does not contain
  - `!ends-with`: Does not end with
  - `!starts-with`: Does not start with
  - `=`: Equals
  - `contains`: Contains
  - `ends-with`: Ends with
  - `starts-with`: Starts with

- **transaction_id**
  Specifies the MMS TID to match.
  `transaction_id` must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters.
**Usage**

Use this command to define rule expressions to match TID field of MMS messages.

**Example**

The following command defines a rule expression to match test in TID field of MMS messages:

```
mms tid = test
```
mms to

This command allows you to define rule expressions to match the “to” field of MMS messages.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] mms to [ case-sensitive ] operator to_address

no
If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive
Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator
Specifies how to match.
operator must be one of the following:
• !=: Does not equal
• !contains: Does not contain
• !ends-with: Does not end with
• !starts-with: Does not start with
• =: Equals
• contains: Contains
• ends-with: Ends with
• starts-with: Starts with

to_address
Specifies the “to” address/name to match.
to_address must be an alphanumeric string of 1 through 127 characters, and may contain punctuation characters and space.
Usage

Use this command to define rule expressions to match “to” field of MMS messages.

Example

The following command defines a rule expression to match user traffic based on \textit{test} in “to” field of MMS messages:

\begin{verbatim}
mms to = test
\end{verbatim}
**mms uplink**

This command allows you to define rule expressions to match uplink (subscriber to network) MMS packets.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```plaintext
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] mms uplink operator condition
```

- **no**

  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**

  Specifies how to match.

  - `!=`: Does not equal
  - `==`: Equals

- **condition**

  Specifies the uplink (from the Mobile Node direction) status to match.

  - `FALSE`
  - `TRUE`

**Usage**

Use this command to define rule expressions to match uplink MMS packets.

**Example**

The following command defines a rule expression to match uplink MMS packets:

```
mms uplink = TRUE
```
mms version

This command allows you to define rule expressions to match the MMS version in MMS packets.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

Active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] mms version operator version

- no
  If previously configured, deletes the specified rule expression from the current ruledef.

- operator
  Specifies how to match.
  operator must be one of the following:
  - !=: Does not equal
  - ==: Equals

- version
  Specifies the MMS version to match.
  version must be an integer from 1 through 65535.

**Important:** MMS protocol analyzer supports decoding of only MMS version 1.0.

Usage
Use this command to define rule expressions to match MMS version in MMS packets.

Example
The following command defines a rule expression to match MMS version 1.0 in MMS packets:

```
mms version = 1
```
multi-line-or all-lines

This command applies the OR operator to all lines in the current ruledef.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```bash
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs-ruledef) #
```

**Syntax**

```bash
[ no ] multi-line-or all-lines
```

- **no**
  
  If previously configured, deletes this configuration in the current ruledef.

- **multi-line-or all-lines**
  
  Applies the OR operator to all lines in the current ruledef.

**Usage**

When a ruledef is evaluated, if the `multi-line-or all-lines` command is configured, the logical OR operator is applied to all the rule expressions in the ruledef to decide if the ruledef matches or not. If the `multi-line-or all-lines` command is not configured, the logical AND operator is applied to all the rule expressions.

The intent of this command is to allow a single ruledef to specify multiple URL expressions. Otherwise, multiple ruledefs need to be created, each with one URL expression. When this CLI command is used, each expression in the ruledef impacts the total number of ruledefs allowed. So from a “maximum number of possible ruledefs” perspective, it makes no difference whether there are N ruledefs with one expression each, or one ruledef with N expressions.
**p2p any-match**

This command allows you to define rule expressions to match all Peer-to-Peer (P2P) packets.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] p2p any-match operator condition
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  `operator` must be one of the following:
  ```
  • =: Equals
  ```

- **condition**
  Specifies the condition to match.
  `condition` must be one of the following:
  ```
  • TRUE: The rule matches any P2P traffic.
  • FALSE: The rule does not match any P2P traffic.
  ```

**Usage**

Use this command to define rule expressions to match all P2P packets.

**Example**

The following command defines a rule expression to match all P2P packets:

```
p2p any-match = TRUE
```
p2p behavioral

This command allows you to define rule expressions to match behavioral detection type — P2P, VoIP, Behavioral Upload or Behavioral Download.

Product
ACS, ADC

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

Syntax
[ no ] p2p behavioral operator behavioral_list

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be one of the following:
- !=: Does not equal
- ==: Equals

behavioral_list
Specifies the behavior to match. The behavioral list is the list of supported behavioral detection logic populated from the currently loaded ADC plugin.
behavioral_list must be one of the following:
- download: Detects unknown flows which are data download using behavioral analysis
- p2p: Detects P2P/file sharing protocols using behavioral analysis
- upload: Detects unknown flows which are data upload using behavioral analysis
- video: Detects video flows using behavioral analysis
- voip: Detects VoIP (voice and video) protocols using behavioral analysis

Usage
Use this command to define rule expressions to detect behavioral protocols. Behavioral P2P and behavioral VoIP are meant for zero day detection of P2P/file sharing protocols and VoIP traffic respectively. Behavioral upload/download is similar to client-server upload/download using HTTP, FTP, SFTP, etc. It must also detect flows of non-standard ports which ECS cannot detect and falls under the client-server model. This feature is
disabled by default and meant only for statistical purposes (not for charging purposes). For detection purposes use the `p2p-detection behavioral` command in the ACS Configuration Mode.

**Example**

The following command specifies to configure behavioral VoIP:

```
p2p behavioral = voip
```
p2p protocol

This command allows you to define rule expressions to match P2P protocol. This command must be used for charging purposes. It must **not** be used for detection purposes.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] p2p protocol operator protocol
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  `operator` must be `=` (equals).

- **protocol**
  Specifies the protocol to match.
  `protocol` must be one of the following:
  - `actionvoip`
  - `actsync`
  - `adobeconnect`
  - `aimini`
  - `amazoncloud`
  - `antsp2p`
  - `apple-push`
  - `apple-store`
  - `applejuice`
  - `applemaps`
  - `ares`
  - `armagettron`
  - `avi`
• badoo
• baidumovie
• battlefld
• bbm
• bitcasa
• bittorrent
• bittorrent-sync
• blackberry-store
• blackberry
• blackdialer
• box
• callofduty
• chikka
• cisco-jabber
• citrix
• clubbox
• clubpenguin
• comodounite
• crossfire
• cyberghost
• ddlink
• didi
• directconnect
• dofus
• dropbox
• ebuddy
• edonkey
• facebook
• facetime

**Important:** The **facetime** protocol is available only in 9.0 and in 11.0 and later releases.

• fasttrack
• feidian
• fical
• fiesta
• filetopia
• flash
• flickr
• florensia
• foursquare
• freenet
• friendster
• fring
• funshion
• gadugadu
• gamekit

**Important:** The gamekit protocol is available only in 9.0 and in 11.0 and later releases.

• gmail
• gnutella
• goober
• google-music
• google-push
• google
• googleplay
• googleplus
• gotomeeting
• gtalk
• guildwars
• halflife2
• hamachivpn
• hbogo
• heytell
• hike-messenger
• hls
• hotspotvpn
• hulu
• hyves
• iax
• icall
• icecast
• icloud
• idrive
• igo
• iheartradio
• imesh
• imessage
• imgur
• imo
• implus
• instagram
• iplayer
• iptv
• irc
• isakmp
• iskoot
• itunes
• jabber
• jap
• jumblo
• kakaotalk
• kik-messenger
• kontiki
• kugoo
• kuro
• linkedin
• lync
• magicjack
• manolito
• mapfactor
• mapi
• maplestory
• meebo
• mgcp
• mig33
• mojo
• monkey3
• mozy
• mozy
• msrp
• mute
• mypeople
• myspace
• nateontalk
• naverline
• navigon
• netflix
• netmotion
• nimbuzz
• nokia-store
• octoshape
• off
• ogg
• oist
• oovoo
• opendrive
• openft
• openvpn
• operamini
• orb
• oscar
• outlook
• paltalk
• pando
• pandora
• path
• pcanywhere
• pinterest
• plingm
• poco
• popo
• pplive
• ppstream
• ps3
• qq
• qqgame
• qqlive
• quake
• quicktime
• radio-paradise
• rdp
• rdt
• regram
• rfactor
• rhapsody
• rmstream
• rodi
• ryn ga
• samsung-store
• scydo
• secondlife
• shoutcast
• silverlight
• siri
• skinny
• skydrive
• skype
• slacker-radio
• slingbox
• smartvoip
• snapchat
• softether
• sopcast
• soribada
• soulseek
• spdy
• speedtest
• splashfighter
• spotify
• ssdp
• stealthnet
• steam
• stun
• sudaphone
• svtplay
• tagged
• talkatone
• tango
• teamspeak
• teamviewer
• telegram
• thunder
• tor
• truecaller
• truphone
• tumblr
• tunnelvoice
• tvants
• tvuplayer
• twitter
• twitch
• ultrabac
• ultrasurf
• upc-phone
• usenet
• ustream
• usee
• vchat
• veohtv
• viber
• vine
• voipdiscount
• vopium
• voxer
• vpnx
• vtok
• vtun
• warcft3
• waze
• webex
p2p protocol

Usage

Use this command to define rule expressions to detect P2P protocols for charging purposes. For detection purposes use the `p2p-detection protocol` command in the ACS Configuration Mode.

Example

The following command specifies to detect orb protocol for charging purposes:

```
p2p protocol = orb
```
**p2p protocol-group**

This command allows you to define rule expressions to match ADC application/protocol group.

**Product**
ACS, ADC

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

`active-charging service service_name > ruledef ruledef_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] p2p protocol-group operator group_list
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match. `operator` must be one of the following:
  - `!=`: Does not equal
  - `=`: Equals

- **group_list**
  Specifies the ADC application/protocol group to match. `group_list` must be one of the following:
  - `anonymous-access`: Anonymous internet access protocols mainly used for illegal purposes.
  - `business`: Applications/Protocols used for business purposes.
  - `communicator`: Applications/Protocols used mainly for messaging which includes IM, IM based file transfer, VoIP or video chats.
  - `cloud`: Applications/Protocols for cloud service.
  - `e-mail`: Applications/Protocols used for electronic mail.
  - `e-news`: Applications/Protocols used for internet news and magazine reading.
  - `e-store`: Applications/Protocols used for electronic stores.
  - `internet-privacy`: Applications/Protocols used for file transfers.
  - `filesharing`: Applications/Protocols used for gaming.
  - `gaming`: Standard protocols used in internet.
  - `p2p-filesharing`: Applications/Protocols used for creating a virtual network over internet mainly for business purposes.
**p2p-anon-filesharing**: Peer to Peer application/protocols used for anonymous filesharing.

**remote-control**: Peer to Peer application/protocols used for filesharing.

**social-nw-game**: Application/Protocols used for remote management.

**social-nw-generic**: Application/Protocols used for social networking games.

**social-nw-videoconf**: Application/Protocols used for social networking.

**standard**: Application/Protocols used for social network video conference.

**streaming**: Application/Protocols used for streaming audio and video.

**untagged**: Default group for protocols not otherwise classified.

---

**Usage**

Use this command to define rule expressions to match ADC protocol group. The list of P2P applications/protocols is populated from the currently loaded P2P plugin.

**Example**

The following command specifies to detect the `gaming` protocol group:

```
p2p protocol-group = gaming
```
p2p traffic-type

This command allows you to define rule expressions to match the traffic type.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] p2p traffic-type operator traffic_type

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be one of the following:
- !=: Does not equal
- ==: Equals

traffic_type
Specifies the traffic type to match.
In 11.0 and later releases, traffic_type must be one of the following:
- audio
- file-transfer
- im
- unclassified
- video
- voipout
In 10.0 and earlier releases, the supported traffic_type was voice.

Usage
Use this command to configure the system to detect voice or non-voice P2P traffic. When the detection of a protocol is enabled then the detection of sub-type is enabled by default.

Example
The following command configures the system to detect video traffic:
p2p traffic-type = video
pop3 any-match

This command allows you to define rule expressions to match all Post Office Protocol 3 (POP3) packets.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

Syntax
[ no ] pop3 any-match operator condition

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be one of the following:
• !=: Does not equal
• ==: Equals

condition
Specifies the condition to match.
condition must be one of the following:
• FALSE
• TRUE

Usage
Use this command to define rule expressions to match all POP3 packets.

Example
The following command defines a rule expression to match all POP3 packets:

    pop3 any-match = TRUE
pop3 command args

This command allows you to define rule expressions to match POP3 command arguments.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] pop3 command args [ case-sensitive ] operator argument

no
If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive
Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator
Specifies how to match.
operator must be one of the following:

• !=: Does not equal
• !contains: Does not contain
• !ends-with: Does not end with
• !starts-with: Does not start with
• :=: Equals
• contains: Contains
• ends-with: Ends with
• starts-with: Starts with

argument
Specifies the command argument to match.
argument must be an alphanumeric string of 1 through 40 characters, and may contain punctuation characters.
Usage
Use this command to define rule expressions to match POP3 command argument.

Example
The following command defines a rule expression to match POP3 command argument test:

```plaintext
pop3 command args = test
```
### pop3 command id

This command allows you to define rule expressions to match POP3 command ID.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] pop3 command id operator command_id
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `<=`: Lesser than or equals
  - `=`: Equals
  - `>=`: Greater than or equals

- **command_id**
  Specifies the command ID to match.
  `command_id` must be an integer from 1 through 12.

**Usage**

Use this command to define rule expressions to match a POP3 command ID.

**Example**

The following command defines a rule expression to match POP3 command ID 8:

```
pop3 command id = 8
```
**pop3 command name**

This command allows you to define rule expressions to match command sent within a POP3 packet.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

`active-charging service service_name > ruledef ruledef_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] pop3 command_name operator command_name
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  - **operator** must be one of the following:
    - `!=`: Does not equal
    - `=`: Equals

- **command_name**
  Specifies the command name to match.
  - **command_name** must be one of the following:
    - `apop`
    - `dele`
    - `list`
    - `noop`
    - `pass`
    - `quit`
    - `retr`
    - `reset`
    - `stat`
    - `top`
    - `uidl`
    - `user`
Usage
Use this command to define rule expressions to match commands sent within POP3 packets.

Example
The following command defines a rule expression to match the `list` command sent in POP3 packets:

```plaintext
  pop3 command name = list
```
pop3 mail-size

This command allows you to define rule expressions to match POP3 mail size.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acsc-ruledef)#

Syntax

[ no ] pop3 mail-size { operator mail_size | { range | !range } range_from to range_to }

---

no

If previously configured, deletes the specified rule expression from the current ruledef.

---

operator

Specifies how to match.

operator must be one of the following:

- !=: Does not equal
- <=: Lesser than or equals
- =: Equals
- >=: Greater than or equals

---

{ range | !range } range_from to range_to

Enables or disables the range criteria.

- range: Enables the range criteria.
- !range: Disables the range criteria.

- range_from: Specifies start of the range.
  range_from must be an integer from 1 through 4000000000.

- range_to: Specifies the end range.
  range_to must be an integer from 1 through 4000000000, and must be greater than range_from.

---

mail_size

Specifies the mail size to match.

mail_size must be an integer from 1 through 4000000000.
Usage

Use this command to define rule expressions to match POP3 mail size.

Example

The following command defines a rule expression to match POP3 mail size of 40000:

```
pop3 mail-size = 40000
```
pop3 pdu-length

This command allows you to define rule expressions to match the Protocol Data Unit (PDU) length of POP3 packets equal to the POP3 header plus POP3 payload.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef) #

Syntax

[ no ] pop3 pdu-length { operator pdu_length | { range | !range } range_from to range_to } }

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- !=: Does not equal
- <=: Lesser than or equals
- =: Equals
- >=: Greater than or equals

{ range | !range } range_from to range_to

Enables or disables the range criteria.

- range: Enables the range criteria.
- !range: Disables the range criteria.

- range_from: Specifies the start of range as an integer from 0 through 65535.

- range_to: Specifies the end range. range_to must be an integer from 0 through 65535, and must be greater than range_from.

pdu_length

Specifies the POP3 PDU length to match.
pdu_length must be an integer from 0 through 65535.
Usage
Use this command to define rule expressions to match POP3 PDU length (header + payload) in bytes.

Example
The following command defines a rule expression to match PDU length of 1000 bytes:

```
pop3 pdu-length = 1000
```
pop3 pdu-type

This command allows you to define rule expressions to match POP3 Protocol Data Unit (PDU) type.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] pop3 pdu-type operator pdu_type

- no
  If previously configured, deletes the specified rule expression from the current ruledef.

- operator
  Specifies how to match.
  operator must be one of the following:
  - !=: Does not equal
  - ==: Equals

- pdu_type
  Specifies the POP3 PDU type to match.
  pdu_type must be one of the following:
  - command-packet
  - data-packet
  - relay-packet

Usage
Use this command to define rule expressions to match POP3 PDU type.

Example
The following command defines a rule expression to match POP3 PDU type relay-packet:

    pop3 pdu-type = relay-packet
**pop3 previous-state**

This command allows you to define rule expressions to match the previous state of POP3 sessions.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

`active-charging service service_name > ruledef ruledef_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] pop3 previous-state operator pop3_previous_state
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `=`: Equals

- **pop3_previous_state**
  Specifies the previous state to match.
  `pop3_previous_state` must be one of the following:
  - `connected`: Connected state
  - `data transaction`: Data transaction state
  - `init`: Initialized state
  - `reply-error`: Reply error state
  - `reply-ok`: Response ok state
  - `waiting-for-reply`: Waiting for reply state

**Usage**

Use this command to define rule expressions to match a POP3 previous state.

**Example**

The following command defines a rule expression to match user traffic for a POP3 previous state of `connected`:

```
pop3 previous-state = connected
```
pop3 reply args

This command allows you to define rule expressions to match specified arguments with POP3 reply.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acis-ruledef)#

Syntax

[ no ] pop3 reply args [ case-sensitive ] operator argument

---

no
If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive
Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator
Specifies how to match.
operator must be one of the following:
- !=: Does not equal
- !contains: Does not contain
- !ends-with: Does not end with
- !starts-with: Does not start with
- =: Equals
- contains: Contains
- ends-with: Ends with
- starts-with: Starts with

---

argument
Specifies the reply argument to match.
In 11.0 and earlier releases, argument must be an alphanumeric string of 1 through 512 characters, and may contain punctuation characters.
In 12.0 and later releases, argument must be an alphanumeric string of 1 through 127 characters, and may contain punctuation characters.
Usage
Use this command to define rule expressions to match specified arguments within a POP3 reply.

Example
The following command defines a rule expression to match the argument test with POP3 replies:

```plaintext
pop3 reply args = test
```
pop3 reply id

This command allows you to define rule expressions to match POP3 reply ID.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] pop3 reply id operator reply_id

- no
  If previously configured, deletes the specified rule expression from the current ruledef.

- operator
  Specifies how to match.
  operator must be one of the following:
  - !=: Does not equal
  - ==: Equals

- reply_id
  Specifies the POP3 reply ID to match.
  reply_id must be one of the following:
  - 0: Unknown reply
  - 1: +OK
  - 2: -Error

Usage
Use this command to define rule expressions to match POP3 reply ID.

Example
The following command defines a rule expression to match POP3 reply ID of 2:

  pop3 reply id = 2
pop3 reply status

This command allows you to define rule expressions to match POP3 reply status.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] pop3 reply status operator reply_status

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be one of the following:

• !=: Does not equal
• ==: Equals

reply_status
Specifies the reply status to match.
reply_status must be one of the following:

• +OK: Reply OK
• -ERR: Reply error

Usage
Use this command to define rule expressions to match POP3 reply status.

Example
The following command defines a rule expression to match POP3 reply status +OK:

        pop3 reply status = +OK
**pop3 session-length**

This command allows you to define rule expressions to match POP3 session-length.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] pop3 session-length { operator session_length | { range | !range } range_from to range_to }
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  
  - **!=**: Does not equal
  - **<=**: Lesser than or equals
  - **==**: Equals
  - **>=**: Greater than or equals

- **session_length**
  Specifies the POP3 session length to match.
  `session_length` must be an integer from 1 through 4000000000.

- **{ range | !range } range_from to range_to**
  Enables or disables the range criteria for POP3 session length.
  - **range**: Enables the range criteria for POP3 session length.
  - **!range**: Disables the range criteria for POP3 session length.
  - **range_from**: Specifies the start of range of POP3 session as an integer from 1 through 4000000000, but less than or equal to `range_to`.
  - **range_to**: Specifies the end of range of POP3 session as an integer from 1 through 4000000000, but greater than or equal to `range_from`.
Usage
Use this command to define rule expressions to match the total length of POP3 sessions.

Example
The following command defines a rule expression to match a POP3 session length of 40000:

```
pop3 session-length = 40000
```
pop3 state

This command allows you to define rule expressions to match the current state of POP3 sessions.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

`active-charging service service_name > ruledef ruledef_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] pop3 state operator current_state
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `==`: Equals

- **current_state**
  Specifies the current state to match.
  `current_state` must be one of the following:
  - `close`
  - `connected`
  - `data-transaction`
  - `reply-error`
  - `reply-ok`
  - `waiting-for-reply`

**Usage**
Use this command to define rule expressions to match the current state of POP3 sessions.

**Example**
The following command defines a rule expression to match the POP3 current state `close`:

```
pop3 state = close
```
pop3 user-name

This command allows you to define rule expressions to match POP3 user name.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acsc-ruledef)#

Syntax

[ no ] pop3 user-name [ case-sensitive ] operator user_name

no
If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive
Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator
Specifies how to match.
operator must be one of the following:

• !=: Does not equal
• !=contains: Does not contain
• !=ends-with: Does not end with
• !=starts-with: Does not start with
• =: Equals
• contains: Contains
• ends-with: Ends with
• starts-with: Starts with

user_name
Specifies the POP3 user name to match.
user_name must be an alphanumeric string of 1 through 64 characters, and may contain punctuation characters and space.
Usage
Use this command to define rule expressions to match POP3 user name.

Example
The following command defines a rule expression to match POP3 user name `test`:

```
    pop3 user-name = test
```
**pppt any-match**

This command allows you to define a rule expression to match all Point-to-Point Tunneling Protocol (PPTP) packets.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

`active-charging service service_name > ruledef ruledef_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] pptp any-match operator condition
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  * operator must be one of the following:
    - `!=`: Does not equal
    - `=`: Equals

- **condition**
  Specifies the condition to match.
  * condition must be one of the following:
    - `FALSE`
    - `TRUE`

**Usage**

Use this command to specify a ruledef to analyze user traffic based on the PPTP any match status.

**Example**

The following command creates a PPTP ruledef for analyzing user traffic using a PPTP any match status of `FALSE`:

```
pptp any-match = FALSE
```
**pptp ctrl-msg-type**

This command allows you to define rule expressions to match control message type in PPTP packets.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] pptp ctrl-msg-type = message_type
```

- **no**
  - If previously configured, deletes the specified rule expression from the current ruledef.

```
message_type
```

- message_type must be one of the following:
  - `call-clear-request`
  - `call-disconnect-notify`
  - `echo-reply`
  - `echo-request`
  - `incoming-call-connected`
  - `incoming-call-reply`
  - `incoming-call-request`
  - `outgoing-call-reply`
  - `outgoing-call-request`
  - `set-link-info`
  - `start-control-connection-reply`
  - `start-control-connection-request`
  - `stop-control-connection-reply`
  - `stop-control-connection-request`
  - `wan-error-notify`

**Usage**

Use this command to define rule expressions to match the control message type in PPTP packets.
Example

The following command specifies to match *echo-reply* message type:

```
pptp ctrl-msg-type = echo-reply
```
**pptp gre any-match**

This command allows you to define rule expressions to match all PPTP Generic Routing Encapsulation (GRE) packets.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

**Syntax**

```
[ no ] pptp gre any-match = condition
```

- **no**
  - If previously configured, deletes the specified rule expression from the current ruledef.

- **condition**
  - *condition* must be one of the following:
    - FALSE
    - TRUE

**Usage**

Use this command to define rule expressions to match all PPTP GRE packets.

**Example**

The following command defines a rule expression to match all PPTP GRE packets:

```
pptp gre any-match = TRUE
```
radius state

This command allows you to define rule expressions to match the current state of an RADIUS session.

Product

- GGSN
- PDSN
- P-GW

Privilege

- Security Administrator, Administrator

Mode

- Exec > ACS Configuration > Ruledef Configuration
- active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

Syntax

```
[ no ] radius state operator radius_state
```

- `no`
  
  If previously configured, deletes the specified rule expression from the current ruledef.

- `operator`
  
  Specifies how to match.
  
  - `!=`: Does not equal
  
  - `=`: Equals

- `radius_state`
  
  Specifies the RADIUS state to match.
  
  `radius_state` must be one of the following:
  
  - `auth-req-rcvd`: Analyzer received the Access-Request message from the client.
  
  - `auth-rsp-fail`: Analyzer received the Access-reject message from the server.
  
  - `auth-rsp-success`: Analyzer received the Access-Accept message from the server as a reply to Access-request.

Usage

Use this command to define rule expressions to match the current state of an RADIUS session.

Example

The following command defines a rule expression to match RADIUS current state `close`:

```
radius state = close
```
rtcp any-match

This command allows you to define rule expressions to match all Real-Time Transport Control Protocol (RTCP) packets.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acis-ruledef)#
```

**Syntax**

```
[ no ] rtcp any-match operator condition
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  ```
  operator must be one of the following:
  • !=: Does not equal
  • ==: Equals
  ```

- **condition**
  Specifies the condition to match.
  ```
  condition must be one of the following:
  • TRUE: The rule matches any RTCP traffic.
  • FALSE: The rule does not match any RTCP traffic.
  ```

**Usage**

Use this command to define rule expressions to match all RTCP packets.

**Example**

The following command defines a rule expression to match all RTCP packets:

```
rtcp any-match = TRUE
```
rtcp jitter

This command allows you to define rule expressions to match the jitter parameter in RTCP packets.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] rtcp jitter operator jitter
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match. 
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `<=`: Lesser than or equals
  - `=`: Equals
  - `>=`: Greater than or equals

- **jitter**
  Specifies the RTCP inter-arrival jitter value (in milliseconds) to match. 
  `jitter` must be an integer from 0 through 4294967295.

**Usage**

Use this command to define rule expressions to match jitter parameter found in the RTCP sender report or receiver report packets.

**Example**

The following command matches packets for jitter greater than or equal to 1295 milliseconds:

```
rtcp jitter >= 1295
```
rtcp parent-proto

This command allows you to define rule expressions to match the parent protocol of the RTCP flow.

⚠️ **Important:** This command is available only in 8.1 and 9.0 and later releases.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] rtcp parent-proto operator parent_protocol
```

- **no**
  - If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  - Specifies how to match.
  - `operator` must be one of the following:
    - `!=`: Does not equal
    - `==`: Equals

- **parent_protocol**
  - Specifies the RTCP parent protocol to match.
  - `parent_protocol` must be one of the following:
    - `rtsp`: Real Time Streaming Protocol
    - `sip`: Session Initiation Protocol

**Usage**

Use this command to define rule expressions to match user traffic based on the parent protocol of the RTCP flow.

**Example**

The following command defines a rule expression to match user traffic based on SIP being the parent protocol of the RTCP flow:

```
rtcp parent-proto = sip
```
rtcp pdu-length

This command allows you to define rule expressions to match Protocol Data Unit (PDU) length of RTCP packets, (RTCP header + RTCP payload).

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] rtcp pdu-length operator pdu_length

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be one of the following:

• !=: Does not equal
• <=: Lesser than or equals
• ==: Equals
• >=: Greater than or equals

pdu_length
Specifies the RTCP length (in bytes) to match.
In 8.1 and later releases, pdu_length must be an integer from 1 through 65535.
In 8.0, pdu_length must be an integer from 1 through 2000.

Usage
Use this command to define rule expressions to match RTCP PDU length (header + payload) in bytes.

Example
The following command defines a rule expression to match user traffic based on an RTCP PDU length of 10000 bytes:

    rtcp pdu-length = 10000
rtcp rtsp-id

This command allows you to define rule expressions to match user traffic based on a Real-time Streaming Protocol (RTSP) ID associated with an RTCP flow.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration
active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] rtcp rtsp-id [ case-sensitive ] operator rtsp_id

no
If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive
Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator
Specifies how to match.
operator must be one of the following:
  • !=: Does not equal
  • !contains: Does not contain
  • !ends-with: Does not end with
  • !starts-with: Does not start with
  • =: Equals
  • contains: Contains
  • ends-with: Ends with
  • starts-with: Starts with

rtsp_id
Specifies the value to match.
rtsp_id must be an alphanumeric string of 1 through 32 characters.
Usage
Use this command to define rule expressions to match an RTSP ID associated with an RTCP flow.

Example
The following command defines a rule expression to match user traffic containing RTSP message ID of test1:

```
rtcp rtsp-id contains test1
```
rtcp session-length

This command allows you to define rule expressions to match the total length of RTCP sessions.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] rtcp session-length operator session_length

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be one of the following:
- !=: Does not equal
- <=: Lesser than or equals
- ==: Equals
- >=: Greater than or equals

session_length
Specifies the RTCP total session length (in bytes) to match.
In 8.1 and later releases, session_length must be an integer from 1 through 4000000000.
In 8.0, session_length must be an integer from 1 through 400000000.

Usage
Use this command to define rule expressions to match RTCP total session length.

Example
The following command defines a rule expression to match user traffic for a total RTCP session length of 200000:

rtcp session-length = 200000
rtcp uri

This command allows you to define rule expressions to match URI associated with RTCP flows.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] rtcp uri [ case-sensitive ] operator uri

- no
  If previously configured, deletes the specified rule expression from the current ruledef.

- case-sensitive
  Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

- operator
  Specifies how to match.
  operator must be one of the following:
  • !=: Does not equal
  • !=contains: Does not contain
  • !=ends-with: Does not end with
  • !=starts-with: Does not start with
  • =: Equals
  • contains: Contains
  • ends-with: Ends with
  • starts-with: Starts with

- uri
  Specifies the URI to match.
  uri must be an alphanumeric string of 1 through 127 characters and may include punctuation characters.

Usage

Use this command to define rule expressions to match URI associated with RTCP flow.
Example

The following command defines a rule expression to match user traffic for RTCP URI `rtsp://www.example.org`:

```
rtcp uri = rtsp://www.example.org
```
rtp any-match

This command allows you to define rule expressions to match all Real-time Transport Protocol (RTP) packets.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] rtp any-match operator condition

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be one of the following:
  • ! =: Does not equal
  • =: Equals

condition
Specifies the condition to match.
condition must be one of the following:
  • FALSE
  • TRUE

Usage
Use this command to define rule expressions to match all RTP packets.

Example
The following command defines a rule expression to match all RTP packets:

   rtp any-match = TRUE
rtp parent-proto

This command allows you to define rule expressions to match the parent protocol of the RTP flow.

⚠️ **Important:** This command is available only in 8.1 and in 9.0 and later releases.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] rtp parent-proto operator parent_protocol
```

- **no**
  
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  
  Specifies how to match.
  
  `operator` must be one of the following:
  
  - `!=`: Does not equal
  - `==`: Equals

- **parent_protocol**
  
  Specifies the RTP parent protocol to match.
  
  `parent_protocol` must be one of the following:
  
  - `rtsp`: Real Time Streaming Protocol
  - `sip`: Session Initiation Protocol

**Usage**

Use this command to define rule expressions to match user traffic based on the parent protocol of the RTP flow.

**Example**

The following command defines a rule expression to match user traffic with parent protocol of the RTP flow being SIP:

```
rtp parent-proto = sip
```
**rtp pdu-length**

This command allows you to define rule expressions to match PDU length of RTP packets, equal to the RTP header + RTP payload.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] rtp pdu-length operator pdu_length
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `<=`: Lesser than or equals
  - `=`: Equals
  - `>=`: Greater than or equals

- **pdu_length**
  Specifies the RTP PDU length (in bytes) to match.
  In 8.1 and later releases, `pdu_length` must be an integer from 1 through 65535.
  In 8.0, `pdu_length` must be an integer from 1 through 2000.

**Usage**

Use this command to define rule expressions to match PDU length (header + payload) of RTP packets in bytes.

**Example**

The following command defines a rule expression to match an RTP PDU length of 1000 bytes:

```
rtp pdu-length = 1000
```
rtp rtsp-id

This command allows you to define rule expressions to match RTSP ID associated with RTP flows.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > ACS Configuration > Ruledef Configuration

`active-charging service service_name > ruledef ruledef_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] rtp rtsp-id [ case-sensitive ] operator rtsp_id
```

- **no**
  
  If previously configured, deletes the specified rule expression from the current ruledef.

- **case-sensitive**
  
  Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

- **operator**
  
  Specifies how to match.
  
  `operator` must be one of the following:

  - `!=`: Does not equal
  - `!contains`: Does not contain
  - `!ends-with`: Does not end with
  - `!starts-with`: Does not start with
  - `=`: Equals
  - `contains`: Contains
  - `ends-with`: Ends with
  - `starts-with`: Starts with

- **rtsp_id**
  
  Specifies the RTSP ID to match.
  
  `rtsp_id` must be an alphanumeric string of 1 through 32 characters.

**Usage**

Use this command to define rule expressions to match RTSP ID associated with RTP flows.
Example

The following command defines a rule expression to match RTSP message ID of `test1`:

```
rtp rtsp-id contains test1
```
rtp session-length

This command allows you to define rule expressions to match the total length of RTP sessions.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] rtp session-length operator session_length

<table>
<thead>
<tr>
<th>no</th>
</tr>
</thead>
</table>
| If previously configured, deletes the specified rule expression from the current ruledef.

<table>
<thead>
<tr>
<th>operator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies how to match.</td>
</tr>
<tr>
<td>operator must be one of the following:</td>
</tr>
<tr>
<td>• !=: Does not equal</td>
</tr>
<tr>
<td>• &lt;=: Lesser than or equals</td>
</tr>
<tr>
<td>• =: Equals</td>
</tr>
<tr>
<td>• &gt;=: Greater than or equals</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>session_length</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the RTP total session length (in bytes) to match.</td>
</tr>
<tr>
<td>In 8.1 and later releases, session_length must be an integer from 1 through 400000000.</td>
</tr>
<tr>
<td>In release 8.0, session_length must be an integer from 1 through 4000000.</td>
</tr>
</tbody>
</table>

Usage

Use this command to define rule expressions to match the RTP total session length. The session-length is calculated by adding together the “rtp pdu-length” values of all relevant packets.

Example

The following command defines a rule expression to match a total RTP session length of 200000:

rtp session-length = 200000
rtp uri

This command allows you to define rule expressions to match the media URI associated with RTP flows.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] rtp uri [ case-sensitive ] operator uri

---

no

If previously configured, deletes the specified rule expression from the current ruledef.

---

case-sensitive

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

---

operator

Specifies how to match.

operator must be one of the following:

- !=: Does not equal
- !contains: Does not contain
- !ends-with: Does not end with
- !starts-with: Does not start with
- =: Equals
- contains: Contains
- ends-with: Ends with
- starts-with: Starts with

---

uri

Specifies the RTP URI to match.

uri must be an alphanumeric string of 1 through 127 characters. uri allows punctuation characters and excludes the “host” portion.
Usage

Use this command to define rule expressions to match media URI associated with RTP flow.

Example

The following command defines a rule expression to match the RTP URI string
rtsp://www.example.org:

\[ \text{rtp uri} = \text{rtsp://www.example.org} \]
rtsp any-match

This command allows you to define rule expressions to match all Real Time Streaming Protocol (RTSP) packets.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] rtsp any-match operator condition

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be one of the following:
• !=: Does not equal
• =: Equals

condition
Specifies the condition to match.
condition must be one of the following:
• FALSE
• TRUE

Usage
Use this command to define rule expressions to match all RTSP packets.

Example
The following command defines a rule expression to match all RTSP packets:

rtsp any-match = TRUE
rtsp content length

This command allows you to define rule expressions to match the content length field in RTSP header.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] rtsp content length operator content_length
```

- **no**
  
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  
  Specifies how to match.

  **operator** must be one of the following:
  
  - !=: Does not equal
  - <=: Lesser than or equals
  - ==: Equals
  - >=: Greater than or equals

- **content_length**
  
  Specifies the content length (in bytes) to match.

  **content_length** must be an integer from 0 through 65535.

**Usage**

Use this command to define rule expressions to match “content length” field in RTSP headers.

**Example**

The following command defines a rule expression to match content length of 10000 in RTSP headers:

```
rtsp content length = 10000
```
**rtsp content type**

This command allows you to define rule expressions to match the content type field in RTSP headers.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

`active-charging service service_name > ruledef ruledef_name`

Entering the above command sequence results in the following prompt:

`[local]host_name(config-acs-ruledef)#`

**Syntax**

```
[ no ] rtsp content type [ case-sensitive ] operator content_type
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **case-sensitive**
  Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

- **operator**
  Specifies how to match.
  - `!=`: Does not equal
  - `!contains`: Does not contain
  - `!ends-with`: Does not end with
  - `!starts-with`: Does not start with
  - `=`: Equals
  - `contains`: Contains
  - `ends-with`: Ends with
  - `starts-with`: Starts with

- **content_type**
  Specifies the content type to match.
  - `content_type` must be an alphanumeric string of 1 through 127 characters, and may contain punctuation characters.
Usage

Use this command to define rule expressions to match “content type” field in RTSP headers.

Example

The following command defines a rule expression to match RTSP content type $abc100$:

```
rtsp content type = abc100
```
rtsp date

This command allows you to define rule expressions to match the date field in the RTSP message headers.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

`active-charging service service_name > ruledef ruledef_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acss-ruledef)#
```

**Syntax**

```
[ no ] rtsp date [ case-sensitive ] operator date
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **case-sensitive**
  Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

- **operator**
  Specifies how to match.
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `!contains`: Does not contain
  - `!ends-with`: Does not end with
  - `!starts-with`: Does not start with
  - `=`: Equals
  - `contains`: Contains
  - `ends-with`: Ends with
  - `starts-with`: Starts with

- **date**
  Specifies the date in RTSP header to match.
  `date` must be an alphanumeric string of 1 through 127 characters, and may contain punctuation characters.

**Usage**

Use this command to define rule expressions to match the “date” field in the RTSP message headers.
Example

The following command defines a rule expression to match the date `12_04_2006` in RTSP message headers:

```plaintext
trsp date = 12_04_2006
```
rtsp previous-state

This command allows you to define rule expressions to match the previous state of RTSP sessions.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration
active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] rtsp previous-state operator rtsp_previous_state

- no
  If previously configured, deletes the specified rule expression from the current ruledef.

- operator
  Specifies how to match.
  operator must be one of the following:
  • !=: Does not equal
  • =: Equals

- rtsp_previous_state
  Specifies the previous state to match.
  rtsp_previous_state must be one of the following:
  • init
  • open
  • play
  • ready
  • record

Usage
Use this command to define rule expressions to match the previous state of RTSP sessions.

Example
The following command defines a rule expression to match RTSP previous state ready:

rtsp previous-state = ready
rtsp reply code

This command allows you to define rule expressions to match the return code in RTSP responses.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] rtsp reply code operator reply_code
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  *operator* must be one of the following:
  - `!=`: Does not equal
  - `<=`: Lesser than or equals
  - `=`: Equals
  - `>=`: Greater than or equals

- **reply_code**
  Specifies the RTSP reply code to match.
  *reply_code* must be an integer from 100 through 599.

**Usage**
Use this command to define rule expressions to match the return code in RTSP response.

**Example**
The following command defines a rule expression to match RTSP return code 302:

```
rtsp reply code = 302
```
rtsp request method

This command allows you to define rule expressions to match the method in RTSP responses.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] rtsp request method operator request_method

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be one of the following:
• !=: Does not equal
• ==: Equals

request_method
Specifies the RTSP request method to match.
request_method must be one of the following requests:
• announce
• describe
• get-parameter
• options
• pause
• play
• record
• redirect
• set-parameter
• setup
• teardown
rtsp request method

Usage
Use this command to define rule expressions to match the method in RTSP responses.

Example
The following command defines a rule expression to match RTSP request method `announce`:

```
rtsp request method = announce
```
rtsp request packet

This command allows you to define rule expressions to match all RTSP request messages.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

**Syntax**

```
[ no ] rtsp request packet operator condition
```

- no
  - If previously configured, deletes the specified rule expression from the current ruledef.

- operator
  - Specifies how to match.
  - `!` is one of the following:
    - `!`: Does not equal
    - `=`: Equals

- condition
  - Specifies the condition to match.
  - `TRUE`: Is request
  - `FALSE`: Is response

**Usage**
Use this command to define rule expressions to match all RTSP request messages.

**Example**
The following command defines a rule expression to match all RTSP request messages:

```
rtsp request packet = TRUE
```
rtsp rtp-seq

This command allows you to define rule expressions to match the “seq” field in the RTP-Info header of RTSP responses.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

cisco-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-ac cs-ruledef)#

Syntax

[ no ] rtsp rtp-seq operator sequence_number

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.

operator must be one of the following:

• !=: Does not equal
• <=: Lesser than or equals
• ==: Equals
• >=: Greater than or equals

sequence_number

Specifies the sequence number in the RTSP RTP-Info field to match.

sequence_number must be an alphanumeric string of 0 through 65535 characters in Normal Play Time (NPT) time format.

Usage

Use this command to define rule expressions to match user traffic matching the “seq” field in the RTP-Info header of RTSP response for a PLAY request.

Example

The following command defines a rule expression to match user traffic based on RTP-seq number npt-12:34:59:

rtsp rtp-seq = npt-12:34:59
**rtsp rtp-time**

This command allows you to define rule expressions to match the “time” field in RTP-Info header of RTSP responses.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] rtsp rtp-time operator time
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `<=`: Lesser than or equals
  - `=`: Equals
  - `>=`: Greater than or equals

- **time**
  Specifies the time to match.
  `time` must be an alphanumeric string of 1 through 2147483647 characters in Normal Play Time (NPT) time format.

**Usage**

Use this command to define rule expressions to match the “time” field in the RTP-Info header of RTSP response for a PLAY request.

**Example**

The following command defines a rule expression to match RTP timestamp of `20120123T153600Z`:

```
rtsp rtp-time = 20120123T153600Z
```
rtsp rtp-uri

This command allows you to define rule expressions to match the URI field in the RTP-Info header of RTSP responses.

Product

ACS

Privilege

Security Administrator, Administrator

Mode

Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] rtsp rtp-uri [ case-sensitive ] operator uri

no

If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator

Specifies how to match.

operator must be one of the following:

• !=: Does not equal
• !contains: Does not contain
• !ends-with: Does not end with
• !starts-with: Does not start with
• ==: Equals
• contains: Contains
• ends-with: Ends with
• starts-with: Starts with

uri

Specifies the value to match with the URI in RTP-Info header of the RTSP message.

uri must be an alphanumeric string of 1 through 127 characters. uri allows punctuation characters and excludes the “host” portion.
Usage

Use this command to define rule expressions to match the URI field in the RTP-Info header of the RTSP response for a PLAY request.

Example

The following command defines a rule expression to match user traffic based on RTP-URI string rtsp://www.foo.com in the RTP-info header of RTSP packet:

```plaintext
rtsp rtp-uri = rtsp://www.foo.com
```
rtsp session-id

This command allows you to define rule expressions to match the session ID in RTSP messages.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

`active-charging service service_name > ruledef ruledef_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

Syntax

```
[ no ] rtsp session-id [ case-sensitive ] operator session_id
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **case-sensitive**
  Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

- **operator**
  Specifies how to match.
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `!contains`: Does not contain
  - `!ends-with`: Does not end with
  - `!starts-with`: Does not start with
  - `=`: Equals
  - `contains`: Contains
  - `ends-with`: Ends with
  - `starts-with`: Starts with

- **session_id**
  Specifies the session ID to match.
  `session_id` must be an alphanumeric string of 1 through 127 characters.

Usage
Use this command to define rule expressions to match the session ID in RTSP messages.
Example

The following command defines a rule expression to match the RTSP session ID 0123abc100:

```
rtsp session-id = 0123abc100
```
rtsp session-length

This command allows you to define rule expressions to match the total length of RTSP sessions.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

active-charging service  service_name > ruledef  ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

**Syntax**

```
[ no ] rtsp session-length  operator  session_length
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  The **operator** must be one of the following:
  - !=: Does not equal
  - <=: Lesser than or equals
  - =: Equals
  - >=: Greater than or equals

- **session_length**
  Specifies the RTSP session length (in bytes) to match.
  The **session_length** must be an integer from 1 through 4000000.

**Usage**

Use this command to define rule expressions to match the total length of RTSP sessions. That is, the sum of the “rtsp pdu-length” values of all relevant packets.

**Example**

The following command defines a rule expression to match RTSP session length of 3000000 bytes:

```
rtsp session-length = 3000000
```
rtsp state

This command allows you to define rule expressions to match the current state of RTSP sessions.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active>charging service service_name>ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] rtsp state operator current_state

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be one of the following:
• !=: Does not equal
• ==: Equals

current_state
Specifies the current state to match.
current_state must be one of the following:
• end
• init
• open
• play
• ready
• record

Usage
Use this command to define rule expressions to match the current state of RTSP sessions.

Example
The following command defines a rule expression to match RTSP current state init:

rtsp state = init
**rtsp uri**

This command allows you to define rule expressions to match URI in RTSP request message.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

**Syntax**

```
[ no ] rtsp uri [ case-sensitive ] operator uri
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **case-sensitive**
  Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

- **operator**
  Specifies how to match.
  `operator` must be one of the following:
  - !=: Does not equal
  - !contains: Does not contain
  - !ends-with: Does not end with
  - !starts-with: Does not start with
  - =: Equals
  - contains: Contains
  - ends-with: Ends with
  - regex: Regular expression
  - starts-with: Starts with

- **uri**
  Specifies the URI to match.
  `uri` must be an alphanumeric string of 1 through 127 characters. `uri` allows punctuation characters and excludes the “host” portion.
Usage

Use this command to define rule expressions to match URI in RTSP request.
The following table lists the special characters that you can use in regex rule expressions. For more information on regex support, refer to the Enhanced Charging Service Administration Guide.

Table 10. Special Characters Supported in Regex Rule Expressions

<table>
<thead>
<tr>
<th>Regex Character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Zero or more characters</td>
</tr>
<tr>
<td>+</td>
<td>Zero or more repeated instances of the token preceding the +</td>
</tr>
<tr>
<td>?</td>
<td>Match zero or one character</td>
</tr>
</tbody>
</table>

Important: The CLI does not support configuring “?” directly, you must instead use “\077”.

For example, if you want to match the string “xyz<any one character>pqr”, you must configure it as:
```
http host regex “xyz\077pqr”
```
In another example, if you want to exactly match the string “url?resource=abc”, you must configure it as:
```
http uri regex ”url\077resource=abc”
```
Where, the first “\” (backslash) is for the escaping of “?” and then “\077” for specifying “?” to the CLI.

<table>
<thead>
<tr>
<th>\character</th>
<th>Escaped character</th>
</tr>
</thead>
<tbody>
<tr>
<td>?</td>
<td>Match the question mark (&lt;ctrl-v&gt;?) character</td>
</tr>
<tr>
<td>+</td>
<td>Match the plus character</td>
</tr>
<tr>
<td>*</td>
<td>Match the asterisk character</td>
</tr>
<tr>
<td>\a</td>
<td>Match the Alert (ASCII 7) character</td>
</tr>
<tr>
<td>\b</td>
<td>Match the Backspace (ASCII 8) character</td>
</tr>
<tr>
<td>\f</td>
<td>Match the Form-feed (ASCII 12) character</td>
</tr>
<tr>
<td>\n</td>
<td>Match the New line (ASCII 10) character</td>
</tr>
<tr>
<td>\r</td>
<td>Match the Carriage return (ASCII 13) character</td>
</tr>
<tr>
<td>\t</td>
<td>Match the Tab (ASCII 9) character</td>
</tr>
<tr>
<td>\v</td>
<td>Match the Vertical tab (ASCII 11) character</td>
</tr>
<tr>
<td>\0</td>
<td>Match the Null (ASCII 0) character</td>
</tr>
<tr>
<td>\</td>
<td>Match the backslash character</td>
</tr>
<tr>
<td>Bracketed range [0-9]</td>
<td>Match any single character from the range</td>
</tr>
<tr>
<td>A leading ^ in a range</td>
<td>Do not match any in the range. All other characters represent themselves.</td>
</tr>
<tr>
<td>\x##</td>
<td>Any ASCII character as specified in two-digit hex notation. For example, \x5A yields a “Z”.</td>
</tr>
</tbody>
</table>
Important: When using the regex operator “|” in regex expressions, always wrap the string in double quotes.

For example, if you want to match the string "pqr" OR "xyz", you must configure it as:

```
http host regex "pqr|xyz".
```

### Example

The following command defines a rule expression to match user traffic based on RTSP URI:

```
rtsp://www.example.com:554/twister/audiotrack:
```

```
rtsp uri = rtsp://www.example.com:554/twister/audiotrack
```

The following command defines a regex rule expression to match either of the following or similar values in the RTSP URI string: rtsp://pvs29p.cvf.fr:554/t1/live/Oui17, rtsp://pvs00p.cvf.fr:554/t1/live/Nrj12, rtsp://pvs90p.cvf.fr:554/t1/live/France24_fr.

```
rtsp.uri regex "rtsp://pvs([0-9][0-9])p.cvf.fr:554/t1/live/(Gulli|Tf1|Tmc|Nrj12|Star|France24_fr|Oui17)"
```
rtsp uri sub-part

This command allows you to define rule expressions to match user traffic by parsing sub-parts of the URI in an RTSP request message.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] rtsp uri sub-part { { absolute-path | host | query } [ case-sensitive ] operator string | port { port_operator port_value | { range | !range } range_from to range_to } }

no
If previously configured, deletes the specified rule expression from the current ruledef.

absolute-path
Specifies the absolute path matching criteria to RTSP URI in an RTSP request message.

host
Specifies the host name matching criteria to RTSP URI in an RTSP request message.

query
Specifies the query string matching criteria to RTSP URI in an RTSP request message.

case-sensitive
Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator
Specifies how to match.
operator must be one of the following:

- !=: Does not equal
- !contains: Does not contain
- !ends-with: Does not end with
- !starts-with: Does not start with
- =: Equals
rtsp uri sub-part

- **contains**: Contains
- **ends-with**: Ends with
- **starts-with**: Starts with

### string

Specifies the absolute path/host name or query string to match with the URI in RTSP header. 
*string* must be an alphanumerical string of 1 through 127 characters. *string* allows punctuation characters and excludes the “host” portion.

### port

Specifies the port related matching for RTSP URI in an RTSP request message.

#### port_operator

Specifies how to match. *operator* must be one of the following:
- **!=**: Does not equal
- **==**: Less than or equals
- **=**: Equal
- **>=**: Greater than or equals

#### port_value

Specifies the RTSP port number to match with port rule in the RTSP flow as an integer from 0 through 65535.

```
{ range | !range } range_from to range_to
```

Enables or disables the range criteria for RTSP flow ports.
- **range**: Enables the range criteria for RTSP flow ports.
- **!range**: Disables the range criteria for RTSP flow ports.
- **range_from**: Specifies the start of range of RTSP flow ports as an integer from 0 through 65535, but less than or equal to *range_to*.
- **range_to**: Specifies the end of range of RTSP flow ports as an integer from 0 through 65535, but more than or equal to *range_from*.

### Usage

Use this command to define rule expressions to match URI sub parts like host, absolute path, port, and query in RTSP request messages.

### Example

The following command defines a URI sub part rule expression to analyze user traffic based on an RTSP URI port number between 1023 and 1068:

```
rtsp uri sub-part port range 1023 to 1068
```
rtsp user-agent

This command allows you to define rule expressions to match the user-agent field in RTSP headers.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] rtsp user-agent [ case-sensitive ] operator user_agent

no
If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive
Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator
Specifies how to match.
operator must be one of the following:

• !=: Does not equal
• !contains: Does not contain
• !ends-with: Does not end with
• !starts-with: Does not start with
• ==: Equals
• contains: Contains
• ends-with: Ends with
• starts-with: Starts with

user_agent
Specifies the user agent to match.
user_agent must be an alphanumeric string of 1 through 127 characters.

Usage

Use this command to define rule expressions to match the “user-agent” field in RTSP header.
Example

The following command defines a rule expression to match `test` in “user-agent” field of RTSP header:

```
rtsp user-agent = test
```

rtsp-stream any-match

This command allows you to define rule expressions to match all user traffic of type RTSP, RTCP, and RTP to achieve an unified charging for RTSP correlated flows.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] rtsp-stream any-match operator condition

---

no
If previously configured, deletes the rtsp-stream any match rule definition.

---

operator
Specifies how to logically match the information in the analyzed field.
operator must be one of the following:

- !=: Does not equal
- =: Equals

---

condition
Specifies the condition to match.
condition must be one of the following:

- FALSE
- TRUE

Usage
Use this command to specify a rule definition to analyze all RTSP, RTCP, and RTP traffic.

Example
The following command defines a rule expression to match all RTSP, RTCP, and RTP user traffic:

rtsp-stream any-match = TRUE
rtsp-stream first-setup-url

This command allows you to define rule expressions to match user traffic of type RTSP, RTCP, and RTP on the first setup URL of the parent RTSP flow to achieve an unified charging for RTSP correlated flows.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax


- **no**
  If previously configured, deletes the rtsp-stream any match rule definition.

- **case-sensitive**
  Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

- **operator**
  Specifies how to logically match the information in the analyzed field. **operator** must be one of the following:

  - `!=`: Does not equal
  - `!contains`: Does not contain
  - `!ends-with`: Does not end with
  - `!starts-with`: Does not start with
  - `=`: Equals
  - `contains`: contains
  - `ends-with`: Ends with
  - `regex`: Regular expression
  - `starts-with`: Starts with

- **url**
  Specifies the URL to match. **url** must be an alphanumeric string of 1 through 127 characters.
## Usage

Use this command to specify a rule definition to analyze RTSP, RTCP, and RTP traffic based on the first setup URL of the parent RTSP flow. The following table lists the special characters that you can use in regex rule expressions. For more information on regex support, refer to the *Enhanced Charging Service Administration Guide*.

**Table 11. Special Characters Supported in Regex Rule Expressions**

<table>
<thead>
<tr>
<th>Regex Character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Zero or more characters</td>
</tr>
<tr>
<td>+</td>
<td>Zero or more repeated instances of the token preceding the +</td>
</tr>
<tr>
<td>?</td>
<td>Match zero or one character</td>
</tr>
</tbody>
</table>

**Important:** The CLI does not support configuring “?” directly, you must instead use “\077”. For example, if you want to match the string “xyz<any one character>pqr”, you must configure it as: `http host regex "xyz\077pqr"`.

In another example, if you want to exactly match the string “url?resource=abc”, you must configure it as: `http uri regex "url\077resource=abc"` Where, the first “\" (backslash) is for the escaping of “?” , and then “\077” for specifying “?” to the CLI.

<table>
<thead>
<tr>
<th>\ character</th>
<th>Escaped character</th>
</tr>
</thead>
<tbody>
<tr>
<td>\</td>
<td>Match the question mark (&lt;ctrl-v&gt;? ) character</td>
</tr>
<tr>
<td>+</td>
<td>Match the plus character</td>
</tr>
<tr>
<td>*</td>
<td>Match the asterisk character</td>
</tr>
<tr>
<td>\a</td>
<td>Match the Alert (ASCII 7) character</td>
</tr>
<tr>
<td>\b</td>
<td>Match the Backspace (ASCII 8) character</td>
</tr>
<tr>
<td>\f</td>
<td>Match the Form-feed (ASCII 12) character</td>
</tr>
<tr>
<td>\n</td>
<td>Match the New line (ASCII 10) character</td>
</tr>
<tr>
<td>\r</td>
<td>Match the Carriage return (ASCII 13) character</td>
</tr>
<tr>
<td>\t</td>
<td>Match the Tab (ASCII 9) character</td>
</tr>
<tr>
<td>\v</td>
<td>Match the Vertical tab (ASCII 11) character</td>
</tr>
<tr>
<td>\0</td>
<td>Match the Null (ASCII 0) character</td>
</tr>
<tr>
<td>\</td>
<td>Match the backslash character</td>
</tr>
<tr>
<td>Bracketed range [0-9]</td>
<td>Match any single character from the range</td>
</tr>
<tr>
<td>A leading ^ in a range</td>
<td>Do not match any in the range. All other characters represent themselves.</td>
</tr>
<tr>
<td>\x##</td>
<td>Any ASCII character as specified in two-digit hex notation. For example, \x5A yields a “Z”.</td>
</tr>
</tbody>
</table>
### Regex Character

<table>
<thead>
<tr>
<th>Regex Character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Specify OR regular expression operator</td>
</tr>
</tbody>
</table>

**Important:** When using the regex operator “|” in regex expressions, always wrap the string in double quotes.

For example, if you want to match the string "pqr" OR “xyz”, you must configure it as:

```plaintext
http host regex "pqr|xyz".
```

### Example

The following command defines a rule expression to match all RTSP, RTCP, and RTP traffic when the parent RTSP’s first setup URL contains `cisco.com`:

```plaintext
rtsp-stream first-setup-url contains cisco.com
```

The following command defines a rule expression to match all RTSP, RTCP, and RTP traffic when the parent RTSP’s first setup URL matches the given regular expression: `rtsp://tvs100.google.fr/t1/M6`

```plaintext
rtsp-stream first-setup-url regex rtsp://tvs[a|l|b][0-9][0-9].google.(fr|:554)/t1/(M6|W9_)*
```
rule-application

This command allows you to specify the purpose of a ruledef, such as for charging, post-processing, routing, and so on.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

Syntax

```plaintext
rule-application { charging | post-processing | routing | tpo }

no rule-application
```

**no**
Disables the rule application configuration.

**charging**
Specifies that the current ruledef is for charging purposes.
Up to 2,048 rule definitions can be defined for the charging application in an Active Charging Service. Default: Enabled

**post-processing**

> **Important:** The `post-processing` keyword is available only in 8.3 and later releases.

Specifies that the current ruledef is for post-processing purposes. This enables processing of packets even if the rule matching for them has been disabled.

**routing**
Specifies that the current ruledef is for routing purposes. Up to 256 rule definitions can be defined for routing in an Active Charging Service. Default: Disabled

**tpo**

> **Important:** The Traffic Performance Optimization (TPO) in-line service is not supported in this release.
Usage

Use this command to specify the rule application for a rule definition. If, when configuring a ruledef, the rule-application is not specified, by default the system configures the ruledef as a charging ruledef.

Example

The following command configures the rule application “charging” to the current rule definition:

```
rule-application charging
```
**sdp any-match**

This command allows you to define rule expressions to match all packets that contain Session Description Protocol (SDP) descriptions.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] sdp any-match operator condition
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  
  - !=: Does not equal
  - =: Equals

- **condition**
  Specifies the condition to match.
  
  - FALSE
  - TRUE

**Usage**

Use this command to define rule expressions to match all packets containing SDP descriptions.

**Example**

The following command defines a rule expression to match all packets containing SDP descriptions:

```
sdp any-match = TRUE
```
sdp connection-ip-address

This command allows you to define rule expressions to match the IP address in the connection field of SDP descriptions.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

**Syntax**

```sh
[ no ] sdp connection-ip-address operator ipv4_address
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `==`: Equals

- **ipv4_address**
  Specifies the IP address to match.
  `ipv4_address` must be in IPv4 dotted-decimal notation.

**Usage**

Use this command to define rule expressions to match IP address in the connection field of SDP descriptions.

**Example**

The following command defines a rule expression to match the IP address *10.1.1.1* in the connection field of SDP descriptions:

```sh
sdp connection-ip-address = 10.1.1.1
```
**sdp media-audio-port**

This command allows you to define rule expressions to match media audio ports specified in the media sections of SDP descriptions.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] sdp media-audio-port operator port
```

- **no**
  
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  
  Specifies how to match.
  
  `operator` must be one of the following:
  
  - `!=`: Does not equal
  - `=`: Equals

- **port**
  
  Specifies the port number to match.
  
  `port` must be an integer from 0 through 65535.

**Usage**

Use this command to define rule expressions to match media audio ports specified in the media sections of SDP descriptions.

**Example**

The following command defines a rule expression to match media audio port 100 in the media sections of SDP descriptions:

```
sdp media-audio-port = 100
```
**sdp media-video-port**

This command allows you to define rule expressions to match media video ports specified in the media sections of SDP descriptions.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] sdp media-video-port operator port
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `==`: Equals

- **port**
  Specifies the port number to match.
  `port` must be an integer from 0 through 65535.

**Usage**

Use this command to define rule expressions to match media video ports specified in the media sections of SDP descriptions.

**Example**

The following command defines a rule expression to match media video port 100 in the media sections of SDP descriptions:

```
sdp media-video-port = 100
```
**sdp uplink**

This command allows you to define rule expressions to match SDP descriptions in the uplink (subscriber to network) direction.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```ssh
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```plaintext
[ no ] sdp uplink operator condition
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  - **!=**: Does not equal
  - **==**: Equals

- **condition**
  Specifies the condition to match.
  - **FALSE**: Is not uplink
  - **TRUE**: Is uplink

**Usage**

Use this command to define rule expressions to match SDP descriptions in uplink direction.

**Example**

The following command defines a rule expression to match all SDP descriptions in the uplink direction:

```
sdp uplink = TRUE
```
secure-http any-match

This command allows you to define rule expressions to match all Secure HTTP (HTTPS) packets.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] secure-http any-match operator condition

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be one of the following:
- !=: Does not equal
- ==: Equals

condition
Specifies the condition to match.
condition must be one of the following:
- FALSE
- TRUE

Usage
Use this command to define rule expressions to match all Secure HTTP packets.

Example
The following command defines a rule expression to match all HTTPS packets:

secure-http any-match = TRUE
secure-http uplink

This command allows you to define rule expressions to match uplink (subscriber to network) HTTPS packets.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration
active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] secure-http uplink operator condition

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match. operator must be one of the following:

• !=: Does not equal
• ==: Equals

condition
Specifies the condition to match. condition must be one of the following:

• FALSE: Is not uplink
• TRUE: Is uplink

Usage
Use this command to define rule expressions to match uplink HTTPS packets.

Example
The following command defines a rule expression to match all uplink HTTPS packets:

    secure-http uplink = TRUE
sip any-match

This command allows you to define rule expressions to match all Session Initiation Protocol (SIP) packets.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] sip any-match operator condition

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be one of the following:
- !: Does not equal
- =: Equals

condition
Specifies the condition to match.
condition must be one of the following:
- FALSE
- TRUE

Usage
Use this command to define rule expressions to match all SIP packets.

Example
The following command defines a rule expression to match all SIP packets:

\[ \text{sip any-match} = \text{TRUE} \]
sip call-id

This command allows you to define rule expressions to match the Call ID in SIP messages.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

`active-charging service service_name > ruledef ruledef_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] sip call-id [ case-sensitive ] operator call_id
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **case-sensitive**
  Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

- **operator**
  Specifies how to match. `operator` must be one of the following:
  - `!=`: Does not equal
  - `!contains`: Does not contain
  - `!ends-with`: Does not end with
  - `!starts-with`: Does not start with
  - `=`: Equals
  - `contains`: Contains
  - `ends-with`: Ends with
  - `starts-with`: Starts with

- **call-id**
  Specifies the call ID to match. `call-id` must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters.
**Usage**

Use this command to define rule expressions to match the call ID in SIP messages.

**Example**

The following command defines a rule expression to match the call ID `test` in SIP messages:

```
sip call-id = test
```
**sip content length**

This command allows you to define rule expressions to match the content-length field in SIP headers.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

**Syntax**

```
[ no ] sip content length operator content_length
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `<=`: Lesser than or equals
  - `=`: Equals
  - `>=`: Greater than or equals

- **content_length**
  Specifies the SIP content length to match.
  `content_length` must be an integer from 0 through 65535.

**Usage**

Use this command to define rule expressions to match the content-length field in SIP headers.

**Example**

The following command defines a rule expression to match the content length 10000 in SIP headers:

```
sip content length = 10000
```
sip content type

This command allows you to define rule expressions to match the content type field in SIP headers.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] sip content type [ case-sensitive ] operator content_type

Syntax Description:

- **no**: If previously configured, deletes the specified rule expression from the current ruledef.
- **case-sensitive**: Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.
- **operator**: Specifies how to match. `operator` must be one of the following:
  - `!=`: Does not equal
  - `!contains`: Does not contain
  - `!ends-with`: Does not end with
  - `!starts-with`: Does not start with
  - `=`: Equals
  - `contains`: Contains
  - `ends-with`: Ends with
  - `starts-with`: Starts with
- **content_type**: Specifies the content type to match. `content_type` must be an alphanumeric string of 1 through 127 characters.

Usage

Use this command to define rule expressions to match the content type field in SIP headers.
Example

The following command defines a rule expression to match content type download_string in SIP headers:

```
sip content type = download_string
```
sip from

This command allows you to define rule expressions to match the from field in SIP messages.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

Syntax

```
[ no ] sip from [ case-sensitive ] operator string
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **case-sensitive**
  Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

- **operator**
  Specifies how to match.
  **operator** must be one of the following:
  - !=: Does not equal
  - !contains: Does not contain
  - !ends-with: Does not end with
  - !starts-with: Does not start with
  - =: Equals
  - contains: Contains
  - ends-with: Ends with
  - starts-with: Starts with

- **string**
  Specifies the value to match.
  **string** must be an alphanumeric string of 1 through 127 characters, and may contain punctuation characters.

Usage

Use this command to define rule expressions to match the “from” field in SIP messages.
Example

The following command defines a rule expression to match `test1` in the “from” field in SIP messages:

```
sip from contains test1
```
**sip previous-state**

This command allows you to define rule expressions to match previous state of SIP sessions.

**Product**  
ACS

**Privilege**  
Security Administrator, Administrator

**Mode**  
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

**Syntax**

```
[ no ] sip previous-state  operator sip_previous_state

```

- **no**  
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**  
  Specifies how to match. 
  operator must be one of the following:
  - !=: Does not equal
  - ==: Equals

- **sip_previous_state**  
  Specifies the previous state to match. 
  sip_previous_state must be one of the following:
  - init
  - provisional-response
  - request-sent
  - response-fail
  - response-ok

**Usage**

Use this command to define rule expressions to match a previous state of SIP sessions.

**Example**

The following command defines a rule expression to match user traffic based on the SIP previous state of request-sent:

```
sip previous-state = request-sent
```
sip reply code

This command allows you to define rule expressions to match the reply code in SIP responses.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] sip reply code operator reply_code

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be one of the following:
• !=: Does not equal
• <=: Lesser than or equals
• ==: Equals
• >=: Greater than or equals

reply_code
Specifies the SIP reply code to match.
reply_code must be an integer from 100 through 699.

Usage
Use this command to define rule expressions to match the reply code in SIP responses.

Example
The following command defines a rule expression to match 180 in the reply code in SIP responses:

    sip reply code = 180
sip request method

This command allows you to define rule expressions to match the method in SIP requests.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] sip request method operator method

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be one of the following:

• !=: Does not equal
• =: Equals

method
Specifies the SIP method to match.
method must be one of the following:

• ack
• bye
• cancel
• invite
• options
• register

Usage
Use this command to define rule expressions to match the method in SIP requests.

Example
The following command defines a rule expression to match the method bye in SIP request messages:

sip request method = bye
**sip request packet**

This command allows you to define rule expressions to match all SIP request packets.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] sip request packet operator condition
```

- **no**
  - If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  - Specifies how to match.
  - `operator` must be one of the following:
    - `=`: Equals
    - `!=`: Does not equal

- **condition**
  - Specifies the condition to match.
  - `condition` must be one of the following:
    - `FALSE`: Is a response
    - `TRUE`: Is a request

**Usage**

Use this command to define rule expressions to match all SIP request packets.

**Example**

The following command defines a rule expression to match all SIP request packets:

```
sip request packet = TRUE
```

### sip state

This command allows you to define rule expressions to match current state of the SIP session.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

`active-charging service service_name > ruledef ruledef_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] sip state operator current_state
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `==`: Equals

- **current_state**
  Specifies the current state to match.
  `current_state` must be one of the following:
  - `ack-received`
  - `provisional-response`
  - `request-sent`
  - `response-fail`
  - `response-ok`

**Usage**

Use this command to define rule expressions to match the current SIP session.

**Example**

The following command defines a rule expression to match user traffic based on SIP current state `request-sent`:

```
sip state = request-sent
```
sip to

This command allows you to define rule expressions to match the “to” field in SIP messages.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] sip to [ case-sensitive ] operator to_address

no
If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive
Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator
Specifies how to match.
operator must be one of the following:
  • !=: Does not equal
  • !contains: Does not contain
  • !ends-with: Does not end with
  • !starts-with: Does not start with
  • =: Equals
  • contains: Contains
  • ends-with: Ends with
  • starts-with: Starts with

to_address
Specifies the “to” address/name to match.
to_address must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters.
Usage
Use this command to define rule expressions to match the “to” field in SIP messages.

Example
The following command defines a rule expression to match `test1` in the “to” field of SIP messages:

```plaintext
dip to contains test1
```
sip uri

This command allows you to define rule expressions to match the URI in SIP messages.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

**active-charging service service_name > ruledef ruledef_name**

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

```plaintext
[ no ] sip uri [ sub-part { headers | host | parameters | port | userinfo } ] [ case-sensitive ] operator uri
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **sub-part { headers | host | parameters | port | userinfo }**
  This is an optional keyword that defines what sub-part of a SIP URI to check.
  - **headers**: Apply the rule to SIP URI header field.
  - **host**: Apply the rule the SIP URI host field.
  - **parameters**: Apply the rule to the SIP URI parameters field.
  - **port**: Apply the rule to the SIP URI port field.
  - **userinfo**: Apply the rule to the SIP URI userinfo field.

- **case-sensitive**
  Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

- **operator**
  Specifies how to match.
  **operator** must be one of the following:
  - **!=**: Does not equal
  - **!contains**: Does not contain
  - **!ends-with**: Does not end with
  - **!starts-with**: Does not start with
  - **==**: Equals
  - **contains**: Contains
• ends-with: Ends with
• starts-with: Starts with

The string for sub-part keyword port must be an integer and requires different operators. Use the following operators with the port keyword:

• !=: Does not equal
• <=: Is less than
• =: Equals
• =>: Is greater than

**uri**

Specifies the SIP URI to match.

uri must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters. The string for sub-part keyword port must be an integer from 0 through 65535.

---

**Usage**

Use this command to define rule expressions to match the URI in SIP messages.

**Example**

The following command defines a rule expression to match the URI string `sip:10.1.1.1:5060` in SIP messages:

```
sip uri = sip:10.1.1.1:5060
```

The following command defines a rule expression to match the URI string `sip:nnnn@host:5060;user=phone` in SIP messages:

```
sip uri = sip:nnnn@host:5060;user=phone
```
smtp any-match

This command allows you to define rule expressions to match all Simple Mail Transfer Protocol (SMTP) packets.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

Syntax
[ no ] smtp any-match operator condition

- no
  If previously configured, deletes the specified rule expression from the current ruledef.

- operator
  Specifies how to match.
  operator must be one of the following:
  - !=: Does not equal
  - ==: Equals

- condition
  Specifies the condition to match.
  condition must be one of the following:
  - FALSE
  - TRUE

Usage
Use this command to define rule expressions to match all SMTP packets.

Example
The following command defines a rule expression to match all SMTP packets:

```plaintext
smtp any-match = TRUE
```
smtp command arguments

This command allows you to define rule expressions to match SMTP command arguments.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] smtp command arguments [ case-sensitive ] operator argument

no
If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive
Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator
Specifies how to match.
operator must be one of the following:
• !=: Does not equal
• !contains: Does not contain
• !ends-with: Does not end with
• !starts-with: Does not start with
• ==: Equals
• contains: Contains
• ends-with: Ends with
• starts-with: Starts with

argument
Specifies the command argument to match.
argument must be an alphanumeric string of 1 through 63 characters and may contain punctuation characters.
Usage

Use this command to define rule expressions to match SMTP command arguments.

Example

The following command defines a rule expression to match SMTP command argument *test*:

```plaintext
smtp command arguments = test
```
smtp command id

This command allows you to define rule expressions to match SMTP command IDs.

Product

ACS

Privilege

Security Administrator, Administrator

Mode

Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] smtp command id operator command_id

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.

operator must be one of the following:

- !==: Does not equal
- <=: Lesser than or equals
- ==: Equals
- >=: Greater than or equals

command_id

Specifies the command argument to match.

command_id must be an integer from 0 through 10.

Usage

Use this command to define rule expressions to match SMTP command IDs.

Example

The following command defines a rule expression to match SMTP command ID 8:

```
smtp command id = 8
```
smtp command name

This command allows you to define rule expressions to match commands sent in SMTP packets.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]\host_name(config-acs-ruledef)#

Syntax

[ no ] smtp command_name operator command_name

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be one of the following:
• !=: Does not equal
• ==: Equals

command_name
Specifies the command name to match.
command_name must be one of the following:
• bdat
• data
• ehlo
• expn
• helo
• mail-from
• mail-from
• noop
• quit
• rcpt-to
• rset
• vrfy
Usage

Use this command to define rule expressions to match commands sent in SMTP packets.

Example

The following command defines a rule expression to match `data` command in SMTP packets:

```
smtp command name = data
```
smtp mail-size

This command allows you to define rule expressions to match the size of mail sent by a SMTP client.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] smtp mail-size { operator mail_size | { { range | !range } range_from to range_to } }

---

no
If previously configured, deletes the specified rule expression from the current ruledef.

---

operator

Specifies how to match.

operator must be one of the following:

- !=: Does not equal
- <=: Lesser than or equals
- ==: Equals
- >=: Greater than or equals

---

mail_size

Specifies the mail size (in bytes) to match.

mail_size must be an integer from 1 through 40000000.

---

{ range | !range } range_from to range_to

Enables or disables the range criteria.

- range: Enables the range criteria.
- !range: Disables the range criteria.

range_from: Specifies the start of range as an integer from 1 through 40000000.

range_to: Specifies the end range. range_to must be an integer from 1 through 40000000, and must be greater than range_from.
Usage

Use this command to define rule expressions to match the size of mail sent by an SMTP client.

Example

The following command defines a rule expression to match mail size of 40000 bytes:

```
smtp mail-size = 40000
```
smtp pdu-length

This command allows you to define rule expressions to match the Protocol Data Unit (PDU) length of SMTP packets.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] smtp pdu-length { operator pdu_length | { { range | !range } range_from to range_to } }
```

---

**no**
If previously configured, deletes the specified rule expression from the current ruledef.

**operator**
Specifies how to match.

- `!`: Does not equal
- `<=`: Lesser than or equals
- `=`: Equals
- `>=`: Greater than or equals

**pdu_length**
Specifies the SMTP PDU length (in bytes) to match.

- `pdu_length` must be an integer from 1 through 65535.

**{ range | !range } range_from to range_to**
Enables or disables the range criteria.

- `range`: Enables the range criteria.
- `!range`: Disables the range criteria.
- `range_from`: Specifies the start of range as an integer from 1 through 65535.
- `range_to`: Specifies the end range. `range_to` must be an integer from 1 through 65535, and must be greater than `range_from`. 
Usage
Use this command to define rule expressions to match PDU length of SMTP packets, that is headers + payload.

Example
The following command defines a rule expression to match a PDU length of 1600 bytes:

```
smtp pdu-length = 1600
```
smtp previous-state

This command allows you to define rule expressions to match previous state of SMTP command sessions.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] smtp previous-state operator smtp_previous_state

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be one of the following:
• !=: Does not equal
• ==: Equals

smtp_previous_state
Specifies the previous state to match.
smtp_previous_state must be one of the following:
• close: Closed state
• init: Initialized state
• response-error: Reply error state
• response-ok: Response ok state
• waiting-for-response: Waiting for response state

Usage
Use this command to define rule expressions to match a previous state of SMTP command sessions.

Example
The following command defines a rule expression to match user traffic based on SMTP previous state close:

smtp previous-state = close
smtp recipient

This command allows you to define rule expressions to match the recipient e-mail ID in the current SMTP transaction.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] smtp recipient [ case-sensitive ] operator argument

<table>
<thead>
<tr>
<th>no</th>
</tr>
</thead>
<tbody>
<tr>
<td>If previously configured, deletes the specified rule expression from the current ruledef.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>case-sensitive</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>operator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies how to match.</td>
</tr>
<tr>
<td>operator must be one of the following:</td>
</tr>
<tr>
<td>• !=: Does not equal</td>
</tr>
<tr>
<td>• !contains: Does not contain</td>
</tr>
<tr>
<td>• !ends-with: Does not end with</td>
</tr>
<tr>
<td>• !starts-with: Does not start with</td>
</tr>
<tr>
<td>• =: Equals</td>
</tr>
<tr>
<td>• contains: Contains</td>
</tr>
<tr>
<td>• ends-with: Ends with</td>
</tr>
<tr>
<td>• starts-with: Starts with</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>argument</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the response argument to match.</td>
</tr>
<tr>
<td>argument must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters.</td>
</tr>
</tbody>
</table>
Usage

Use this command to define rule expressions to match the recipient e-mail ID in the current SMTP transaction.

Example

The following command defines a rule expression to match recipient e-mail ID containing test in the current SMTP transaction:

```plaintext
smtp recipient contains test
```
smtp reply arguments

This command allows you to define rule expressions to match the arguments within SMTP responses.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```bash
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] smtp reply arguments [ case-sensitive ] operator argument
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **case-sensitive**
  Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

- **operator**
  Specifies how to match.
  ```
  operator must be one of the following:
  * !=: Does not equal
  * !contains: Does not contain
  * !ends-with: Does not end with
  * !starts-with: Does not start with
  *=: Equals
  * contains: Contains
  * ends-with: Ends with
  * starts-with: Starts with
  ```

- **argument**
  Specifies the reply argument to match.
  ```
  argument must be an alphanumeric string of 1 through 63 characters and may contain punctuation characters.
  ```
Usage

Use this command to define rule expressions to match the arguments with SMTP response.

Example

The following command defines a rule expression to match reply argument `forward-path` in SMTP response:

```
smtp reply arguments = forward-path
```
smtp reply id

This command allows you to define rule expressions to match reply ID assigned to SMTP responses.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

Syntax

[ no ] smtp reply id operator reply_id

- **no**
  
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  
  Specifies how to match.
  
  - !=: Does not equal
  - ==: Equals

- **reply_id**
  
  Specifies the reply ID to match.
  
  reply_id must be one of the following:
  
  - 0: +NO reply
  - 1: +OK reply
  - 2: -ERR reply

Usage

Use this command to define rule expressions to reply ID assigned to SMTP response.

Example

The following command defines a rule expression to match reply ID 2 assigned to SMTP response:

```
smtp reply id = 2
```
smtp reply status

This command allows you to define rule expressions to match the reply status in SMTP packets.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] smtp reply status operator reply_status

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be one of the following:
• !=: Does not equal
• ==: Equals

reply_status
Specifies the SMTP reply status to match.
reply_status must be one of the following:
• +OK: Response OK
• -ERR: Response error

Usage
Use this command to define rule expressions to match reply status in SMTP packets.

Example
The following command defines a rule expression to match reply status +OK in SMTP packets:

smtp reply status = +OK
smtp sender

This command allows you to define rule expressions to match sender e-mail ID in the current SMTP transaction.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:
[local]host_name(config-acs-ruledef)#

Syntax

[ no ] smtp sender [ case-sensitive ] operator sender

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **case-sensitive**
  Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

- **operator**
  Specifies how to match.
  **operator** must be one of the following:
  - !=: Does not equal
  - !contains: Does not contain
  - !ends-with: Does not end with
  - !starts-with: Does not start with
  - =: Equals
  - contains: Contains
  - ends-with: Ends with
  - starts-with: Starts with

- **sender**
  Specifies the sender value to match.
  **sender** must be an alphanumeric string of 1 through 127 characters.

Usage

Use this command to define rule expressions to match sender e-mail ID in the current SMTP transaction.
Example

The following command defines a rule expression to match sender e-mail ID containing \textit{test} in the current SMTP transaction:

\begin{verbatim}
  smtp sender contains test
\end{verbatim}
smtp session-length

This command allows you to define rule expressions to match total length of SMTP sessions.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef) #

Syntax

[ no ] smtp session-length { operator session_length | { range | !range } range_from to range_to }

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

- !=: Does not equal
- <=: Lesser than or equals
- =: Equals
- >=: Greater than or equals

session_length

Specifies the session length to match.
session_length must be an integer from 1 through 40000000.

{ range | !range } range_from to range_to

Enables or disables the range criteria.

- range: Enables the range criteria.
- !range: Disables the range criteria.

- range_from: Specifies the start of range as an integer from 1 through 40000000.
- range_to: Specifies the end range. range_to must be an integer from 1 through 40000000, and must be greater than range_from.
Usage

Use this command to define rule expressions to match total length of SMTP session.

Example

The following command defines a rule expression to match SMTP session length of 4000000:

```
smtp session-length = 4000000
```
**smtp state**

This command allows you to define rule expressions to match current state of a SMTP command session.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

\texttt{active-charging service service_name > ruledef ruledef_name}

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

**Syntax**

```
[ no ] smtp state operator current_state
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  \texttt{operator} must be one of the following:
  - !=: Does not equal
  - ==: Equals

- **current_state**
  Specifies the current state to match.
  \texttt{current_state} must be one of the following:
  - close: Closed state
  - init: Initialized state
  - response-error: Response of error state
  - response-ok: Response of ok state
  - waiting-for-response: Waiting for response state

**Usage**

Use this command to define rule expressions to match current state of SMTP command session.

**Example**

The following command defines a rule expression to match current state as close of SMTP command session:

```
smtp state = close
```
tcp analyzed out-of-order

This command allows you to define rule expressions to determine whether the received TCP packet was received before all of the earlier sequenced packets have been received. This functionality is for whether the packet was analyzed or discarded because the earlier sequenced packet(s) was (were) not received before a timeout expired.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] tcp analyzed out-of-order operator condition

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be one of the following:
• !=: Does not equal
• ==: Equals

condition
Specifies the condition to match.
condition must be one of the following:
• FALSE: Not analyzed
• TRUE: Analyzed

Usage
This command is used to set the status flag to ‘analyzed’ or ‘not analyzed’ for all TCP packets received at the ACSMgr/SessMgr prior to their earlier packets.
When a packet reaches ACSMgr/SessMgr prior to earlier packet(s), it and subsequent packets are buffered at ACSMgr/SessMgr as TCP out-of-order packets and ACSMgr/SessMgr waits for missing packet(s) until the time-out duration expires. If the packet(s) with the missing sequence number(s) arrives within the time-out duration, all buffered packets with the correct sequence will be presented to upper layers (HTTP etc.) for analysis; otherwise buffered TCP out-of-order packets will be sent to charging with analysis done flag at the TCP/IP layer only.
If this command is enabled the TCP out-of-order packets are marked and sent to TCP analyzer as analyzed for charging action, otherwise they are discarded.

**Example**

The following command sets to analyze TCP out-of-order packets:

```
tcp analyzed out-of-order = TRUE
```
tcp any-match

This command allows you to define rule expressions to match all TCP packets.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:
```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] tcp any-match operator condition
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  - !(!=): Does not equal
  - ==(=): Equals

- **condition**
  Specifies the condition to match.
  - FALSE: Not analyzed
  - TRUE: Analyzed

**Usage**

Use this command to define rule expressions to match all TCP packets.

**Example**

The following command defines a rule expression to match all TCP packets:

```
tcp any-match = TRUE
```
**tcp connection-initiator**

This command allows you to define rule expressions to match the TCP connection initiator.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```
activate-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-accs-ruledef)#
```

**Syntax**

```
[ no ] tcp connection-initiator operator subscriber
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  - **!=**: Does not equal
  - **==**: Equals

- **subscriber**
  Specifies that the connection is being initiated by the subscriber.

**Usage**

Use this command to define rule expressions to match the TCP connection initiator, and to allow the operator to differentiate when the connection initiated by subscriber or the subscriber is acting as a Transaction Control Server (TCS) server.

**Example**

The following command defines a rule expression to match user traffic based on TCP connection initiator subscriber:

```
tcp connection-initiator = subscriber
```
tcp downlink

This command allows you to define rule expressions to match downlink (network to subscriber) TCP packets.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] tcp downlink operator condition

- no
  If previously configured, deletes the specified rule expression from the current ruledef.

- operator
  Specifies how to match.
  operator must be one of the following:
  - !=: Does not equal
  - ==: Equals

- condition
  Specifies the condition to match.
  condition must be one of the following:
  - FALSE
  - TRUE

Usage
Use this command to define rule expressions to match downlink (to subscriber) TCP packets.

Example

The following command defines a rule expression to match downlink TCP packets:

    tcp downlink = TRUE
**tcp dst-port**

This command allows you to define rule expressions to match destination port number in TCP headers.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] tcp dst-port { operator port_number | { !range | range } { start_range to end_range | port-map port_map_name } }
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  - **operator** must be one of the following:
    - !=: Does not equal
    - <=: Lesser than or equals
    - =: Equals
    - >=: Greater than or equals

- **port_number**
  Specifies the port number to match.
  - **port_number** must be an integer from 1 through 65535.

- **range | !range**
  Specifies the range criteria:
  - **!range**: Not in the range
  - **range**: In the range

- **start_range to end_range**
  Specifies the starting and ending port numbers for the range of destination TCP ports.
  - **start_range** must be an integer from 1 through 65535.
  - **end_range** must be an integer from 1 through 65535, and must be greater than **start_range**.
**port-map port_map_name**

Specifies the port map for the port range. *port_map_name* must be an alphanumeric string of 1 through 63 characters.

**Usage**

Use this command to define rule expressions to match destination port number in TCP headers.

**Example**

The following command defines a rule expression to match destination port number 10 in TCP headers:

```
tcp dst-port = 10
```
tcp duplicate

This command allows you to define rule expressions to match TCP retransmissions.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration
active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] tcp duplicate operator condition

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be one of the following:
- !=: Does not equal
- ==: Equals

condition
Specifies the condition to match.
condition must be one of the following:
- FALSE: Not duplicated/retransmitted
- TRUE: Duplicated/retransmitted

Usage
Use this command to specify rule expressions to match TCP retransmission.

Example
The following command defines a rule expression to match TCP retransmissions:

tcp duplicate = TRUE
tcp either-port

This command allows you to define rule expressions to match either a destination or source port number in TCP headers.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] tcp either-port { operator port_number | { !range | range } { start_range to end_range | port-map port_map_name } }
```

---

**no**
If previously configured, deletes the specified rule expression from the current ruledef.

---

**operator**
Specifies how to match.

* operator must be one of the following:
  - !=: Does not equal
  - <=: Lesser than or equals
  - =: Equals
  - =>: Greater than or equals

---

**port_number**
Specifies the port number to match.

* port_number must be an integer from 1 through 65535.

---

**range | !range**
Specifies the range criteria:

* !range: Not in the range
* range: In the range

---

**start_range to end_range**
Specifies the starting and ending port numbers for the port range.

* start_range must be an integer from 1 through 65535.
* end_range must be an integer from 1 through 65535, and must be greater than start_range.
**port-map** **port_map_name**

Specifies the port map for the port range. **port_map_name** must be an alphanumeric string of 1 through 63 characters.

**Usage**

Use this command to define rule expressions to match either a destination or source port number in TCP headers. This command expression allows you to create a single ruledef using either-port, rather than needing two ruledefs (one with dst-port and one with src-port).

**Example**

The following command defines a rule expression to match destination/source port number 10 in TCP header:

```
tcp either-port = 10
```
**tcp error**

This command allows you to define rule expressions to identify errors, either in the packet (for example, TCP checksum error) or in the TCP analyzer's Finite State Machine (FSM).

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] tcp error operator condition
```

- **no**
  
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  
  Specifies how to match.

  - `!=`: Does not equal
  - `==`: Equals

- **condition**
  
  Specifies the condition to match.

  - `FALSE`
  - `TRUE`

**Usage**

Use this command to define a rule expression to identify errors, either in the packet (for example, TCP checksum error) or in the TCP analyzer's FSM.

**Example**

The following command defines a rule expression to match TCP errors:

```
tcp error = TRUE
```
tcp flag

This command allows you to define rule expressions to match bit within the flag field of TCP headers.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```plaintext
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] tcp flag operator flag
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.

  - `!contains`: Does not contain
  - `contains`: Contains
  - `!=`: Does not equal
  - `=`: Equals

- **flag**
  Specifies the flag value to match.

  - `ack`: TCP FLAG ACK
  - `fin`: TCP FLAG FIN
  - `push`: TCP FLAG PUSH
  - `reset`: TCP FLAG RESET
  - `syn`: TCP FLAG SYN

**Usage**

Use this command to define rule expressions to match a bit within the flag field of TCP headers.

**Example**

The following command defines a rule expression to match `reset` within flag field of TCP headers:
tcp flag = reset
tcp initial-handshake-lost

This command allows you to define rule expressions to match data packets when there has been no TCP handshaking to establish TCP connection.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

Syntax
[ no ] tcp initial-handshake-lost operator condition

- no
  If previously configured, deletes the specified rule expression from the current ruledef.

- operator
  Specifies how to match.
  operator must be one of the following:
  - !=: Does not equal
  - ==: Equals

- condition
  Specifies the condition to match.
  condition must be one of the following:
  - FALSE
  - TRUE

Usage
Use this command to define rule expressions to match data packets when there has been no TCP handshaking to establish TCP connection.

Example
The following command defines a rule expression to identify TCP flow where the initial handshake was not seen:

tcp initial-handshake-lost = TRUE
tcp payload

This command allows you to define rule expressions to match hexadecimal or ASCII string content in the payload protocol-signature field of the TCP payload.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] tcp payload starts-with { hex-signature hex_string | string-signature string }
```

- **no**
  - If previously configured, deletes the specified rule expression from the current ruledef.

- **hex-signature hex_string**
  - Specifies hexadecimal protocol signature in payload field.
  - `hex_string` must be a dash-delimited list of hex data of size smaller than 32.

- **string-signature string**
  - Specifies protocol signature in payload field.
  - `string` must be an alphanumeric string of 1 through 32 characters.

**Usage**
Use this command to define rule expressions to match for Hex/ASCII string content in payload protocol-signature field.
This rule expression is useful for detecting certain applications.

**Example**

The following command defines a rule expression to identify user traffic based on TCP protocol signature `tcp1`:

```
tcp payload starts-with string-signature tcp1
```
**tcp payload-length**

This command allows you to define rule expressions to match the length of a TCP payload.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] tcp payload-length operator payload_length
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `<=`: Lesser than or equals
  - `==`: Equals
  - `>=`: Greater than or equals

- **payload_length**
  Specifies the TCP payload length to match.
  `payload_length` must be an integer from 0 through 40000000.

**Usage**

Use this command to define rule expressions to match length of TCP payload, excluding the TCP or lower layer headers.
To match TCP control packets configure a payload-length of 0 (zero).

**Example**

The following command defines a rule expression to match TCP payload length of 10000:

```
tcp payload-length = 10000
```
tcp previous-state

This command allows you to define rule expressions to match previous state of TCP connections.

Product  
ACS

Privilege  
Security Administrator, Administrator

Mode  
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] tcp previous-state operator tcp_previous_state

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:
- !=: Does not equal
- ==: Equals

tcp_previous_state

Specifies the previous state to match.
tcp_previous_state must be one of the following:
- close
- close-wait
- closing
- established
- fin-wait1
- fin-wait2
- last-ack
- listen
- syn-received
- syn-sent
- time-wait
Usage

Use this command to define rule expressions to match a TCP previous state.

Example

The following command defines a rule expression to match user traffic based on previous state `time-wait`:

```
tcp previous-state = time-wait
```
**tcp proxy-prev-state**

This command allows you to define rule expressions to match TCP previous state on the ingress side of the TCP proxy.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] tcp proxy-prev-state operator previous_state
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `==`: Equals

- **previous_state**
  Specifies the previous state to match.
  `previous_state` must be one of the following:
  - `close`
  - `close-wait`
  - `closing`
  - `established`
  - `fin-wait1`
  - `fin-wait2`
  - `last-ack`
  - `listen`
  - `syn-received`
  - `syn-sent`
  - `time-wait`
**Usage**

If there is no TCP proxy configured, this configuration is not applicable.

For proxy-enabled flows, TCP state handling interprets the ingress side as the radio side and the egress side as the Internet side of the TCP connection.

- `tcp state` and `tcp prev-state` is the state of the client stack, which would be either the state of the subscriber's stack (if flow is not proxy enabled) or the MS state of proxy on the egress-side (if flow is proxy-enabled).

- `tcp proxy-state` and `tcp proxy-prev-state` is the state of the embedded TCP proxy server, that is the proxy ingress-side.

So, depending on the use case, if using `tcp state` and `tcp prev-state` an existing configuration may work fine regardless of whether proxy is enabled. For other use cases, other ruledefs may have to be created.

Both `tcp state` and `tcp proxy-state` can be used in the same ruledef. If proxy was being used, they would map to the egress-side and ingress-side, respectively. If proxy was not being used, then this would not match ruledef because proxy state would not be applicable.

**Example**

The following command defines a rule expression to match user traffic based on TCP proxy previous state of established:

```
tcp proxy-prev-state = established
```
tcp proxy-state

This command allows you to define rule expressions to match the TCP state on the ingress side of the TCP proxy.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] tcp proxy-state operator state

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be one of the following:

• !=: Does not equal
• ==: Equals

state
Specifies the state to match.
state must be one of the following:

• close
• close-wait
• closing
• established
• fin-wait1
• fin-wait2
• last-ack
• listen
• syn-received
• syn-sent
• time-wait
Usage

If there is no TCP proxy configured, this configuration is not applicable.
For proxy-enabled flows, TCP state handling interprets the ingress side as the radio side and the egress side as the Internet side of the TCP connection.

`tcp state` and `tcp prev-state` is the state of the client stack, which would be either the state of the subscriber's stack (if flow is not proxy enabled) or the MS state of proxy on egress-side (if flow is proxy-enabled).

`tcp proxy-state` and `tcp proxy-prev-state` is the state of the embedded TCP proxy server, that is the proxy ingress-side.
So, depending on the use case, if using `tcp state` and `tcp prev-state` an existing configuration may work fine regardless of whether proxy is enabled. For other use cases, other ruledefs may have to be created.
Both `tcp state` and `tcp proxy-state` can be used in the same ruledef. If proxy was being used, they would map to the egress-side and ingress-side, respectively. If proxy was not being used, then this would not match the ruledef because proxy state would not be applicable.

Example

The following command defines a rule expression to match user traffic based on TCP proxy previous state of established:

```
tcp proxy-state = established
```
tcp session-length

This command allows you to define rule expressions to match the total length of a TCP session.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] tcp session-length operator session_length

- no
  If previously configured, deletes the specified rule expression from the current ruledef.

- operator
  Specifies how to match.
  operator must be one of the following:
  - !=: Does not equal
  - <=: Lesser than or equals
  - ==: Equals
  - >=: Greater than or equals

- session_length
  Specifies the TCP session length (in bytes) to match as be an integer from 0 through 400000000.

Usage

Use this command to define rule expressions to match the total length of a TCP session.
The session-length is calculated by adding together the TCP payload-length values of all relevant packets.

Example

The following command defines a rule expression to match user traffic based on TCP session length of 2000 bytes:

tcp session-length = 2000
**tcp src-port**

This command allows you to define rule expressions to match source a port number in TCP headers.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acn-ruledef)#
```

**Syntax**

```
[ no ] tcp src-port { operator port_number | { !range | range } | port-map port_map_name } 
```

- **no**
  - If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  - Specifies how to match.
  - **operator** must be one of the following:
    - !=: Does not equal
    - <=: Lesser than or equals
    - ==: Equals
    - >=: Greater than or equals

- **port_number**
  - Specifies the port number to match.
  - **port_number** must be an integer from 1 through 65535.

- **range | !range**
  - Specifies the range criteria:
    - !range: Not in the range
    - range: In the range

- **start_range to end_range**
  - Specifies the starting and ending port numbers for the port range.
  - **start_range** must be an integer from 1 through 65535.
  - **end_range** must be an integer from 1 through 65535, and must be greater than **start_range**.
port-map  port_map_name

Specifies the port map for the port range.  port_map_name must be an alphanumeric string of 1 through 63 characters.

Usage

Use this command to define rule expressions to match source a port number in TCP headers.

Example

The following command defines a rule expression to analyze user traffic matching TCP source port 10:

```plaintext
tcp src-port = 10
```
**tcp state**

This command allows you to define rule expressions to match current state of TCP connections.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]<host_name>(config-accs-ruledef)#
```

**Syntax**

```
[ no ] tcp state operator current_state
```

- **no**
  - If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  - Specifies how to match.
  - `operator` must be one of the following:
    - `!=`: Does not equal
    - `=`: Equals

- **current_state**
  - Specifies the current state to match.
  - `current_state` must be one of the following:
    - `close`
    - `close-wait`
    - `closing`
    - `established`
    - `fin-wait1`
    - `fin-wait2`
    - `last-ack`
    - `listen`
    - `syn-received`
    - `syn-sent`
    - `time-wait`
Usage
Use this command to define rule expressions to match a current state of TCP connections.

Example
The following command defines a rule expression to match user traffic based on current state `close`:

```
tcp state = close
```
**tcp uplink**

This command allows you to define rule expressions to match uplink (subscriber to network) TCP packets.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] tcp uplink operator condition
```

- **no**
  
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  
  Specifies how to match.

  - !=: Does not equal
  - ==: Equals

- **condition**
  
  Specifies the condition.

  - FALSE
  - TRUE

**Usage**

Use this command to define rule expressions to uplink TCP packets.

**Example**

The following command defines a rule expression to uplink TCP packets:

```
tcp uplink = TRUE
```
tethering-detection

This command allows you to define rule expressions to match tethered or non-tethered flows.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

tethering-detection { flow-not-tethered | flow-tethered }  

no tethering-detection

no

 Deletes the tethering detection configuration from the ruledef.

flow-not-tethered

Specifies to match if tethering is not detected on flow.

flow-tethered

Specifies to match if tethering is detected on flow.

Usage

Use this command to define rule expressions to match tethered/non-tethered flows. Note that in order for the rule containing the tethering-detection configuration to get matched, at least one valid rule line has to be present in it. This configuration is treated in a special manner by the rule matching engine in that it is excluded from the condition multi-line-or all-lines. For example, if there are three rule-lines in a ruledef and multi-line-or is enabled as follows:

ruledef all-tethered-web-traffic

http any-match = TRUE
wsp any-match = TRUE
multi-line-or all-lines
tethering-detection flow-tethered
exit

In this case, if for a packet only the rule line `tethering-detection flow-tethered` matches, it is not sufficient to result in a rule match even though `multi-line-or all-lines` is enabled in the ruledef.

Example

The following command defines a rule expression to match tethered flows:

```
tethering-detection flow-tethered
```
tftp any-match

This command allows you to define rule expressions to match all Trivial File Transfer Protocol (TFTP) packets.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] tftp any-match operator condition
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `=`: Equals

- **condition**
  Specifies the condition to match.
  `condition` must be one of the following:
  - `FALSE`: Not analyzed
  - `TRUE`: Analyzed

**Usage**

Use this command to define rule expressions to match all TFTP packets.

**Example**

The following command defines a rule expression to match all TFTP packets:

```
tftp any-match = TRUE
```
tftp data-any-match

This command allows you to define rule expressions to match all TFTP data packets.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] tftp data-any-match operator condition
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  operator must be one of the following:
  - !=: Does not equal
  - ==: Equals

- **condition**
  Specifies the condition to match.
  condition must be one of the following:
  - FALSE: Not analyzed
  - TRUE: Analyzed

**Usage**

Use this command to define rule expressions to match all TFTP data packets.

**Example**

The following command defines a rule expression to match all TFTP data packets:

```
tftp data-any-match = TRUE
```
**udp any-match**

This command allows you to define rule expressions to match all UDP packets.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] udp any-match operator condition
```

- **operator**
  Specifies how to match.
  - !=: Does not equal
  - =: Equals

- **condition**
  Specifies the condition to match.
  - FALSE
  - TRUE

**Usage**

Use this command to define rule expressions to match all UDP packets.

**Example**

The following command defines a rule expression to match all UDP packets:

```
udp any-match = TRUE
```
udp downlink

This command allows you to define rule expressions to match downlink (network to subscriber) UDP packets.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

*active-charging service service_name > ruledef ruledef_name*

Entering the above command sequence results in the following prompt:

[local]host_name(config-acd-ruledef)#

**Syntax**

```
[ no ] udp downlink operator condition
```

- **no**
  
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  - `operator` must be one of the following:
    - `=`: Equals

- **condition**
  Specifies the condition to match.
  - `condition` must be one of the following:
    - `FALSE`
    - `TRUE`

**Usage**

Use this command to define rule expressions to match downlink UDP packets.

**Example**

The following command defines a rule expression to match downlink UDP packets:

```
udp downlink = TRUE
```
udp dst-port

This command allows you to define rule expressions to match destination port number in UDP headers.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] udp dst-port { operator port_number | { !range | range } { start_range to end_range | port-map port_map_name } }

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be one of the following:
- !=: Does not equal
- <=: Lesser than or equals
- ==: Equals
- >=: Greater than or equals

port_number
Specifies the port number to match.
port_number must be an integer from 1 through 65535.

!range | range
Specifies the range criteria.
- !range: Not in the range
- range: In the range

start_range to end_range
Specifies the starting and ending port numbers for the port range.
- start_range must be an integer from 1 through 65535.
- end_range must be an integer from 1 through 65535, and must be greater than start_range.
**port-map**  *port_map_name*

Specifies the port map for the port range. *port_map_name* must be an alphanumeric string of 1 through 63 characters.

**Usage**

Use this command to define rule expressions to match destination port number in UDP headers.

**Example**

The following command defines a rule expression to match user traffic based on destination port number 10:

```
udp dst-port = 10
```
**udp either-port**

This command allows you to define rule expressions to match either a destination or source port number in UDP headers.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] udp either-port { operator port_number | !range | range } { start_range to end_range | port-map port_map_name }
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  **operator** must be one of the following:
  - !=: Does not equal
  - <=: Lesser than or equals
  - =: Equals
  - >=: Greater than or equals

- **port_number**
  Specifies the port number to match.
  **port_number** must be an integer from 1 through 65535.

- **!range | range**
  Specifies the range criteria.
  - !range: Not in the range
  - range: In the range

- **start_range to end_range**
  Specifies the starting and ending port numbers for the port range.
  **start_range** must be an integer from 1 through 65535.
  **end_range** must be an integer from 1 through 65535, and must be greater than **start_range**.
**port-map** *port_map_name*

Specifies the port map for the port range. *port_map_name* must be an alphanumeric string of 1 through 63 characters.

**Usage**

Use this command to define rule expressions to match either destination or source port number in UDP headers.

**Example**

The following command defines a rule expression to match user traffic based on match either source/destination port number 10:

```
udp either-port = 10
```
**udp payload starts-with**

This command allows you to define rule expressions to match hex/ASCII string content in UDP payload protocol-signature field.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] udp payload starts-with { hex-signature hex_string | string-signature string }
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **hex-signature hex_string**
  Specifies hexadecimal protocol signature in payload field.
  *hex_string* must be a dash-delimited list of hex data of size smaller than 32.

- **string-signature string**
  Specifies protocol signature in payload field.
  *string* must be an alphanumeric string of 1 through 32 characters.

**Usage**

Use this command to define rule expressions to match for Hex/ASCII string content in UDP payload protocol-signature field.

This rule expression is useful for detecting certain applications.

**Example**

The following command defines a UDP rule expression to analyze user traffic based on UDP protocol signature *udp1*:

```
udp payload starts-with string-signature udp1
```
udp src-port

This command allows you to define rule expressions to match source port number in UDP headers.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

```plaintext
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

Syntax

```
[ no ] udp src-port { operator port_number | { !range | range } { start_range to end_range | port-map port_map_name } }
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `<=`: Lesser than or equals
  - `=`: Equals
  - `>=`: Greater than or equals

- **port_number**
  Specifies the port number to match.
  `port_number` must be an integer from 1 through 65535.

- **!range | range**
  Specifies the range criteria.
  - `!range`: Not in the range
  - `range`: In the range

- **start_range to end_range**
  Specifies the starting and ending port numbers for the port range.
  - `start_range` must be an integer from 1 through 65535.
  - `end_range` must be an integer from 1 through 65535, and must be greater than `start_range`. 
port-map  port_map_name

Specifies the port map for the port range. port_map_name must be an alphanumeric string of 1 through 63 characters.

Usage

Use this command to define rule expressions to match source port number in UDP headers.

Example

The following command defines a rule expression to match source port number 10 in UDP headers:

    udp src-port = 10
**udp uplink**

This command allows you to define rule expressions to match uplink (subscriber to network) UDP packets.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

`active-charging service service_name > ruledef ruledef_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] udp uplink operator condition
```

**no**

If previously configured, deletes the specified rule expression from the current ruledef.

**operator**

Specifies how to match.

- `=`: Equals

**condition**

Specifies the condition to match.

- `FALSE`
- `TRUE`

**Usage**

Use this command to define rule expressions to match uplink UDP packets.

**Example**

The following command defines a rule expression to match uplink (from subscriber) UDP packets:

```
udp uplink = TRUE
```
**wsp any-match**

This command allows you to define rule expressions to match all Wireless Session Protocol (WSP) packets.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] wsp any-match operator condition
```

- **no**
  
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**

  Specifies how to match.

  - !=: Does not equal
  - ==: Equals

- **condition**

  Specifies the condition to match.

  - FALSE
  - TRUE

**Usage**

Use this command to specify a rule expression to match all WSP packets.

**Example**

The following command defines a rule expression to match all WSP packets:

```
wsp any-match = TRUE
```
wsp content type

This command allows you to define rule expressions to match the content type field in WSP headers.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs-ruledef) #
```

**Syntax**

```
[ no ] wsp content type [ case-sensitive ] operator content_type
```

- **no**
  
  If previously configured, deletes the specified rule expression from the current ruledef.

- **case-sensitive**
  
  Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

- **operator**
  
  Specifies how to match.

  `operator` must be one of the following:

  - `!=`: Does not equal
  - `!contains`: Does not contain
  - `!ends-with`: Does not end with
  - `!starts-with`: Does not start with
  - `=`: Equals
  - `contains`: Contains
  - `ends-with`: Ends with
  - `starts-with`: Starts with

- **content_type**
  
  Specifies content type to match.

  `content_type` must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters.
Usage

Use this command to define rule expressions to match “content type” field in WSP headers.

Example

The following command defines a rule expression to WSP content type test:

```
wsp content type = test
```
**wsp domain**

This command allows you to define rule expressions to match domain portion of the URI for WSP packets.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

`active-charging service service_name > ruledef ruledef_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] wsp domain [ case-sensitive ] operator domain
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **case-sensitive**
  Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

- **operator**
  Specifies how to match.
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `!contains`: Does not contain
  - `!ends-with`: Does not end with
  - `!starts-with`: Does not start with
  - `=`: Equals
  - `contains`: Contains
  - `ends-with`: Ends with
  - `starts-with`: Starts with

- **domain**
  Specifies the domain to match.
  `domain` must be an alphanumeric string of 1 through 127 characters.

**Usage**

Use this command to define rule expressions to match the domain portion of URIs in WSP packets.
From the URL, after http:// (if present) is removed, everything until the first "/" is the domain.

Example

The following command defines a rule expression to match user traffic based on domain name testdomain:

```
wsp domain = testdomain
```
**wsp downlink**

This command allows you to define rule expressions to match downlink (network to subscriber) WSP packets.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] wsp downlink operator condition
```

- **no**
  If previously configured, deletes the specified rule expression from the current `ruledef`.

- **operator**
  Specifies how to match.
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `==`: Equals

- **condition**
  Specifies the downlink (from the Mobile Node direction) status to match.
  `condition` must be one of the following:
  - `FALSE`
  - `TRUE`

**Usage**

Use this command to define rule expressions to match downlink WSP packets.

**Example**

The following command defines a rule expression to match downlink WSP packets:

```
  wsp downlink = TRUE
```
**wsp first-request-packet**

This command allows you to define rule expressions to match WSP first-request-packet.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

`active-charging service service_name > ruledef ruledef_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] wsp first-request-packet operator condition
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `=`: Equals

- **condition**
  Specifies the condition to match.
  `condition` must be one of the following:
  - `FALSE`
  - `TRUE`

**Usage**

Use this command to define rule expressions to match the GET or POST request, if it is the first WSP request for the subscriber's session.

**Example**

The following command defines a rule expression to match WSP first-request-packet:

```
wsp first-request-packet = TRUE
```
wsp host

This command allows you to define rule expressions to match the host name header field in WSP headers.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] wsp host [ case-sensitive ] operator host_name

no
If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive
Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator
Specifies how to match.
operator must be one of the following:
● !=: Does not equal
● !contains: Does not contain
● !ends-with: Does not end with
● !starts-with: Does not start with
● =: Equals
● contains: Contains
● ends-with: Ends with
● starts-with: Starts with

host_name
Specifies the WSP host name to match.
host_name must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters.
Usage

Use this command to define rule expressions to match host name header field in WSP headers.

Example

The following command defines a rule expression to match host name **host1** in WSP headers:

```plaintext
wsp host contains host1
```
wsp pdu-length

This command allows you to define rule expressions to match WSP PDU length.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

`active-charging service service_name > ruledef ruledef_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] wsp pdu-length operator pdu_length
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `<=`: Lesser than or equals
  - `==`: Equals
  - `>=`: Greater than or equals

- **pdu_length**
  Specifies the WSP PDU length (in bytes) to match.
  `pdu_length` must be an integer from 1 through 65535.

**Usage**

Use this command to define rule expressions to match WSP PDU length (header + payload) in bytes.

**Example**

The following command defines a rule expression to match user traffic based on WSP PDU length of 10000 bytes:

```
wsp pdu-length = 10000
```
wsp pdu-type

This command allows you to define rule expressions to match WSP PDU type in the current packet.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] wsp pdu-type operator pdu_type

no

If previously configured, deletes the specified rule expression from the current ruledef.

operator

Specifies how to match.
operator must be one of the following:

• !=: Does not equal
• ==: Equals

pdu_type

Specifies the WSP PDU type to match.
pdu_type must be one of the following:

• confirmed push
• connect-reply
• connect-request
• data-fragment
• delete
• disconnect
• get
• head
• options
• post
• push
• put
**wsp pdu-type**

- redirect
- reply
- resume
- suspend
- trace

**Usage**

Use this command to define rule expressions to match WSP PDU type value in current packet.

**Example**

The following command defines a rule expression to match WSP PDU type `resume`:

```
wsp pdu-type resume
```
wsp previous-state

This command allows you to define rule expressions to match previous WSP method invocation state.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] wsp previous-state operator wsp_previous_state

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be one of the following:
  • !=: Does not equal
  • =: Equals

wsp_previous_state
Specifies the previous state to match.
wsp_previous_state must be one of the following:
  • init
  • response-error
  • response-ok
  • waiting-for-response

Usage
Use this command to define rule expressions to match WSP previous state.

Example
The following command defines a rule expression to match WSP previous state of response-ok:

wsp previous-state = response-ok
**wsp reply code**

This command allows you to define rule expressions to match WSP reply code.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] wsp reply code operator reply_code
```

- **no**
  
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  
  Specifies how to match.

  **operator** must be one of the following:

  - !=: Does not equal
  - <=: Lesser than or equals
  - =: Equals
  - >=: Greater than or equals

- **reply_code**
  
  Specifies the WSP reply code to match.

  **reply_code** must be an integer from 0 through 101.

**Usage**

Use this command to define rule expressions to match WSP reply code.

**Example**

The following command defines a rule expression to match WSP reply code of 50:

```
wsp reply code = 50
```
wsp session-length

This command allows you to define rule expressions to match total length of a WSP session.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

Syntax

[ no ] wsp session-length operator session_length

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be one of the following:

• !=: Does not equal
• <=: less than equals
• =: Equals
• >=: greater than equals

session_length
Specifies the WSP session length (in bytes) to match.

Usage
Use this command to define rule expressions to match total length of WSP session.

Example
The following command defines a rule expression to match WSP session length of 2000 bytes:

    wsp session-length = 2000
wsp session-management

This command allows you to define rule expressions to match WSP Session Management state.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration
active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] wsp session-management { previous-state | state } operator state

- no
  If previously configured, deletes the specified rule expression from the current ruledef.

- previous-state
  Specifies the previous WSP Session Management state.

- state
  Specifies current WSP Session Management Finite State Machine (FSM) state.

- operator
  Specifies how to match.
  operator must be one of the following:
  - !=: Does not equal
  - ==: Equals

- state
  Specifies the state to match.
  For previous-state, state must be one of the following:
  - connected
  - connecting
  - init
  - resuming
  - suspended
  For state, state must be one of the following:
  - close
• connected
• connecting
• init
• resuming
• suspended

Usage
Use this command to define rule expressions to match a WSP Session Management state.

Example
The following command defines a rule expression to match previous WSP Session Management state of connecting:

wsp session-management previous-state = connecting
**wsp state**

This command allows you to define rule expressions to match WSP Method Invocation state.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] wsp state operator current_state
```

- **no**
  
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**

  Specifies how to match.
  
  `operator` must be one of the following:
  
  - `!=`: Does not equal
  - `==`: Equals

- **current_state**

  Specifies the current state to match.
  
  `current_state` must be one of the following:
  
  - `close`
  - `response-error`
  - `response-ok`
  - `waiting-for-response`

**Usage**

Use this command to define rule expressions to match WSP Method Invocation state.

**Example**

The following command defines a rule expression to match a WSP Method Invocation state `close`:

```
wsp state = close
```
wsp status

This command has been deprecated. See the wsp reply-code command.
**wsp tid**

This command allows you to define rule expressions to match Transaction Identifier (TID) field for connection-less WSP.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] wsp tid operator transaction_id
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `==`: Equals

- **transaction_id**
  Specifies the transaction identifier to match.
  `transaction_id` must be an integer from 0 through 255.

**Usage**

Use this command to define rule expressions to match TID field for connection-less WSP.

**Example**

The following command defines a rule expression to match a TID value of 22 for connection-less WSP:

```
  wsp tid = 22
```
wsp total-length

This command has been deprecated. See the wsp session-length command.
wsp transfer-encoding

This command allows you to define rule expressions to match transfer encoding present in WSP headers.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > ACS Configuration > Ruledef Configuration

`active-charging service service_name > ruledef ruledef_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] wsp transfer-encoding [ case-sensitive ] operator transfer_encoding
```

<table>
<thead>
<tr>
<th>no</th>
</tr>
</thead>
<tbody>
<tr>
<td>If previously configured, deletes the specified rule expression from the current ruledef.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>case-sensitive</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>operator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies how to match.</td>
</tr>
</tbody>
</table>

`operator` must be one of the following:

- `!=`: Does not equal
- `!contains`: Does not contain
- `!ends-with`: Does not end with
- `!starts-with`: Does not start with
- `=`: Equals
- `contains`: Contains
- `ends-with`: Ends with
- `starts-with`: Starts with

<table>
<thead>
<tr>
<th>transfer_encoding</th>
</tr>
</thead>
<tbody>
<tr>
<td>This must be an alphanumeric string of 1 through 127 characters.</td>
</tr>
</tbody>
</table>

**Usage**

Use this command to define rule expressions to match transfer encoding present in WSP header.

**Example**

Use this command to define rule expressions to match transfer encoding present in WSP header.
The following command defines a rule expression to match user traffic based on WSP transfer encoding 7:

```
wsp transfer-encoding contains 7
```
**wsp uplink**

This command allows you to define rule expressions to match uplink (subscriber to network) WSP packets.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] wsp uplink operator condition
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `==`: Equals

- **condition**
  Specifies the uplink (to the Mobile Node direction) status to match.
  `condition` must be one of the following:
  - `FALSE`
  - `TRUE`

**Usage**
Use this command to define rule expressions to match uplink WSP packets.

**Example**
The following command defines a rule expression to match uplink WSP packets:

```
wsp uplink = TRUE
```
wsp url

This command allows you to define rule expressions to match WSP URL.

<table>
<thead>
<tr>
<th>Product</th>
<th>ACS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privilege</td>
<td>Security Administrator, Administrator</td>
</tr>
<tr>
<td>Mode</td>
<td>Exec &gt; ACS Configuration &gt; Ruledef Configuration</td>
</tr>
</tbody>
</table>

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] wsp url [ case-sensitive ] operator url

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **case-sensitive**
  Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

- **operator**
  Specifies how to match.
  operator must be one of the following:
  - !=: Does not equal
  - !contains: Does not contain
  - !ends-with: Does not end with
  - !starts-with: Does not start with
  - =: Equals
  - contains: Contains
  - ends-with: Ends with
  - regex: Regular expression
  - starts-with: Starts with

- **url**
  Specifies the URL to match.
  url must be an alphanumeric string of 1 through 127 characters.
Usage

Use this command to define rule expressions to match the complete URL, including the host portion. The following table lists the special characters that you can use in regex rule expressions. For more information on regex support, refer to the Enhanced Charging Service Administration Guide.

Table 12. Special Characters Supported in Regex Rule Expressions

<table>
<thead>
<tr>
<th>Regex Character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Zero or more characters</td>
</tr>
<tr>
<td>+</td>
<td>Zero or more repeated instances of the token preceding the +</td>
</tr>
<tr>
<td>?</td>
<td>Match zero or one character</td>
</tr>
</tbody>
</table>

**Important:** The CLI does not support configuring “?” directly, you must instead use “\077”.

For example, if you want to match the string “xyz<any one character>pqr”, you must configure it as:

```
http host regex "xyz\077pqr"
```

In another example, if you want to exactly match the string “url?resource=abc”, you must configure it as:

```
http uri regex "url\077resource=abc"
```

Where, the first “\” (backslash) is for the escaping of “?”, and then “\077” for specifying “?” to the CLI.

<table>
<thead>
<tr>
<th>\ character</th>
<th>Escaped character</th>
</tr>
</thead>
<tbody>
<tr>
<td>?</td>
<td>Match the question mark (&lt;ctrl-v&gt;) character</td>
</tr>
<tr>
<td>+</td>
<td>Match the plus character</td>
</tr>
<tr>
<td>\*</td>
<td>Match the asterisk character</td>
</tr>
<tr>
<td>\a</td>
<td>Match the Alert (ASCII 7) character</td>
</tr>
<tr>
<td>\b</td>
<td>Match the Backspace (ASCII 8) character</td>
</tr>
<tr>
<td>\f</td>
<td>Match the Form-feed (ASCII 12) character</td>
</tr>
<tr>
<td>\n</td>
<td>Match the New line (ASCII 10) character</td>
</tr>
<tr>
<td>\r</td>
<td>Match the Carriage return (ASCII 13) character</td>
</tr>
<tr>
<td>\t</td>
<td>Match the Tab (ASCII 9) character</td>
</tr>
<tr>
<td>\v</td>
<td>Match the Vertical tab (ASCII 11) character</td>
</tr>
<tr>
<td>\0</td>
<td>Match the Null (ASCII 0) character</td>
</tr>
<tr>
<td>\</td>
<td>Match the backslash character</td>
</tr>
<tr>
<td>[0-9]</td>
<td>Match any single character from the range</td>
</tr>
<tr>
<td>^</td>
<td>Do not match any in the range. All other characters represent themselves.</td>
</tr>
<tr>
<td>\x##</td>
<td>Any ASCII character as specified in two-digit hex notation. For example, \x5A yields a “Z”.</td>
</tr>
</tbody>
</table>
Important: When using the regex operator “|” in regex expressions, always wrap the string in double quotes.

For example, if you want to match the string "pqr" OR "xyz", you must configure it as:
```
http host regex "pqr|xyz".
```

### Example

The following command defines a rule expression to match user traffic based on WSP URL `wsp://wiki.tcl.tk`:
```
wsp url = wsp://wiki.tcl.tk
```

The following command defines a regex rule expression to match any of the following or similar values in the WSP URL string: `wsp://home.opera.yahoo.com`, `wsp://dwld.yahoo.com`, `wsp://dwld2.yahoo.com`.
```
wsp url regex "wsp://(dwld|opera|home.opera|dwld[1-3]).yahoo.com"
```
wsp user-agent

This command allows you to define rule expressions to match user agent field in WSP headers.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] wsp user-agent [ case-sensitive ] operator user_agent

---

**no**

If previously configured, deletes the specified rule expression from the current ruledef.

---

**case-sensitive**

Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

---

**operator**

Specifies how to match.

**operator** must be one of the following:

- !=: Does not equal
- !contains: Does not contain
- !ends-with: Does not end with
- !starts-with: Does not start with
- =: Equals
- contains: Contains
- ends-with: Ends with
- starts-with: Starts with

---

**user_agent**

Specifies the WSP user agent to match.

**user_agent** must be an alphanumeric string of 1 through 127 characters.

---

Usage

Use this command to define rule expressions to match a user agent field in WSP headers.
Example

The following command defines a rule expression to match value *test* in user agent field in WSP headers:

```
wsp user-agent contains test
```
wsp x-header

This command allows you to define rule expressions to match WSP extension-headers (x-headers).

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

activate-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acis-ruledef)#

Syntax

[ no ] wsp x-header name [ case-sensitive ] operator string

no
If previously configured, deletes the specified rule expression from the current ruledef.

name
Specifies the x-header value as an alphanumeric string of 1 through 31 characters.

case-sensitive
Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator
Specifies how to match.

operator must be one of the following:

- !=: Does not equal
- !contains: Does not contain
- !ends-with: Does not end with
- !starts-with: Does not start with
- =: Equals
- contains: Contains
- ends-with: Ends with
- starts-with: Starts with

string
Specifies the value of the extension header as an alphanumeric string of 1 through 127 characters.
Usage

Use this command to configure any x-header field in WSP and parse it. The extension-header mechanism allows additional header fields to be defined without changing the protocol. The extension-header can be any header fields that are not specified in the RFC standard.

Example

The following command defines a rule expression to analyze user traffic containing WSP extension-header of *test_field* and value of *test_string*:

```
  wsp x-header test_field = test_string
```
wtp any-match

This command allows you to define rule expressions to match all Wireless Transaction Protocol (WTP) packets.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] wtp any-match operator condition

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be one of the following:
• !=: Does not equal
• ==: Equals

condition
Specifies the condition to match.
condition must be one of the following:
• FALSE
• TRUE

Usage
Use this command to define rule expressions to match all WTP packets.

Example
The following command defines a rule expression to match all WTP packets:

wtp any-match = TRUE
wtp downlink

This command allows you to define rule expressions to match downlink (network to subscriber) WTP packets.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

Syntax
[ no ] wtp downlink operator condition

- no
  If previously configured, deletes the specified rule expression from the current ruledef.

- operator
  Specifies how to match.
  operator must be one of the following:
  - !=: Does not equal
  - ==: Equals

- condition
  Specifies the downlink (from the Mobile Node direction) status to match.
  condition must be one of the following:
  - FALSE
  - TRUE

Usage
Use this command to define rule expressions to match downlink WTP packets.

Example
The following command defines a rule expression to match all downlink WTP packets:

  wtp downlink = TRUE
**wtp gtr**

This command allows you to define rule expressions to match Group Transmission (GTR) flag in the current WTP PDU.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec &gt; ACS Configuration &gt; Ruledef Configuration

active-charging service service_name &gt; ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[l]host_name(config-acd-ruledef)#

**Syntax**

[ no ] wtp gtr operator condition

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  operator must be one of the following:
  - !=: Does not equal
  - ==: Equals

- **condition**
  Specifies the condition to match.
  condition must be one of the following:
  - FALSE
  - TRUE

**Usage**

Use this command to define rule expressions to match the GTR flag (that indicates the last packet of a packet group) in the current WTP PDU.

**Example**

The following command defines a rule expression to match WTP user traffic based on WTP GTR:

```plaintext
wtp gtr = TRUE
```
**wtp pdu-length**

This command allows you to define rule expressions to match WTP PDU length.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] wtp pdu-length operator pdu_length
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `==`: Equals

- **pdu_length**
  Specifies the WTP PDU length (in bytes) to match.
  `pdu_length` must be an integer from 1 through 65535.

**Usage**

Use this command to define rule expressions to match WTP PDU length (header + payload) in bytes.

**Example**

The following command defines a rule expression to match WTP PDU length of 9647 bytes:

```
wtp pdu-length = 9647
```
**wtp pdu-type**

This command allows you to define rule expressions to match WTP PDU type.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] wtp pdu-type operator pdu_type
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  *operator* must be one of the following:
  - `!=`: Does not equal
  - `==`: Equals

- **pdu_type**
  Specifies the WTP PDU type to match.
  *pdu_type* must be one of the following:
  - `abort`
  - `ack`
  - `invoke`
  - `negative-ack`
  - `result`
  - `segment.invoke`
  - `segment.result`

**Usage**

Use this command to define rule expressions to match WTP PDU type.

**Example**

The following command defines a rule expression to match the WTP PDU type `result`:
wtp pdu-type = result
**wtp previous-state**

This command allows you to define rule expressions to match previous WTP state.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

`active-charging service service_name > ruledef ruledef_name`

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] wtp previous-state operator wtp_previous_state
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  - `!=`: Does not equal
  - `==`: Equals

- **wtp_previous_state**
  Specifies the previous state to match.
  - `ack-sent`
  - `init`
  - `invoke-sent`
  - `rcvd`
  - `result-rcvd`

**Usage**

Use this command to define rule expressions to match WTP previous state.

**Example**

The following command defines a rule expression to match user traffic based on WTP previous state of `ack-sent`:

```
wtp previous-state = ack-sent
```
**wtp rid**

This command allows you to define rule expressions to match Re-transmission Indicator (RID) flag set in WTP traffic.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acg-ruledef)#
```

**Syntax**

```
[ no ] wtp rid operator condition
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `==`: Equals

- **condition**
  Specifies the condition to match.
  `condition` must be one of the following:
  - `FALSE`
  - `TRUE`

**Usage**

Use this command to define rule expressions to match WTP RID flag.

**Example**

The following command defines a rule expression to match user traffic containing WTP RID flag:

```
wtp rid = TRUE
```
**wtp state**

This command allows you to define rule expressions to match current WTP state.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] wtp state operator current_state
```

- **no**
  - If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  - Specifies how to match.
  - `operator` must be one of the following:
    - `!=`: Does not equal
    - `=`: Equals

- **current_state**
  - Specifies the current state to match.
  - `current_state` must be one of the following:
    - `ack-sent`
    - `close`
    - `init`
    - `invoke-sent`
    - `rcvd`
    - `result-rcvd`

**Usage**

Use this command to define rule expressions to match current WTP state.

**Example**

The following command defines a rule expression to match user traffic based on current WTP state `close`:

```
wtp state = close
```
**wtp tid**

This command allows you to define rule expressions to match WTP Transaction Identifier (TID).

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] wtp tid operator transaction_id
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `=`: Equals

- **transaction_id**
  Specifies the transaction identifier to match.
  `transaction_id` must be an integer from 0 through 65535.

**Usage**

Use this command to define rule expressions to match WTP TID. This expression ignores the high order bit in the protocol that indicates the direction.

**Example**

The following command defines a rule expression to match user traffic containing WTP TID value of 22:

```
wtp tid = 22
```
wtp transaction class

This command allows you to define rule expressions to match WTP Transaction Class (TCL) state.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acns-ruledef)#

Syntax

[ no ] wtp transaction class operator transaction_class

- **no**
  - If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  - Specifies how to match.
  - **operator** must be one of the following:
    - !=: Does not equal
    - ==: Equals

- **transaction_class**
  - Specifies the WTP TCL to match.
  - **transaction_class** must be an integer from 0 through 2.

Usage
Use this command to define rule expressions to match WTP transaction class.

Example
The following command defines a rule expression to match WTP traffic based on WTP transaction class 2:

wtp transaction class = 2
**wtp ttr**

This command allows you to define rule expressions to match WTP Trailer Transmission (TTR) flag.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```plaintext
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] wtp ttr operator condition
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `==`: Equals

- **condition**
  Specifies the condition to match.
  `condition` must be one of the following:
  - `FALSE`
  - `TRUE`

**Usage**

Use this command to define rule expressions to match TTR flag (used to indicate the last packet in a segmented message) in the current WTP PDU.

**Example**

The following command defines a rule expression to match WTP traffic based on the presence of the WTP TTR flag:

```
wtp ttr = TRUE
```
wtp uplink

This command allows you to define rule expressions to match uplink (subscriber to network) WTP packets.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acsc-ruledef)#
```

**Syntax**

```
[ no ] wtp uplink operator condition
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match. 
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `=`: Equals

- **condition**
  Specifies the condition to match. 
  `condition` must be one of the following:
  - `FALSE`
  - `TRUE`

**Usage**

Use this command to define rule expressions to match uplink WTP packets.

**Example**

The following command defines a rule expression to match all uplink WTP packets:

```
wtp uplink = TRUE
```
www any-match

This command allows you to define rule expressions to match all WWW packets. It is true for HTTP, WAP1.x, and WAP2.0 protocols.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] www any-match operator condition

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be one of the following:
• !=: Does not equal
• ==: Equals

condition
Specifies the condition to match.
condition must be one of the following:
• FALSE
• TRUE

Usage
Use this command to define rule expressions to match all WWW packets. This expression is true for HTTP, WAP1.x, and WAP2.0 protocols

Example
The following command defines a rule expression to match all WWW packets:

www any-match = TRUE
www content type

This command allows you to define rule expressions to match the Content-Type field of HTTP/WSP headers.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local] host_name(config-acs-ruledef)#

Syntax

[ no ] www content type [ case-sensitive ] operator content_type

---

no
If previously configured, deletes the specified rule expression from the current ruledef.

---

case-sensitive
Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

---

operator
Specifies how to match.
operator must be one of the following:

- !=: Does not equal
- !contains: Does not contain
- !ends-with: Does not end with
- !starts-with: Does not start with
- =: Equals
- contains: Contains
- ends-with: Ends with
- starts-with: Starts with

---

content_type
Specifies the value to match.
content_type must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters.
Usage
Use this command to define rule expressions to match the “content type” field of HTTP/WSP header.

Example
The following command defines a rule expression to match the WWW content type Accept:

```
www content type = Accept
```
www domain

This command allows you to define rule expressions to match the domain portion of URIs in WSP/HTTP packets.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] www domain [ case-sensitive ] operator domain

no
If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive
Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator
Specifies how to match.
operator must be one of the following:
• !=: Does not equal
• !contains: Does not contain
• !ends-with: Does not end with
• !starts-with: Does not start with
• =: Equals
• contains: Contains
• ends-with: Ends with
• starts-with: Starts with

domain
Specifies the domain to match.
domain must be an alphanumeric string of 1 through 127 characters.

Usage
Use this command to define rule expressions to match the domain portion of URIs in WSP/HTTP packets.
From the URL, after http:// (if present) is removed, everything until the first "/" is the domain.

The following command defines a rule expression to match user traffic based on domain name testdomain:

```plaintext
www domain = testdomain
```
**www downlink**

This command allows you to define rule expressions to match downlink (network to subscriber) HTTP/WSP packets.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > ACS Configuration > Ruledef Configuration

`active-charging service service_name > ruledef ruledef_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] www downlink operator condition
```

- **no**
  
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  
  Specifies how to match.

  - Operator must be one of the following:
    - !=: Does not equal
    - ==: Equals

- **condition**
  
  Specifies the condition to match.

  - Condition must be one of the following:
    - FALSE
    - TRUE

**Usage**

Use this command to define rule expressions to match downlink HTTP/WSP packets.

**Example**

The following command defines a rule expression to match all downlink WWW packets:

```
www downlink = TRUE
```
www first-request-packet

This command allows you to define rule expressions to match the GET or POST request, if it is the first WSP/HTTP request for the subscriber’s session.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax
[ no ] www first-request-packet operator condition

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  - !=: Does not equal
  - ==: Equals

- **condition**
  Specifies the condition to match.
  - FALSE
  - TRUE

Usage
Use this command to define rule expressions to match the GET or POST request, if it is the first WSP/HTTP request for the subscriber’s session.

Example
The following command defines a rule expression to match user traffic based on the WWW first-request-packet:

```plaintext
www first-request-packet = TRUE
```
www header-length

This command allows you to define rule expressions to match WWW packet header length.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] www header-length operator header_length

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be one of the following:
- !=: Does not equal
- <=: Lesser than or equals
- ==: Equals
- >=: Greater than or equals

header_length
Specifies the WWW packet header length (in bytes) to match, header_length must be an integer from 0 through 65535.

Usage
Use this command to define rule expressions to match WWW packet header length.

Example
The following command defines a rule expression to match user traffic based on WWW packet header length of 10000 bytes:

www header-length = 10000
**www host**

This command allows you to define rule expressions to match the “host name” header field present in HTTP/WSP headers.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] www host [ case-sensitive ] operator host_name
```

- **no**
  
  If previously configured, deletes the specified rule expression from the current ruledef.

- **case-sensitive**
  
  Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

- **operator**
  
  Specifies how to match. 
  **operator** must be one of the following:
  - `!=`: Does not equal
  - `!contains`: Does not contain
  - `!ends-with`: Does not end with
  - `!starts-with`: Does not start with
  - `=`: Equals
  - `contains`: Contains
  - `ends-with`: Ends with
  - `starts-with`: Starts with

- **host_name**
  
  Specifies the WWW host name to match. 
  **host_name** must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters.
Usage

Use this command to define rule expressions to match the host name header field present in HTTP/WSP headers.

Example

The following command defines a rule expression to match user traffic based on WWW host name `host1`:

```plaintext
www host = host1
```
www payload-length

This command allows you to define rule expressions to match WWW payload length.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] www payload-length operator payload_length

---

no

If previously configured, deletes the specified rule expression from the current ruledef.

---

operator

Specifies how to match.

operator must be one of the following:

• !=: Does not equal
• <=: Lesser than or equals
• ==: Equals
• =>: Greater than or equals

---

payload_length

Specifies the payload length (in bytes) to match.

payload_length must be an integer from 1 through 400000000.

Usage

Use this command to define rule expressions to match WWW payload length.

Example

The following command defines a rule expression to match user traffic based on WWW payload length of 10000:

www payload-length = 10000
www pdu-length

This command allows you to define rule expressions to match WWW PDU length.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] www pdu-length operator pdu_length

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be one of the following:
• !=: Does not equal
• <=: Lesser than or equals
• ==: Equals
• >=: Greater than or equals

pdu_length
Specifies the WWW PDU length (in bytes) to match.
pdu_length must be an integer from 0 through 65535.

Usage
Use this command to define rule expressions to match WWW PDU length (header + payload) in bytes.

Example
The following command defines a rule expression to match user traffic based on WWW PDU length of 9767 bytes:

www pdu-length = 9767
www previous-state

This command allows you to define rule expressions to match previous HTTP/WSP(HTTP) state.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] www previous-state operator www_previous_state

no
If previously configured, deletes the specified rule expression from the current ruledef.

operator
Specifies how to match.
operator must be one of the following:
• !=: Does not equal
• =: Equals

www_previous_state
Specifies the previous state to match.
www_previous_state must be one of the following:
• init
• response-error
• response-ok
• waiting-for-response

Usage
Use this command to define rule expressions to match a previous HTTP/WSP(HTTP) state.

Example
The following command defines a rule expression to match user traffic based on WWW previous state init:

www previous-state = init
www reply code

This command allows you to define rule expressions to match WWW reply code arguments.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] www reply code operator reply_code

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  * **operator** must be one of the following:
    - !=: Does not equal
    - <=: Lesser than or equals
    - =: Equals
    - >=: Greater than or equals

- **reply_code**
  Specifies the reply code to match.
  * **reply_code** must be an integer from 100 through 599.

Usage

Use this command to define rule expressions to match HTTP 1.1 status code, or WSP status code that has been remapped to the corresponding HTTP value.

WSP status codes 0 – 101 are automatically remapped to the HTTP status code values, as defined by Table 36 WAP-230-WSP Version 5.

Example

The following command defines a rule expression to analyze WWW user traffic based on reply code of 125:

www reply code = 125
www state

This command allows you to define rule expressions to match current HTTP/WSP(HTTP) state.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Ruledef Configuration

```
active-charging service service_name > ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-ruledef)#
```

**Syntax**

```
[ no ] www state operator current_state
```

- **no**
  If previously configured, deletes the specified rule expression from the current ruledef.

- **operator**
  Specifies how to match.
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `=`: Equals

- **current_state**
  Specifies the current state to match.
  `current_state` must be one of the following:
  - `close`
  - `response-error`
  - `response-ok`
  - `waiting-for-response`

**Usage**

Use this command to define rule expressions to match current HTTP/WSP state.

**Example**

The following command defines a rule expression to match user traffic based on the current WWW state:

```
www state = close
```
www transfer-encoding

This command allows you to define rule expressions to match the transfer encoding field present in HTTP/WSP(HTTP) headers.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration
active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] www transfer-encoding [ case-sensitive ] operator transfer_encoding

no
If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive
Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator
Specifies how to match.
operator must be one of the following:
  -=: Does not equal
  -!contains: Does not contain
  -!ends-with: Does not end with
  -!starts-with: Does not start with
  -:=: Equals
  -contains: Contains
  -ends-with: Ends with
  -starts-with: Starts with

transfer_encoding
Specifies the WWW transfer encoding to match.
transfer_encoding must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters.
Usage

Use this command to define rule expressions to match the “transfer encoding” field present in HTTP/WSP(HTTP) headers.

Example

The following command defines a rule expression to match user traffic based on the WWW transfer encoding user1:

```plaintext
www transfer-encoding = user1
```
www url

This command allows you to define rule expressions to match URL for any Web protocol analyzer—HTTP, WAP1.X, WAP2.0.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Ruledef Configuration

active-charging service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-ruledef)#

Syntax

[ no ] www url [ case-sensitive ] operator url

no
If previously configured, deletes the specified rule expression from the current ruledef.

case-sensitive
Specifies that the rule expression be case-sensitive. By default, rule expressions are not case-sensitive.

operator
Specifies how to match.

operator must be one of the following:
- !=: Does not equal
- !contains: Does not contain
- !ends-with: Does not end with
- !starts-with: Does not start with
- =: Equals
- contains: Contains
- ends-with: Ends with
- regex: Regular expression
- starts-with: Starts with

url
Specifies the URL to match.
url must be an alphanumeric string of 1 through 127 characters and may contain punctuation characters.
Usage

Use this command to define rule expressions to match the URL for any Web protocol analyzer—HTTP, WAP1.X, WAP2.0.

The following table lists the special characters that you can use in regex rule expressions. For more information on regex support, refer to the Enhanced Charging Service Administration Guide.

### Table 13. Special Characters Supported in Regex Rule Expressions

<table>
<thead>
<tr>
<th>Regex Character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Zero or more characters</td>
</tr>
<tr>
<td>+</td>
<td>Zero or more repeated instances of the token preceding the +</td>
</tr>
<tr>
<td>?</td>
<td>Match zero or one character</td>
</tr>
<tr>
<td>\</td>
<td>Escaped character</td>
</tr>
<tr>
<td>?</td>
<td>Match the question mark (&lt;ctrl-v&gt;? character</td>
</tr>
<tr>
<td>+</td>
<td>Match the plus character</td>
</tr>
<tr>
<td>*</td>
<td>Match the asterisk character</td>
</tr>
<tr>
<td>\a</td>
<td>Match the Alert (ASCII 7) character</td>
</tr>
<tr>
<td>\b</td>
<td>Match the Backspace (ASCII 8) character</td>
</tr>
<tr>
<td>\f</td>
<td>Match the Form-feed (ASCII 12) character</td>
</tr>
<tr>
<td>\n</td>
<td>Match the New line (ASCII 10) character</td>
</tr>
<tr>
<td>\r</td>
<td>Match the Carriage return (ASCII 13) character</td>
</tr>
<tr>
<td>\t</td>
<td>Match the Tab (ASCII 9) character</td>
</tr>
<tr>
<td>\v</td>
<td>Match the Vertical tab (ASCII 11) character</td>
</tr>
<tr>
<td>\0</td>
<td>Match the Null (ASCII 0) character</td>
</tr>
<tr>
<td>\</td>
<td>Match the backslash character</td>
</tr>
<tr>
<td>Bracketed range [0-9]</td>
<td>Match any single character from the range</td>
</tr>
<tr>
<td>A leading ^ in a range</td>
<td>Do not match any in the range. All other characters represent themselves.</td>
</tr>
<tr>
<td>\x##</td>
<td>Any ASCII character as specified in two-digit hex notation. For example, \x5A yields a “Z”.</td>
</tr>
</tbody>
</table>

**Important:** The CLI does not support configuring “?” directly, you must instead use “\077”.

For example, if you want to match the string “xyz<any one character>pqr”, you must configure it as: `http host regex "xyz\077pqr"`

In another example, if you want to exactly match the string “url?resource=abc”, you must configure it as: `http uri regex "url\077resource=abc"`

Where, the first “\” (backslash) is for the escaping of “?” and then “\077” for specifying “?” to the CLI.
**Regex Character** | **Description**
---|---
| | Specify OR regular expression operator

**Important:** When using the regex operator “|” in regex expressions, always wrap the string in double quotes.

For example, if you want to match the string "pqr" OR "xyz", you must configure it as:

```
http host regex "pqr|xyz".
```

### Example

The following command defines a rule expression to match user traffic based on WWW URL `www.abc.com`:

```
www url = www.abc.com
```


```
www url regex
"http://(tp2.site.com|134.210.11.3)/httppvcdnsssite.com.wap.symphonieserver.musicwaver.com/"
```
Chapter 20
ACS Timedef Configuration Mode Commands

The ACS Timedef Configuration Mode enables configuring the Time-of-Day Activation/Deactivation feature.

Important: This configuration mode is only available in StarOS 8.1 and in StarOS 9.0 and later releases.

Mode

Exec > ACS Configuration > Timedef Configuration

active-charging service service_name > timedef timedef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-timedef)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

end

**Usage**
Use this command to return to the Exec mode.
**exit**

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Use this command to return to the parent configuration mode.
**start**

This command allows you to configure timeslots in the current timedef.

**Important:** This command is only available in StarOS 8.1 and in StarOS 9.0 and later releases.

**Important:** A maximum of 24 timeslots can be specified within a timedef.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > ACS Configuration > Timedef Configuration

```
active-charging service service_name > timedef timedef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-timedef)#
```

**Syntax**

```
[ no ] start day { friday | monday | saturday | sunday | thursday | tuesday | wednesday } time hh mm ss end day { friday | monday | saturday | sunday | thursday | tuesday | wednesday } time hh mm ss
```

```
[ no ] start time hh mm ss end time hh mm ss
```

If previously configured, removes the specified timeslot from the current timedef.

```
start day { friday | monday | saturday | sunday | thursday | tuesday | wednesday } time hh mm ss end day { friday | monday | saturday | sunday | thursday | tuesday | wednesday } time hh mm ss
```

Specifies a timeslot with a start day and time, and an end day and time.

- **start day**: Specifies the start day and start time.
- **end day**: Specifies the end day and end time.
- **time hh mm ss**: Specifies the start/end time:
  - **hh**: Specifies the start/end hour, and must be an integer from 0 through 23.
  - **mm**: Specifies the start/end minute, and must be an integer from 0 through 59.
  - **ss**: Specifies the start/end second, and must be an integer from 0 through 59.

```
start time hh mm ss end time hh mm ss
```

Specifies a timeslot with a start time and an end time to be applicable for all days of the week.
In specifying the start/end time:
- **hh**: Specifies the start/end hour, and must be an integer from 0 through 23.
- **mm**: Specifies the start/end minute, and must be an integer from 0 through 59.
- **ss**: Specifies the start/end second, and must be an integer from 0 through 59.

**Usage**

Use this command to create timeslots in a timedef during which rules have to be active. Timedefs enable activation/deactivation of ruledefs/group-of-ruledefs such that they are available for rule matching only when they are active.

When a packet is received, and a ruledef/group-of-ruledefs is eligible for rule matching, if a timedef is associated with the ruledef/group-of-ruledefs, before rule matching, the packet-arrival time is compared with the timeslots configured in the timedef. If the packet arrived in any of the timeslots configured in the associated timedef, rule matching is undertaken, else the next ruledef/group-of-ruledefs is considered.

**Important**: The time considered for timedef matching is the system’s local time.

This release does not support configuring a timeslot for a specific date.

If in a timeslot, only the time is specified that timeslot will be applicable for all days.

If for a timeslot “start time” is after “end time”, that rule will span midnight and be considered to be active from the current day until the next day.

If for a timeslot, “start day” is after “end day”, that rule will span the current week until the end day in the next week.

In the following cases a rule will be active all the time:
- A timedef is not configured in an action priority
- A timedef is configured in an action priority, but the named timedef is not defined
- A timedef is defined but without timeslots

**Example**

The following command specifies a timeslot that starts on **Tuesday at 09:00:00** and ends on **Friday at 21:30:00**:

```
start day tuesday time 9 0 0 end day friday time 21 30 0
```

The following command specifies a timeslot that starts at **15:00:00** and ends at **17:00:00** on all days of the week:

```
start time 15 0 0 end time 17 0 0
```

The following command specifies a timeslot that starts on **Friday at 22:00:00** and ends on **Tuesday at 08:00:00**. This timeslot spans the complete week until the end day, up to **Tuesday**.

```
start day friday time 22 0 0 end day tuesday time 8 0 0
```

The following command specifies a timeslot that starts at **16:00:00** and ends at **09:00:00** on all days of the week. Also, as start time > end time, this timeslot spans midnight too (that is, from **16:00:00 to 23:59:59** and from **00:00:00 to 09:00:00**).

```
start time 16 0 0 end time 9 0 0
```
The ACS x-header Format Configuration Mode is used to create and configure extension-header (x-header) formats.

**Important**: This feature is license dependent. Please contact your Cisco sales representative for more information.

**Mode**

Exec > ACS Configuration > ACS xheader Format Configuration

```
active-charging service service_name > xheader-format format_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-acs-xheader)#
```

**Important**: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Use this command to return to the parent configuration mode.
**insert**

This command allows you to configure the x-header fields to be inserted in HTTP/WSP GET and POST request packets.

---

**Important:** This command is license dependent. Please contact your Cisco accounts representative for more information.

---

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > ACS xheader Format Configuration

```
active-charging service service_name > xheader-format format_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-acs-xheader)#
```

**Syntax**

In StarOS 8.1, StarOS 9.0, and later releases:

```
insert xheader_field_name { string-constant xheader_field_value | variable { bearer { 3gpp { apn | charging-characteristics | charging-id | imei | imsi | qos | rat-type | smcc-mnc | ggsn-address } | acr | congestion-level | customer-id | dest-server-ip-address-port | ggsn-address | mdn | msisdn-no-cc radius-string | radius-calling-station-id | session-id | sn-rulebase | subscriber-ip-address | time-of-day | username } [ encrypt ] | http { host | url } } [ delete-existing ] }
```

```
no insert xheader_field_name
```

In StarOS 8.0:

```
insert xheader_field_name { string-constant xheader_field_value | variable { bearer { 3gpp charging-id | ggsn-address | imsi | radius-string | radius-calling-station-id | ggsn-address | sn-rulebase | subscriber-ip-address } | http { host | url } }
```

```
no insert xheader_field_name
```

**no**

If previously configured, removes the specified x-header field configuration.

```
xheader_field_name
```

Specifies the x-header field name to be inserted in the packets.

*xheader_field_name* must be an alphanumeric string of 1 through 31 characters.

Up to ten fields can be inserted in each x-header format.
**string-constant xheader_field_value**

Specifies constant a string value for x-header field to be inserted in the packets. 

*xheader_field_value* must be the x-header field value, and must be an alphanumeric string of 1 through 63 characters.

---

**variable**

Specifies name of the x-header field whose value must be inserted in the packets.

```c
bearer { 3gpp { apn | charging-characteristics | charging-id | imei | imsi | qos | rat-type | s-mcc-mnc | ggsn-address } | acr | congestion-level | customer-id | dest-server-ip-address-port | ggsn-address | mdn | msisdn-no-cc | radius-string | radius-calling-station-id | session-id | sn-rulebase | subscriber-ip-address | time-of-day | username } [ encrypt ]
```

Specifies value of x-header field to be inserted:

- **3gpp**: 3GPP service.
  - **apn**: APN of the bearer flow. This field is deprecated from under *bearer apn* and has been added within *bearer 3gpp apn*. The APN added via *bearer 3gpp apn*.
  - **charging-characteristics**: Charging characteristics of the bearer flow.
  - **charging-id**: Charging ID of the bearer flow.
  - **imei**: IMEI or IMEISV (depending on the case) associated with the bearer flow.
  - **imsi**: Specific Mobile Station Identification number.
  - **qos**: EPC QoS associated with the bearer flow.
  - The inserted x-header is seen as:
    ```
    x-bearer-qos: 020400000100000002000000010000000200
    ```
  - **rat-type**: This field is deprecated from under *bearer rat-type* and has been added within *bearer 3gpp rat-type*. The RAT type as added via *bearer 3gpp rat-type*.
  - **s-mcc-mnc**: 3GPP serving node MCC + MNC associated with the bearer.
    ```
    x-s-mcc-mnc: 123765
    ```
  - **ggsn-address**: GGSN IP address field.
  - **imsi**: This field is deprecated from within *bearer imsi* and has been moved within *bearer 3gpp imsi*. The IMSI as added via *bearer 3gpp imsi*.
  - **mdn**: MDN of the bearer flow.
  - **msisdn-no-cc**: MSISDN of the mobile handling the flow without the country code.
- **radius-string**: SN-Transparent-Data Attribute received in RADIUS ACCESS ACCEPT message.
- **radius-calling-station-id**: Calling Station ID of the mobile handling the flow. Use this for MSISDN of the mobile handling the flow with the country code.
- **session-id**: Accounting session ID of the bearer flow.
- **sn-rulebase**: Name of the ACS rulebase.
- **sgsn-address**: This field is deprecated from under **bearer sgsn-address** and has been moved within **bearer 3gpp sgsn-address**. The SGSN address as added via **bearer 3gpp sgsn-address**.
- **subscriber-ip-address**: Subscriber IP address.
- **time-of-day**: The current date, time, and time zone offset of the subscriber.
- **username**: User name of the bearer flow.

**encrypt**: Specifies encryption of x-header field configuration. This option must only be configured when x-header encryption is enabled.

```
http { host | url }
```

Specifies value of the x-header field to be inserted:
- **host**: Host
- **url**: Uniform Resource Locator

**delete-existing**

Specifies enabling detection of spoofing in x-header fields. The x-header field configured with this keyword will be removed from the HTTP header if it already exists, and only the gateway inserted field will remain. By default, anti spoofing is disabled, and if required, should be enabled at a field level.

**Usage**

Use this command to configure the x-header fields to be inserted in HTTP/WSP GET and POST request packets. The x-headers would be inserted at the end of the HTTP/WSP header. This CLI command may be used up to 10 times. There is no control over the order of the fields that are to be inserted. Any of the indicated ruledef variables may be inserted using the variable option, or a static string may be inserted using the string-constant option.

Operators may insert x-headers in some HTTP/WSP packets, for which some rules will be configured. The charging-action associated with these rules will contain the list of x-headers to be inserted in the packets.

**Example**

The following command configures an x-header field named test12 with a constant string value of testing to be inserted in HTTP/WSP GET and POST request packets:

```
insert test12 string-constant testing
```
Chapter 22
ALCAP Configuration Mode Commands

The ALCAP Service Configuration Mode is used to create, provide, and manage the Access Link Control Application Part (ALCAP) on HNB-GW to support IuCS-over-ATM connectivity to HNB subscriber in a 3G UMTS networks towards CS core network.

Mode

Exec > Global Configuration > Context Configuration > ALCAP Service Configuration

configure > context context_name > alcap-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-alcap-service-service_name)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
aal2-node

This command creates/configures AAL2 node configuration to defined AAL2 node properties for IuCS-over-ATM functionality.

Product
HNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > ALCAP Service Configuration
configure > context context_name > alcap-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-alcap-service-service_name)#

Syntax

```
aal2-node aal2_node_name [-noconfirm]
no aal2-node aal2_node_name
```

- `no`: Removes the configured AAL2 node from ALCAP service configuration.

  ```
  aal2_node_name
  ```

  Identifies the name of the AAL2 node name to configure the AAL2 node parameters. The `aal2_node_name` must be an alphanumerical string from 1 through 63 characters.

Usage

Use this command to create/configure the AAL2 node configuration and switch to AAL2 Node Configuration mode.

Entering this command results in the following prompt:

```
[context_name]host_name(config-alcap-service-service_name)#
```

A maximum of TBD AAL2 node can be configured in one ALCAP service.

**Important:** The AAL2 Node configured here will be used to bind with ATM port in PVC Configuration sub-mode of ATM Configuration mode for IuCS-over-ATM functionality.

**Important:** For more information on AAL2 node configuration, refer *AAL2 Node Configuration Mode Commands*.

Example

Following command creates AAL2 node configuration mode named `aal2_1` within the specific ALCAP service for IuCS-over-ATM support towards CS core networks and switch the user to AAL2 Node Configuration Mode named `aal2_1`:
`aal2-node aal2_node_name -noconfirm`
**aal2-route**

This command defines a route for each ATM Endpoint Service Address (AESA) with which it can have transport layer communication. This route actually maps an AESA to one or more AAL2 paths which will be used to setup an end to end communication path.

**Product**

HNB-GW

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > ALCAP Service Configuration

`configure > context context_name > alcap-service service_name`

Entering the above command sequence results in the following prompt:

```
[context_name] host_name(config-alcap-service-service_name)#
```

**Syntax**

```
aal2-route end-point {AESA_address | default} aal2-node aal2_node_name
no aal2-route end-point {AESA_address | default} [aal2-node aal2_node_name]
```

*no*

Removes defined AAL2 route from ALCAP service configuration.

```
end-point {AESA_address | default}
```

Specifies the AESA address in an ATM (or AAL2) network to map with adjacent AAL2 node. The AESA is based on the generic network service access point (NSAP) format. The ATM connection from HNB-GW terminates at this point.

The **AESA_address** must be an alpha/numeric string from 1 through 63 characters.

The **default** keyword is used to configure a default AAL2 route which will match any AESA received from MSC and for which AESA specific route is not configured. When a connection is established an AESA specific route will have higher priority than **default** route.

```
aal2-node aal2_node_name
```

Identifies the name of the AAL2 node name to configure in AAL2 route.

The **aal2_node_name** must be an alphanumerical string from 1 through 63 characters.

**Usage**

Use this command to create a mapping between ATM endpoint and adjacent node for AAL2 connection routing purposes.

It defines a route for each ATM Endpoint Service Address (AESA) with which it can have transport layer communication. This route actually maps an AESA to one or more AAL2 paths which will be used to setup an end to end communication path.
The **default** keyword can be used to configure a default **aal2-route** which will match any AESA received from MSC and for which AESA specific route is not configured. When a connection is established an AESA specific route will have higher priority than default route.

**Important:** The default route shall not be used when AESA specific route exists.

If an HNB-GW configured with a route for **MGW1** which consists of **AAL2_path_A** and **AAL2_path_B** for **AAL2 switch-A** and **AAL2 switch-B** switch respectively then similarly **AAL2 switch-A** and **AAL2 switch-B** need to be configured with routes for **MGW1**. A maximum of **TBD** AAL2 routes can be configured in one ALCAP service.

**Example**

Following command create a mapping between ATM endpoint **MGW1** and AAL2 node **aal2_1** for AAL2 connection routing purposes:

```
aal2-route end-point MGW1 aal2-node aal2_1
```
associate

This command associates a previously configured SS7 routing domain with this ALCAP service on HNB-GW node which will be used to define the SS7 routing domain in 3G UMTS networks.

Product
HNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > ALCAP Service Configuration
configure > context context_name > alcap-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-alcap-service-service_name)#

Syntax

**associate ss7-routing-domain ss7_rd_id**

**no associate ss7-routing-domain**

**no**

Removes the associated SS7 routing domain id from this ALCAP service configuration.

**ss7_rd_id**

Identifies the SS7 routing domain index configured in Global configuration mode to associate with ALCAP service for IuCS-over-ATM support.

The ss7_rd_id must be an integer from 1 through 12.

**Important:** For SS7 routing domain configuration, refer *SS7 Routing Domain Configuration Commands Mode* chapter.

Usage

Use this command to associate a preconfigured SS7 routing domain index to provide IuCS-over-ATM support towards CS core network for HNB subscriber.

A maximum of TBD SS7 routing domains can be configured in one ALCAP service.

Example

Following command associates a predefined SS7 routing domain id 3 with ALCAP service to define routing domain for IuCS-over-ATM support towards CS core networks:

```bash
associate ss7-routing-domain 3
```
end

Exits the current mode and returns to the Exec Mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**
Change the mode back to the Exec mode.
exit

Exits the current mode and returns to the previous mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
exit
```

**Usage**

Return to the previous mode.
maximum reset-retransmission

This command sets the maximum number of retries allowed for transmission of RESET message to reset the AAL2 path.

Product  
HNB-GW

Privilege  
Security Administrator, Administrator

Mode  
Exec > Global Configuration > Context Configuration > ALCAP Service Configuration
configure > context context_name > alcap-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-alcap-service-service_name)#

Syntax

maximum reset-retransmissions retries

default maximum reset-retransmissions

default

Sets the number of RESET message retries to default value of 1.

retries

Sets the maximum number of retries allowed for transmission of RESET message to reset the AAL2 path by ALCAP service.

retries must be an integer value from 0 through 4. When 0 is used retransmission will be disabled. Default: 1

Usage

Use this command to sets the maximum number of retries allowed for transmission of RESET message by ALCAP service to reset the AAL2 path when Timer_RES expires. Once the maximum number of RESET retries have been performed the ALCAP service shall stop the RESET procedure for the affected path and path will become available for connections.

Example

The following command configures ALCAP service to send maximum number of 2 RESET messages after expiry of RESET timer for AAL2 path RESET procedure:

maximum reset-retransmissions 2

Cisco ASR 5x00 Command Line Interface Reference
self-point-code

This command specifies the SS7 point code address for ALCAP service.

Product
HNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > ALCAP Service Configuration

configure > context context_name > alcap-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-alcap-service-service_name)#

Syntax

self-point-code point_code

no self-point-code

no

Deletes the configured self point code for this ALCAP service.

point_code

Defines the point code to assign to this ALCAP service.

point_code: value entered must adhere to the point code variant selected when the ALCAP service instance was defined:

- ITU Range 0.0.1 to 7.255.7
- ANSI Range 0.0.1 to 255.255.255
- TTC Range 0.0.1 to 15.31.255
- a string of 1 to 11 combined digits and period.

Usage

Use this command to assign the self point code to use for this ALCAP service.

Example

The following command sets an ITU-based point code for this ALCAP service:

self-pointcode 4.121.5

The following command removes the configured self-point code:

no self-pointcode
timeout alcap

This command configures the timeout duration for various ALCAP procedure timers in ALCAP service.

**Product**
HNB-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > ALCAP Service Configuration

```
configure > context context_name > alcap-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-alcap-service-service_name)#
```

**Syntax**

```
timeout alcap {blo blo_timer_value | erq erq_timer_value | mod mod_timer_value | rel rel_timer_value | res res_timer_value | ubl ubl_timer_value}

default timeout alcap {blo | erq | mod | rel | res | ubl}
```

**default**
Sets the timer values to default duration for specific ALCAP procedure in an ALCAP service.

**blo blo_timer_value**
Specifies the maximum time, in seconds, the system waits for response from adjacent AAL2 node before reporting the failure of AAL2 Path Block procedure. When a request to block a particular AAL2 path is received by ALCAP service, the ALCAP service sends ALCAP-BLOCK-REQUEST message to AAL2 node/peer ALCAP Manage and starts Timer_BLO timer. The timer waits for specified timeout duration `blo_timer_value` for ALCAP-BLOCK-CONFIRM message before reporting error in procedure. If AAL2 Node responds with ALCAP-BLOCK-CONFIRM message the timer will stop before the expiry of timeout duration and system reports the successful completion of the procedure. `blo_timer_value` must be an integer value from 2 through 60.

Default: 5

**erq erq_timer_value**
Specifies the maximum time, in seconds, the system waits for response from adjacent AAL2 node before reporting the failure of AAL2 Establish Request procedure. When a request to establish a connection through ALCAP-ESTABLISH-REQUEST message is sent to AAL2 node the system starts the Timer_ERQ timer. The timer waits for specified timeout duration `erq_timer_value` for ALCAP-ESTABLISH-CONFIRM message before reporting error in procedure and system requests ALCAP Manager to free the AAL2-channel used for connection and also indicates to start the RESET procedure for this channel. If AAL2 Node responds with ALCAP-ESTABLISH-CONFIRM message the timer will stop before the expiry of timeout duration and system reports the successful completion of the procedure. `erq_timer_value` must be an integer value from 5 through 30.

Default: 5
mod  mod_timer_value

Specifies the maximum time, in seconds, the system waits for response from adjacent AAL2 node before reporting the failure of AAL2 Modify Request procedure. When a request to modify a connection or channel through ALCAP-MODIFY-REQUEST message is sent to AAL2 node the system starts the Timer_MOD timer. The timer waits for specified timeout duration mod_timer_value for ALCAP-MODIFY-CONFIRM message before reporting error in procedure and system requests ALCAP Manager to initiates the RESET or any other appropriate procedure for this channel and HNB-GW shall release the RUA connection towards HNB and SCCP connection towards CN.

If AAL2 Node responds with ALCAP-MODIFY-CONFIRM message the timer will stop before the expiry of timeout duration and system reports the successful completion of the procedure.

mod_timer_value must be an integer value from 5 through 30.
Default: 5

rel  rel_timer_value

Specifies the maximum time, in seconds, the system waits for response from adjacent AAL2 node before reporting the failure of AAL2 Release Request procedure. When a request to release a connection or channel through ALCAP-RELEASE-REQUEST message is sent to AAL2 node the system starts the Timer_REL timer and sends RAB-ASST-REQ to HNB. The timer waits for specified timeout duration rel_timer_value for ALCAP-RELEASE-CONFIRM message before reporting error in procedure and system requests ALCAP Manager to release the AAL2 channel. System also indicates to start RESET procedure for this channel.

If AAL2 Node responds with ALCAP-RELEASE-CONFIRM message the timer will stop before the expiry of timeout duration and system reports the successful completion of the procedure.

rel_timer_value must be an integer value from 2 through 60.
Default: 2

res  res_timer_value

Specifies the maximum time, in seconds, the system waits for response from adjacent AAL2 node before reporting the failure of AAL2 Reset Request procedure. When a request to reset a connection or channel through ALCAP-RESET-REQUEST message is sent to AAL2 node the system starts the Timer_RES timer. The timer waits for specified timeout duration res_timer_value for ALCAP-RESET-CONFIRM message before retrying the RESET procedure. The system will retry the RESET procedure for configured number of times and on completion of retry limit the stops the RESET procedure for the affected path and path will become available for connections.

If AAL2 Node responds with ALCAP-RESET-CONFIRM message the timer will stop before the expiry of timeout duration and system reports the successful completion of the procedure.

res_timer_value must be an integer value from 2 through 60.
Default: 2

ubl  ubl_timer_value

Specifies the maximum time, in seconds, the system waits for response from adjacent AAL2 node before reporting the failure of AAL2 Path UnBlock procedure. When a request to unblock a particular AAL2 path is received by ALCAP service, the ALCAP service sends ALCAP-UNBLOCK-REQUEST message to AAL2 node/peer ALCAP Manager and start Timer_BLO timer. The timer waits for specified timeout duration ubl_timer_value for ALCAP-UNBLOCK-CONFIRM message before reporting error in procedure.

If AAL2 node/peer ALCAP Manager responds with ALCAP-BLOCK-CONFIRM message the timer will stop before the expiry of timeout duration and system reports the successful completion of the procedure.

ubl_timer_value must be an integer value from 2 through 60.
Default: 2
Usage
Use this command to configure the timeout duration for various ALCAP procedures in ALCAP service.

Example
The following command sets the timeout duration of 10 seconds for ALCAP-MODIFY-REQUEST procedure:

```
timeout alcap mod 10
```
timeout stc

This command configures the timeout duration for STC long (T30) and and STC short (T29) timers used in congestion indication procedure at Signaling Transport Converter (STC) layer in ALCAP service.

Product
HNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > ALCAP Service Configuration
configure > context context_name > alcap-service service_name

Entering the above command sequence results in the following prompt:
context_name host_name(config-alcap-service-service_name)#

Syntax

timeout stc {long long_timer_value | short short_timer_value}

default timeout stc {long | short}

default
Sets the timer values to default duration for specific STC procedure in an ALCAP service.

long long_timer_value
Specifies the duration in milliseconds for STC long timer. This timer is used by the congestion indication procedure. Receipt of a repeated congestion indication from MTP3B before the expiry of this timer is interpreted as the congestion situation. On the other hand, if no congestion indication is received from MTP3B before expiry of this timer, the congestion situation is considered to have improved. long_timer_value must be an integer value from 5000 through 10000. Default: 5000

short short_timer_value
Specifies the duration in milliseconds for STC short timer. This timer is used by the congestion indication procedure. The role of this timer is to avoid overreacting if multiple congestion indications are received from MTP3B in quick succession. short_timer_value must be an integer value from 300 through 600. Default: 300

Usage
Use this command to configure the long (T30) and short (T29) timer for congestion indication procedure in ALCAP service.
When the first congestion indication is received by, the traffic load into the affected destination point code is reduced and the same time two timers STC short timer (T29) and STC long timer (T30) are started. During STC short timer all received congestion indications for the same destination point code are ignored in order
not to reduce traffic too rapidly. Reception of a congestion indication after the expiry of STC short timer, but still during STC long timer, will decrease the traffic load by one more step and restart both the timers again. If STC long timer expires (i.e. no congestion indications having been received during the STC long timer period), traffic will be increased by one step and STC long timer will be restarted unless full traffic load has been resumed.

**Example**

The following command sets the timeout duration of 5000 milliseconds for STC long timer:

```
default timeout stc long
```

The following command sets the timeout duration of 300 milliseconds for STC short timer:

```
default timeout stc short
```
Chapter 23
APN Configuration Mode Commands

The Access Point Name (APN) Configuration Mode is used to create and configure APN profiles within the current system context of an UMTS/LTE service.

Mode

Exec > Global Configuration > Context Configuration > APN Configuration

configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-apn)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
aaa

This command configures Authentication, Authorization, and Accounting (AAA) functionality at the Access Point Name (APN) level.

Product
GGSN
P-GW
SAEGW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > APN Configuration

configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-apn)#

Syntax

aaa { group aaa_group_name | secondary-group aaa_group_name }

default aaa { group | secondary-group aaa_group_name }

no aaa { group aaa_group_name | secondary-group }

no aaa
Disables the specified AAA group for the specific APN.

no aaa { group | secondary-group }

• group: Uses the default AAA group.
• secondary-group: Removes the secondary AAA group from the APN’s configuration.

default aaa { group | secondary-group }

Configures the default setting for the specified parameter.

• group: Uses the default AAA group—the one specified at the context level or in the APN template.
• secondary-group: Removes the secondary AAA group from the APN configuration.

aaa_group_name

Specifies the AAA server group for the APN.

aaa_group_name must be an alphanumeric string of 1 through 63 characters.

secondary-group aaa_group_name

Specifies the secondary AAA server group for the APN.

aaa_group_name must be an alphanumeric string of 1 through 63 characters.
Usage

Use this command to configure AAA functionality at the APN level. Instead of having a single list of servers per context, this feature configures multiple server groups within a context and applies individual server group for APNs in that context. Each server group consists of a list of AAA servers for each AAA function (accounting, authentication, charging, etc.).

The AAA secondary server group supports the RADIUS Fire-and-Forget feature in conjunction with GGSN for secondary accounting (with different RADIUS accounting group configuration) to the RADIUS servers without expecting acknowledgement from the server, in addition to standard RADIUS accounting. This secondary accounting will be an exact copy of all the standard RADIUS accounting message (RADIUS Start / Interim / Stop) sent to the standard AAA RADIUS server.

If the same AAA group is configured with both the `aaa group aaa_group_name` and the `aaa secondary-group aaa_group_name` commands, then this configuration will have no effect and secondary accounting will not happen.

The AAA secondary server group configuration takes effect only when used with APN accounting-mode set to radius-diameter (or) with mediation-acct enabled. The RADIUS accounting triggers for both standard RADIUS accounting and secondary accounting will be taken from the AAA group configured with the `aaa group aaa_group_name` command. On the fly change of this configuration is not supported. Any change to the configuration will have effect only for new calls.

Example

The following command applies the AAA server group `star1` to an APN within the specific context:

```bash
aaa group star1
```
access-link

Configures IP fragmentation processing over the Access-link (PPP, GTP etc.).

Product
GGSN
P-GW
SAEGW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > APN Configuration

```bash
configure > context context_name > apn apn_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-apn)#
```

Syntax

```bash
access-link ip-fragmentation { normal | df-ignore | df-fragment-and-icmp-notify }
```

**default access-link ip-fragmentation**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
</table>
| normal        | Default: Enabled
|               | Drops the packet and sends an ICMP unreachable message to the source of packet. This is the default behavior. |
| df-ignore     | Default: Disabled
|               | Ignores the DF (Don’t Fragment) bit setting; fragments and forwards the packet over the access link. |
| df-fragment-and-icmp-notify | Default: Disabled
|               | Partially ignore the DF bit; fragments and forwards the packet, but also returns an ICMP error message to the source of the packet. The number of ICMP errors sent like this is rate-limited to one ICMP error packet per second per session. |

**Usage**

If the IP packet to be forwarded is larger than the access-link MTU and if the DF (Don't Fragment) bit is set for the packet, then the fragmentation behavior configured by this command is applied. Use this command to fragment packets even if they are larger than the access-link MTU. Fragmentation may also occur for other reasons, regardless of whether or not fragmentation is performed because of one of the above reasons. Payloads are encapsulated within IP/UDP/GTP before being sent to the SGSN. If that encapsulation causes the packet to exceed 1500 bytes, the inner IP payload is fragmented (even if it's not considered too-large by
the above tests) into two payloads (if the DF bit is not set). If the DF bit is set (and access-link ip-
fragmentation normal is configured), the system performs IP fragmentation of the entire packet (i.e., IP
fragmentation in the outer IP header) rather than fragmenting the inner IP payload. Either way, the result is
two packets, but in one case the MS would have to perform IP reassembly while in the other case the SGSN
would have to perform reassembly.

Example

Set fragmentation so that the DF bit is ignored and the packet is forwarded anyway by entering the following
command:

access-link ip-fragmentation df-ignore
accounting-mode

Configures the protocol to be used for PDP context accounting by this APN.

Product
eWAG
GGSN
P-GW
SAEGW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > APN Configuration

configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-apn)#

Syntax

accounting-mode { gtpp | none | radius-diameter [ no-early-pdus ] [ no-interims ] }

default accounting-mode

default
Restores the command to its default setting.

gtpp
Configures the APN to use GPRS Tunneling Protocol Prime for accounting purposes. If used, accounting will begin as soon as the PDP context is established. This is the default setting. Default: Enabled

Important: The system’s GTPP parameters must be configured prior to using this protocol for accounting. Refer to the gtpp commands in the Context Configuration Mode Commands chapter.

none
Disables accounting for PDP contexts using this APN.
When accounting mode is set to none, it indicates to the GTP stack at session manager to not generate the regular GTPP accounting triggers. Default: Disabled.

radius-diameter
Configures the APN to use RADIUS protocol for accounting purposes. Default: Disabled
**Important:** The system’s RADIUS accounting parameters must be configured prior to using either of the protocols for accounting. Refer to the `radius` commands in the *Context Configuration Mode Commands* and the *AAA Server Group Configuration Mode Commands* chapters.

---

**no-early-pdus**

Configures the GGSN to discard user traffic once the buffer is full until the RADIUS server has returned a response to the GGSN’s accounting START request per 3GPP standards.

Configures the GGSN to delay PDUs from/to MS until the RADIUS server returns a response to the GGSN’s accounting START request as per 3GPP standards. The GGSN buffers up to two PDUs per call. Additional PDUs disable the queuing. On receiving the Accounting response message, the GGSN forwards all the subsequent PDUs for that call.

---

**Important:** For StarOS 10.0 and earlier releases, the system buffers up to four PDUs and queues or discards the remaining PDUs.

**Important:** For StarOS 11.0 and later releases, the system is configured so that none of the PDUs are discarded.

**no-interims**

Disables the generation of RADIUS interims per APN.

When configured, RADIUS interim updates for this APN will not be sent, regardless of what is configured in the context that is used for RADIUS accounting.

---

**Important:** Different CLI commands are used to disable RADIUS interims for RADIUS accounting and mediation accounting. To disable RADIUS interims for RADIUS accounting, use the following command: `accounting-mode radius no-interims`. To disable RADIUS interims for mediation accounting, use the following command: `mediation-device context-name context_name no-interims`.

---

**Usage**

This command specifies which protocol, if any, will be used to provide accounting for PDP contexts accessing the APN profile.

When the GTPP protocol is used, accounting messages are sent to the charging gateways (CGs) over the Ga interface. The Ga interface and GTPP functionality are typically configured within the system’s source context. As specified by the standards, a CDR is not generated when a session starts - CDRs are generated according to the interim triggers (configured using the `cc` command in the GGSN service configuration mode) and a CDR is generated when the session ends. For interim accounting, STOP/START pairs are sent based on configured triggers.

GTPP version 2 is always used. However, if version 2 is not supported by the CGF, the system reverts to using GTPP version 1. All subsequent CDRs are always fully-qualified partial CDRs. All CDR fields are R4.

If the `radius` option is used, RADIUS protocol is used as configured in the Context Configuration mode or the AAA Server Group Configuration mode.

If the RADIUS protocol is used, accounting messages can be sent over a AAA interface or the Gi to the RADIUS server. The AAA or Gi interface(s) and RADIUS functionality are typically configured with the system’s destination context along with the APN. RADIUS accounting begins immediately after an IP address is allocated for the MS. Interim accounting can be configured using the `radius` accounting...
**interim interval.** The `radius accounting interim interval` command sends INTERIM-UPDATE messages at specific intervals.

Keywords to this command can be used in combination to each other, depending on configuration requirements.

**Important:** If the accounting type in the APN is set to ‘none’ then G-CDRs will not be generated. If accounting type is left as default “GTPP” and “billing-records” are configured in the ACS Rulebase Configuration Mode, then both G-CDRs and eG-CDRs would be generated.

**Example**

The following command configures the APN to use the RADIUSr protocol for accounting:

```
accounting-mode radius
accounting-mode radius no-interims no-early-pdus
accounting-mode radius no-early-pdus no-interims
```
**active-charging bandwidth-policy**

Configures the bandwidth policy to be used for subscribers who use this APN.

**Product**

ACS

GGSN

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > APN Configuration

    configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

    \[context_name\]host_name(config-apn)\#

**Syntax**

    active-charging bandwidth-policy bandwidth_policy_name

    \{ default | no \} active-charging bandwidth-policy \[ fallback-enabled \]

---

**default**

Configures the default setting.

Default: The default bandwidth policy configured in the rulebase is used for subscribers who use this APN.

---

**no**

Disables bandwidth control for the APN.

---

**bandwidth-policy bandwidth_policy_name**

Specifies the bandwidth policy name. \(\text{bandwidth_policy_name}\) must be an alphanumeric string from 1 through 63 characters.

---

**fallback-enabled**

Determines whether policy under rulebase can be applied as a fallback value. Fallback is disabled by default.

---

**Usage**

Use this command to configure bandwidth policy to be used for subscribers who use this APN.

**Example**

The following command configures a bandwidth policy named \textit{standard} for the APN:

    active-charging bandwidth-policy standard \[ fallback-enabled \]
active-charging link-monitor tcp

Enables the TCP link monitoring feature on the Mobile Video Gateway. This command can be configured in either APN Configuration Mode or Subscriber Configuration Mode.

Product
MVG

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > APN Configuration
configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-apn)#

Syntax


default
Sets TCP link monitoring to its default value, which is the same as no.

no
Deletes the TCP link monitoring settings and disables TCP link monitoring if previously configured.

link-monitor tcp

Enables the TCP link monitoring feature on the Mobile Video Gateway. Note that TCP link monitoring is not enabled by default. Also note that when this command is configured without the log option, TCP link monitoring is enabled without logging, and the output from TCP link monitoring is only used by the dynamic translating feature.


This option enables statistical logging for TCP link monitoring.
The rtt option can be used to enable either histogram or time-series logging for RTT.
Similarly, the bitrate option can be used to enable either histogram or time-series logging for bit rate.
When rtt and bitrate options are used without additional options, histogram and time-series logging are enabled for RTT and/or bit rate respectively.

-noconfirm
Specifies that the command must execute without prompting for confirmation.
Usage

Use this command to enable TCP link monitoring on the Mobile Video Gateway.

Examples

The following command enables TCP link monitoring with statistical logging, with histogram and time-series logging enabled for both RTT and bit rate:

```
active-charging link-monitor tcp log
```

The following command enables TCP link monitoring with statistical logging, with histogram and time-series logging enabled for RTT:

```
active-charging link-monitor tcp log rtt
```

The following command enables TCP link monitoring with statistical logging, with histogram logging enabled for RTT:

```
active-charging link-monitor tcp log rtt histogram
```

The following command enables TCP link monitoring with statistical logging, with histogram logging enabled for RTT and time-series logging enabled for bit rate:

```
active-charging link-monitor tcp log rtt histogram bitrate time-series
```
active-charging rulebase

Specifies the name of the Active Charging Service (ACS) rulebase to be used for subscribers who use this APN.

**Product**
- ACS
- eWAG
- GGSN
- MVG
- P-GW
- SAEGW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > APN Configuration

`configure > context context_name > apn apn_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-apn)#
```

**Syntax**

```
active-charging rulebase rulebase_name

no active-charging rulebase
```

- **no**
  - Removes the rulebase previously configured for this APN.

- **rulebase_name**
  - Specifies the name of the ACS rulebase as an alphanumeric string of 1 through 63 characters.

**Usage**

Use this command to specify the ACS rulebase to be used for subscribers who use the APN.

**Example**

The following command specifies the ACS rulebase named `rule1` for the APN:

```
active-charging rulebase rule1
```
active-charging rulebase-list

Specifies the name of the ACS rulebase list to be used for subscribers who use this APN.

Product

ACS
GGSN
MVG
P-GW

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > Context Configuration > APN Configuration

configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-apn)#

Syntax

active-charging rulebase-list rulebase_list_name

no active-charging rulebase-list

no

If previously configured, removes the rulebase list configured in the APN.

rulebase_list_name

Specifies the name of the ACS rulebase list.

rulebase_list_name must be an alphanumeric string of 1 through 63 characters.

Usage

Use this command to specify the ACS rulebase list to be used for subscribers who use the APN. The rulebase list is created and configured in the ACS Configuration Mode. For more information, see the rulebase-list command in the ACS Configuration Mode Commands chapter.

Example

The following command specifies the ACS rulebase list named rblist for the APN:

active-charging rulebase-list rblist

The following command removes the rulebase list named rblist from the APN:

no active-charging rulebase-list rblist
apn-ambr

Configures the Aggregated Maximum Bit Rate (AMBR) for all PDNs using this APN.

Product
- P-GW
- SAEGW
- GGSN

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > APN Configuration

configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-apn)#

Syntax

apn-ambr rate-limit direction { downlink | uplink } [ burst-size { auto-readjust duration seconds | bytes } | violate-action { drop | lower-ip-precedence | shape [ transmit-when-buffer-full ] | transmit } ]

[ default | no ] apn-ambr rate-limit direction { downlink | uplink }

default

Returns the selected command to it’s default setting of no APN-AMBR.

no

Disables the selected command.

rate-limit direction { downlink | uplink }

Specifies that the rate limit is to be applied to either the downlink (network to subscriber) traffic or the uplink (subscriber to network) traffic.

downlink: Applies the AMBR parameters to the downlink direction.
uplink: Applies the AMBR parameters to the uplink direction.

burst-size { auto-readjust duration seconds | bytes }

This parameter is used by policing and shaping algorithms to permit short bursts of traffic in order to not exceed the allowed data rates. It is the maximum size of the token bucket.

auto-readjust duration seconds: The duration (in seconds) used in this burst size calculation: burst size = peak data rate/8 * auto-readjust duration

seconds must be an integer value from 1 to 30. Default is 1 second

bytes: Specifies the burst size in bytes allowed by this APN for the associated PDNs. It must be an integer from 1 to 4294967295 (1 byte to 4 GB).
**Important:** In 17.3 and later releases, this option has been deprecated.

```
violate-action { drop | lower-ip-precedence | shape [ transmit-when-buffer-full ] | transmit }
```

The action that the P-GW will take when the data rate of the bearer context exceeds the AMBR.
- **drop:** Drops violating packets.
- **lower-ip-precedence:** Sets the DSCP value to zero ("best effort") for violating packets.
- **shape [ transmit-when-buffer-full ]:** Places all violating packets into a buffer and, optionally, transmits the packets when the buffer is full.

**Important:** The **shape** keyword and optional **transmit-when-buffer-full** are only available in StarOS v12.0 and earlier releases. P-GW does not currently support traffic shaping for APN-AMBR.

- **transmit:** Transmits violating packets. This is the default setting.

**Usage**

Use this command to enforce the AMBR for the APN on bearers that do not have a Guaranteed Bit Rate (GBR).

**Example**

The following command sets the downlink burst rate to use an auto-readjust duration of 2 seconds and lowers the IP precedence of violating packets:

```
apn-ambr rate-limit direction downlink burst-size auto-readjust duration 2 violate-action lower-ip-precedence
```
associate accounting-policy

Associates the APN with specific pre-configured policies configured in the same context.

**Product**

P-GW  
SAEGW

**Privilege**

Administrator

**Mode**

Exec > Global Configuration > Context Configuration > APN Configuration  
**configure > context context_name > apn apn_name**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-apn)#
```

**Syntax**

```
[ no ] associate accounting-policy name
```

- **no**
  
  Removes the selected association from this APN.

- **name**

  Associates the P-GW APN with an accounting policy configured in the same context. *name* must be an existing accounting policy expressed as a string of 1 through 63 characters.  
  Accounting policies are configured through the `policy accounting` command in the Context Configuration mode.

**Usage**

Use this command to associate the P-GW APN with an accounting policy configured in this context.

**Example**

The following command associates this P-GW APN with an accounting policy called *acct1*:

```
associate accounting-policy acct1
```
associate qci-qos-mapping

Associates a pre-configured QCI-QoS-Mapping table with this APN to support per APN DSCP marking.

**Product**
- P-GW
- SAEGW

**Privilege**
- Administrator

**Mode**
- Exec > Global Configuration > Context Configuration > APN Configuration
- configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-apn)>
```

**Syntax**

```
[ no ] associate qci-qos-mapping qci_qos_map_table_name
```

- **no**
  - Removes the selected association of QCI-QoS-Mapping table from this APN.

- **qci_qos_map_table_name**
  - Specifies a preconfigured QCI-QoS-Mapping table from global configuration mode to this APN.
  - `qci_qos_map_table_name` must be an existing QCI-QoS-mapping table expressed as a string of 1 through 63 characters.
  - QCI-QoS-Mapping tables are configured in QCI-QoS_Mapping Configuration mode.

**Usage**

Use this command to associate a preconfigured QCI-QoS-Mapping table with an APN to provide per APN basis DSCP marking.

The GGSN/PGW supports configurable DSCP marking of the outer header of a GTP-U tunnel packet based on a QCI/THP table for the Gn/Gp and S5/S8 interfaces. This feature allows configuring DSCP marking table on a per APN basis.

**Important:** In order to be backward compatible with old configuration, if a DSCP marking table is associated with GGSN service and not with the APN, then the one in GGSN service will be used. If table is associated in both GGSN service and APN, then the one on APN will take precedence.

**Example**

The following command associates a preconfigured QCI-QoS-Mapping table `dscp_mark_table1` with this APN.

```
associate qci-qos-mapping dscp_mark_table1
```
authentication

Configures the APN’s authentication parameters.

Product
- GGSN
- P-GW
- PDG/TTG
- SAEGW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > APN Configuration
```
configure > context context_name > apn apn_name
```

Entering the above command sequence results in the following prompt:
```
[context_name]host_name(config-apn)#
```

Syntax

```
```

default authentication

**default**

Sets the default authentication type for this APN. By default **allow-noauth** is the type for authentication for an APN.

**msid-auth**

Obsolete. Use **imsi-auth**.

**imsi-auth**

Default: Disabled.
Configures the APN to attempt to authenticate the subscriber based on their International Mobile Subscriber Identification (IMSI) number.

**msisdn-auth**

Default: Disabled.
Configures the APN to attempt to authenticate the subscriber based on their Mobile Station International Integrated Services Digital Network (MSISDN) number as described in the *Usage* section of this command.
<table>
<thead>
<tr>
<th>Command</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>username-strip-apn</td>
<td>Disabled</td>
<td>This keyword if enabled, either with <strong>msisd-auth</strong> or <strong>imsi-auth</strong> strips the APN name from the user name <strong>msisd-apn</strong> or <strong>imsi@apn</strong> received from AAA and makes the user name as <strong>msisd</strong> or <strong>imsi</strong> respectively.</td>
</tr>
<tr>
<td>username-append-apn</td>
<td>Disabled</td>
<td>This keyword if enabled, works only with pap and chap options. If username-append-apn option enabled in authentication CLI, then apn name will be appended to the pco received username and same username will be used across all interfaces.</td>
</tr>
<tr>
<td>password-use-pco</td>
<td>Disabled</td>
<td>This keyword, if enabled, uses the password received through Protocol Configuration Options (PCO) from AAA for authentication.</td>
</tr>
<tr>
<td>prefer-chap-pco</td>
<td>Disabled</td>
<td>If this keyword along with msisd-auth/imsi-auth is enabled, GGSN performs Challenge Handshake Authentication Protocol (CHAP) authentication, if CHAP parameters are received in Protocol Configuration Options (PCO). If CHAP parameters are not received in the PCO IE of the CPC Request, GGSN does normal Password Authentication Protocol (PAP) authentication with PAP username as <strong>msisd-apn</strong> or <strong>imsi@apn</strong> (ignoring any PAP username if received).</td>
</tr>
<tr>
<td>eap initial-access-request</td>
<td>Enabled</td>
<td>Configures the type of initial access request to be used in Diameter EAP (Extensible Authentication Protocol) request. This feature is applicable to only Diameter-based AAA interface and not applicable to RADIUS or any other type of AAA interface.</td>
</tr>
<tr>
<td>authenticate-authorize</td>
<td>Enabled</td>
<td>Configures the “authenticate and authorize” type of initial access request to be used in a Diameter EAP request.</td>
</tr>
<tr>
<td>authenticate-only</td>
<td>Disabled</td>
<td>Configures the “authenticate only” type of initial access request to be used in a Diameter EAP request.</td>
</tr>
<tr>
<td>allow-noauth</td>
<td>Enabled</td>
<td>Configures the APN to not perform authentication for PDP contexts as described in the <em>Usage</em> section.</td>
</tr>
<tr>
<td>pco-username</td>
<td>Disabled</td>
<td></td>
</tr>
</tbody>
</table>
This option is used in conjunction with allow-noauth. It allows session to get established when PCO contains both pap and chap in authentication disabled case.

<table>
<thead>
<tr>
<th>Command</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>chap preference</strong></td>
<td>Disabled</td>
<td>Configures the APN to attempt to use CHAP to authenticate the subscriber as described in the Usage section of this command. A preference must be specified in conjunction with this option. Priorities specify which authentication protocol should be attempted first, second, third and so on. It must be an integer from 1 through 1000. The lower the integer, the higher the preference.</td>
</tr>
<tr>
<td><strong>convert-to-mschap</strong></td>
<td>Disabled</td>
<td>If enabled, the CHAP parameters received with the length of 49 bytes, the AAAmgr converts it to MSCHAP.</td>
</tr>
<tr>
<td><strong>mschap preference</strong></td>
<td>Disabled</td>
<td>Configures the APN to attempt to use the Microsoft Challenge Handshake Authentication Protocol (MSCHAP) to authenticate the subscriber as described in the Usage section of this command. A preference can be specified in conjunction with this option. Priorities specify which authentication protocol should be attempted first, second, third and so on. It must be an integer from 1 through 1000. The lower the integer, the higher the preference.</td>
</tr>
<tr>
<td><strong>pap preference</strong></td>
<td>Disabled</td>
<td>Configures the APN to attempt to use PAP to authenticate the subscriber as described in the Usage section of this command. A preference must be specified in conjunction with this option. Priorities specify which authentication protocol should be attempted first, second, third and so on. It must be an integer from 1 through 1000. The lower the integer, the higher the preference.</td>
</tr>
</tbody>
</table>

**Usage**

Use this command to specify how the APN profile should handle PDP context authentication and what protocols to use (if any). The ability to configure this option is provided to accommodate the fact that not every MS will implement the same authentication protocols. The authentication process varies depending on whether the PDP context is of type IP or PPP. Table given in this section describes these differences. For IP PDP contexts, the authentication protocol and values will be passed from the SGSN as Protocol Configuration Options (PCOs) within the create PDP context PDU to the GGSN. The GGSN requires that the authentication protocol is specified by this command (with no regard to priority) and will use this information to authenticate the subscriber.

**Table 14. Authentication Process Variances Between PDP Context Type**

<table>
<thead>
<tr>
<th>Authentication Mechanism</th>
<th>IP PDP Context Behavior</th>
<th>PPP PDP Context Behavior</th>
</tr>
</thead>
</table>
### Authentication Mechanism

<table>
<thead>
<tr>
<th>Mechanism</th>
<th>IP PDP Context Behavior</th>
<th>PPP PDP Context Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>allow-noauth</strong></td>
<td>Allows the session even if the PCOs do not match any of the configured algorithms. If there was no match and the <code>aaa constructed-nai authentication</code> parameter is enabled in the authentication context, the system attempts to determine a subscriber profile (via PAP with no password) using the subscriber’s MSISDN as the username.</td>
<td>Allows the session with no authentication algorithm selected. If the <code>aaa constructed-nai authentication</code> parameter is enabled in the authentication context, the system attempts to determine a subscriber profile (via PAP with no password) using the subscriber’s MSISDN as the username.</td>
</tr>
<tr>
<td><strong>chap</strong></td>
<td>If also specified in the PCOs, this protocol will be used to authenticate the subscriber.</td>
<td>Attempts this protocol according to its configured priority. If accepted by the remote end of the PPP connection, this protocol will be used to provide authentication.</td>
</tr>
<tr>
<td><strong>mschap</strong></td>
<td>If also specified in the PCOs, this protocol will be used to authenticate the subscriber.</td>
<td>Attempts this protocol according to its configured priority. If accepted by the remote end of the PPP connection, this protocol will be used to provide authentication.</td>
</tr>
<tr>
<td><strong>pap</strong></td>
<td>If also specified in the PCOs, this protocol will be used to authenticate the subscriber. If this protocol is used is specified and the <code>allow-noauth</code> parameter is disabled, the system will attempt to use the APN’s default username/password specified by the <code>outbound</code> command for authentication via PAP.</td>
<td>Attempts this protocol according to its configured priority. If accepted by the remote end of the PPP connection, this protocol will be used to provide authentication.</td>
</tr>
<tr>
<td><strong>msid-auth</strong></td>
<td>Values in the PCOs are ignored. The subscriber’s IMSI is used as the username for PAP authentication. No password is used.</td>
<td>Obsolete. Use <code>imsi-auth</code>.</td>
</tr>
<tr>
<td><strong>imsi-auth</strong></td>
<td>Values in the PCOs are ignored. The subscriber’s IMSI is used as the username for PAP authentication. No password is used.</td>
<td>Obsolete. Use <code>imsi-auth</code>.</td>
</tr>
<tr>
<td><strong>msisd-auth</strong></td>
<td>Values in the PCOs are ignored. The subscriber’s MSISDN is used as the username for PAP authentication. No password is used.</td>
<td>Option not available.</td>
</tr>
</tbody>
</table>

### Example

The following command would configure the system to attempt subscriber authentication first using MSCHAP, then CHAP, and finally PAP. Since the `allow-noauth` command was also issued, if all attempts to authenticate the subscriber using these protocols fail, then the subscriber would still be allowed access.

```
authentication mschap 1 chap 2 pap 3 allow-noauth
```

To enable `imsi-auth` or `msisd-auth`, the following command instances must be issued:

```
authentication imsi-auth

authentication msisd-auth
```

---

**Cisco ASR 5x00 Command Line Interface Reference**

1251
authorize-with-hss

This command enables or disables subscriber session authorization per APN via a Home Subscriber Server (HSS) over an S6b Diameter interface. This feature is required to support the interworking of GGSN with P-GW and HA.

**Product**
- P-GW
- SAEGW

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > APN Configuration

```
configure > context context_name > apn apn_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-apn)>
```

**Syntax**

```
authorize-with-hss [ egtp | lma [ s6b-aaa-group aaa-group-name | report-ipv6-addr ] ]
```

```
{ default | no } authorize-with-hss
```

- **default | no**
  Disables the default authorization of subscriber over S6b interface. Resets the command to the default setting of “authorize locally” from an internal APN authorization configuration.

- **egtp**
  Enables S6b authorization for eGTP only.

- **lma [ s6b-aaa-group aaa-group-name ]**
  Enables S6b authorization for LMA only.
  The keyword `s6b-aaa-group aaa-group-name` is used to enable the configuration of AAA group used for S6b authorization in PMIP P-GW.
  Two AAA groups are defined within APN configuration, one for RADIUS and another one for Diameter. All the parameters required for RADIUS authentication and accounting will go under `radius_group`. Similarly, Diameter authentication parameters will go under `s6b_group`.

- **Important:** If the S6b AAA group is configured under both APN and P-GW service, the APN level configuration takes higher precedence.

- **report-ipv6-addr**
  Enables the IPv6 address reporting through Authorization-Authentication-Request (AAR) towards the S6b interface.
Usage

Use this command to enable/disable the authorization support per APN for subscriber over S6b interface, which is used between P-GW and the 3GPP AAA to exchange the information related to charging, GGSN discovery, etc.
**bearer-control-mode**

Enables or disables the bearer control mode for network controlled QoS (NCQoS) through this APN. It also controls the sending of an IE in GTP messages.

**Product**
- GGSN
- P-GW
- SAEGW

**Privilege**
- Security Administrator, Administrator

**Mode**
EXEC > Global Configuration > Context Configuration > APN Configuration

```bash
configure > context context_name > apn apn_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-apn)#
```

**Syntax**

```bash
bearer-control-mode [ mixed | ms-only | none [ prefer-local-value ] ]
```

**default bearer-control-mode**

```bash
default
```

Sets the bearer control mode to default mode of “none”.

```bash
mixed
```

Default: Disabled.
This keyword indicates that the bearer will be controlled by User Equipment (UE) and network side (from GGSN) as well.
To enable network controlled QoS this option must be enabled.

```bash
ms-only
```

Default: Disabled.
This keyword indicates that the bearer will be controlled by the UE side.

```bash
none
```

Default: Enabled.
This keyword indicates that the system will not send any BCM mode information, BCM IE and BCM information in the protocol configuration option (PCO) IE within GTPC messages sent by the GGSN. This option is useful in networks where AGWs or firewalls do not support unknown optional IEs in GTP messages.

```bash
prefer-local-value
```

Default: Disabled.
This keyword indicates that the APN configured with “none” option for bearer control mode will not be overridden by any other interface (e.g. Gx interface towards PCRF). As a result it is ensured that BCM IE is never sent in GTP message.

**Important:** When bearer control mode is set to “none” with the keyword set “prefer-local-value”, even PCRF provided values will not override APN config and therefore sending of BCM mode IE and BCM in PCO IE in CPC Response is supressed.

**Usage**

Use this command to enable the QoS through bearer control. This can be done either through the MS side or from both the GGSN and MS. To enable network requested QoS user need to enable “Mixed” mode for bearer control.

With this keyword the operator can control sending of BCM information in GTPC messages from the GGSN. With MS-Only or Mixed options in this mode, the system sends the BCM information element in every Create PDP Context Response and Unknown PDP Context Request and Response message. In some networks AGWs/Firewall drop/reject GTPC messages if there is an Unknown optional IE. To resolve this, the operator can use the “none” option to control sending of BCM IE and BCM information in the PCO IE within GTPC messages from the GGSN.

**Example**

The following command enables the bearer control from network and MS side for NCQoS.

```
bearer-control-mode mixed
```
**cc-home**

Configures the home subscriber charging characteristics (CC) used by the GGSN when those from the SGSN will not be accepted.

**Product**

GGSN  
P-GW  
SAEGW

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > APN Configuration

```bash
configure > context context_name > apn apn_name
```

Entering the above command sequence results in the following prompt:

```bash
[context_name]host_name(config-apn)#
```

**Syntax**

```bash
cc-home { behavior bits | profile index }
```

default cc-home

- **default**
  
  Restores the cc-home parameter to its default setting of the following:
  
  - **behavior bits**: 0x00
  - **profile index**: 8

- **behavior bits**
  
  Specifies the behavior bit for the home subscriber charging characteristic. `bits` can be configured to any unique bit from 001H to FFFH (0001 to 1111 1111 1111 bin) where the least-significant bit corresponds to B1 and the most-significant bit corresponds to B12.

- **profile index**
  
  Specifies the profile index for the home subscriber charging characteristic. `index` can be configured to any integer value between 0 and 15. Default: 8

**Important:** 3GPP standards suggest that profile index values of 1, 2, 4, and 8 be used for hot billing, flat rate billing, prepaid billing and normal billing, respectively. A single charging characteristics profile can contain multiple behavior settings.

**Usage**

When the GGSN is configured to reject the charging characteristics sent by the SGSN for “home” subscribers, it uses the profile index specified by this command to determine the appropriate CCs to use.
Multiple behavior bits can be configured for a single profile index by ORing the bit strings together and converting the result to hexadecimal. The properties of the actual CC profile index are configured as part of the GGSN service using the `cc` `profile` command. Refer to the `GGSN Service Configuration Mode` chapter of this reference for additional information on this command.

**Example**

The following command configures a behavior bit of 2 (0000 0000 0010) and a profile in dex of 10 for home subscribers charging characteristics:

```
cc-home behavior 2 profile 10
```

The following command configures the behavior bits 3 (0000 0000 0100) and 5 (0000 0001 0000 bin) and a profile index of 14 for home subscriber charging characteristics:

```
cc-home behavior 14 profile 14
```
**cc-roaming**

Configures the roaming subscriber charging characteristics (CC) used by the GGSN when those from the SGSN will not be accepted.

**Product**
- GGSN
- P-GW
- SAEGW

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration > Context Configuration > APN Configuration
- `configure > context context_name > apn apn_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-apn)#
```

**Syntax**

```
cc-roaming { behavior bits | profile index }  
default cc-roaming
```

**default cc-roaming**

- `default`
  Restores the cc-roaming parameter to its default setting of the following:
  - **behavior bits**: 0x00
  - **profile index**: 8

**behavior bits**

Specifies the behavior bit for the roaming subscriber charging characteristic. `bits` can be configured to any unique bit from 001H to FFFH (0001 to 1111 1111 1111 bin) where the least-significant bit corresponds to B1 and the most-significant bit corresponds to B12.

**profile index**

Specifies the profile index for the roaming subscriber charging characteristic. `index` can be configured to any integer value between 0 and 15. Default: 8

**Important:** 3GPP standards suggest that profile index values of 1, 2, 4, and 8 be used for hot billing, flat rate billing, prepaid billing and normal billing, respectively. A single charging characteristics profile can contain multiple behavior settings.

**Usage**

When the GGSN is configured to reject the charging characteristics sent by the SGSN for “roaming” subscribers, it uses the profile index specified by this command to determine the appropriate CCs to use.
Multiple behavior bits can be configured for a single profile index by ORing the bit strings together and convert the result to hexadecimal.

The properties of the actual CC profile index are configured as part of the GGSN service using the `cc profile` command. Refer to the GGSN Service Configuration Mode chapter of this reference for additional information on this command.

**Example**

The following command configures a behavior bit 10 (0010 0000 0000) and a profile index of 10 for roaming subscriber charging characteristics:

```
cc-roaming behavior 200 profile 10
```

The following command configures the behavior bits 9 (0001 0000 0000) and 6 (0000 0010 0000) and a profile index of 14 for roaming subscriber charging characteristics:

```
cc-roaming behavior 120 profile 14
```
**cc-sgsn**

Specifies the source for charging characteristics (CC) - those configured locally or those received from the SGSN.

**Product**
- GGSN
- P-GW
- SAEGW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > APN Configuration

`configure > context context_name > apn apn_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-apn)#
```

**Syntax**

```
cce-sgsn { gx-returned | home-subscriber-use-GGSN | radius-returned | roaming-subscriber-use-GGSN | visiting-subscriber-use-GGSN } +

cce-sgsn { use-GGSN behavior bits profile index[ 0...15 ] | radius-returned { accept-invalid | replace-invalid } | gx-returned { accept-invalid | replace-invalid } }

default cce-sgsn

no cce-sgsn { { radius-returned | home-subscriber-use-GGSN | roaming-subscriber-use-GGSN | visiting-subscriber-use-GGSN } + } | { use-GGSN } | { radius-returned { accept-invalid | replace-invalid } | gx-returned { accept-invalid | replace-invalid } }

default cce-sgsn
```

**Restores the cc-sgsn parameter to its default setting of the following:**
- **home-subscriber-use-GGSN**: Disabled
- **roaming-subscriber-use-GGSN**: Disabled
- **visiting-subscriber-use-GGSN**: Disabled

**no cc-sgsn**

Causes the GGSN/P-GW to accept CCs from the SGSN(s) when the **no cc-sgsn** command is entered with all applicable keywords. Otherwise, **no cc-sgsn** can be used to turn off one or more of the GGSN/P-GW sources of CC.

- **roaming-subscriber-use-GGSN**
- **home-subscriber-use-GGSN**
- **roaming-subscriber-use-GGSN**
- **visiting-subscriber-use-GGSN**
Before entering no cc-sgsn, it is helpful to determine which CC sources have been configured. This can be done with either show configuration or show apn name in Exec Mode.

**home-subscriber-use-GGSN**

Configures the GGSN/P-GW to use the locally defined charging characteristics for home subscribers, as configured with the APN Configuration Mode cc-home command.

**radiusreturned**

Configures the GGSN/P-GW to accept Gx returned charging characteristics for all subscribers for the APN.

**gxreturned**

Configures the GGSN/P-GW to accept charging characteristics returned from the RADIUS server for all subscribers for the APN.

**acceptinvalid**

Configures the GGSN/P-GW to accept charging characteristics returned from PCRF for all subscribers for the APN. It always accepts CC with profile index zero.

**replaceinvalid**

Configures GGSN/P-GW to accept charging characteristics returned from PCRF for all subscribers for the APN, except if CC profile index is zero, it will be replaced with default profile index. Default profile index is 8. This is the default behavior for gx-returned CC.

**roaming-subscriber-use-GGSN**

Configures the GGSN/P-GW to use the locally defined charging characteristics for roaming subscribers, as configured with the APN Configuration Mode cc-roaming command.

**use-GGSN [ behavior bits ] profile index [ 0 ... 15 ]**

Configures the GGSN/P-GW to accept charging characteristics for all subscribers in the APN. 

*bits* specifies the behavior bit for the charging characteristic. This variable can be configured to any unique bit from 001H to FFFH (0001 to 1111 1111 1111 bin) where the least-significant bit corresponds to B1 and the most-significant bit corresponds to B12.

*index* indicates which profile defined with cc profile in GGSN Service Configuration mode, the GGSN will use as a source for CCs. The index can be configured to an integer from 0 to 15. The use-GGSN keyword can be entered alone or in conjunction with the radiusreturned keyword. When entered, this keyword overrides the previous configuration using any of the home, roaming, and/or visiting keywords.

**visiting-subscriber-use-GGSN**

Configures the GGSN/P-GW to use the locally defined charging characteristics for visiting subscribers, as configured with the APN Configuration Mode cc-visiting command.

More than one of the above keywords can be entered within a single command.
**Usage**

This command specifies whether or not CCs received from the SGSN will be accepted. If they are not accepted, the GGSN/P-GW will use those that have been configured locally. The GGSN/P-GW’s behavior can be configured for the following subscriber types:

- **Home**: Subscribers belonging to the same Public Land Mobile Network (PLMN) as the one on which the GGSN/P-GW is located.

- **Roaming**: Subscribers that are serviced by a SGSN belonging to a different PLMN than the one on which the GGSN/P-GW is located.

- **Visiting**: Subscribers belonging to a different PLMN than the one on which the GGSN/P-GW is located.

- Any subscriber in the APN.

**Example**

The following command instructs the GGSN/P-GW to accept CCs for any subscriber in the APN based on local profile configurations of CCs.

```
cc-sgsn use-GGSN profile x
```

Assuming the CC source as defined with the previous command, the following command instructs the GGSN/P-GW to accept CCs supplied by the SGSN(s) and disables the acceptance of CCs supplied by the GGSN/P-GW for any subscriber within the APN:

```
no cc-sgsn use-GGSN
```

The following command instructs the GGSN/P-GW to accept CCs for any subscriber in the APN based on CC information returned from the RADIUS server. This command can be issued after the previous command to expand the possible sources.

```
cc-sgsn radius-returned
```

The following command disables the acceptance of CCs supplied by the GGSN/P-GW for visiting and roaming subscribers:

```
no cc-sgsn roaming-subscriber-use-GGSN visiting-subscriber-use-GGSN
```
cc-visiting

Configures the visiting subscriber charging characteristics (CC) used by the GGSN when those from the SGSN will not be accepted.

**Product**

GGSN
P-GW
SAEGW

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > APN Configuration

```
configure > context context_name > apn apn_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-apn)#
```

**Syntax**

```
cc-visiting behavior bits profile index

default cc-visiting
```

**Default cc-visiting**

Restores the cc-visiting parameter to its default setting of the following:

- **behavior bits**: 0x00
- **profile index**: 8

**behavior bits**

Specifies the behavior bit for the visiting subscriber charging characteristic. **bits** can be configured to any unique bit from 001H to FFFH (0001 to 1111 1111 1111 bin) where the least-significant bit corresponds to B1 and the most-significant bit corresponds to B12.

**profile index**

Specifies the profile index for the visiting subscriber charging characteristic. **index** can be configured to any integer value between 0 and 15. Default: 8

**Important**: 3GPP standards suggest that profile index values of 1, 2, 4, and 8 be used for hot billing, flat rate billing, prepaid billing and normal billing, respectively. A single charging characteristics profile can contain multiple behavior settings.

**Usage**

When the GGSN is configured to reject the charging characteristics sent by the SGSN for “visiting” subscribers, it uses the profile index specified by this command to determine the appropriate CCs to use.
Multiple behavior bits can be configured for a single profile index by ORing the bit strings together and convert the result to hexadecimal. The properties of the actual CC profile index are configured as part of the GGSN service using the cc profile command. Refer to the GGSN Service Configuration Mode chapter of this reference for additional information on this command.

Example

The following command configures a behavior bit 7 (0000 0100 0000) and a profile index of 10 for visiting subscriber charging characteristics:

```
cc-visiting behavior 40 profile 10
```

The following command configures the behavior bits 1 (0000 0000 0001) and 12 (1000 0000 0000) and a profile index of 14 for visiting subscriber charging characteristics:

```
cc-visiting behavior 801 profile 14
```
content-filtering category

Enables or disables the specified pre-configured Category Policy Identifier for Category-based Content Filtering support.

Product
CF

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > APN Configuration

configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-apn)#

Syntax

content-filtering category policy-id cf_policy_id

no content-filtering category policy-id

no

Disables the previously configured category policy identifier for Content Filtering support to the APN. This is the default setting.

policy-id cf_policy_id

Applies the specified content filtering category policy ID, configured in the ACS Configuration Mode, to this APN.

cf_policy_id must be a category policy ID entered as an integer from 1 through 4294967295.
If the specified category policy ID is not configured in the ACS Configuration Mode, all packets will be passed regardless of the categories determined for such packets.

Important: Category Policy ID configured through this mode overrides the Category Policy ID configured through content-filtering category policy-id command in the ACS Rulebase Configuration Mode.

Usage

Use this command to enter the Content Filtering Policy Configuration Mode and to enable or disable the Content Filtering Category Policy ID for an APN.

Important: If Content Filtering Category Policy ID is not specified here the similar command in the ACS Rulebase Configuration Mode determines the policy.

Example

Up to 64 different policy IDs can be defined.
The following command enters the Content Filtering Policy Configuration Mode and enables the Category Policy ID 101 for Content Filtering support:

```
content-filtering category policy-id 101
```
credit-control-client

Configures the credit-control client parameters for subscribers who use this APN.

Product
- GGSN
- HA
- IPSG
- PDSN
- P-GW

Privilege
- Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > APN Configuration
configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-apn)#

Syntax

credit-control-client { event-based-charging | override session-mode { per-sub-session | per-subscriber } }

no credit-control-client { event-based-charging | override session-mode }

default credit-control-client event-based-charging

---

no
Disables the configured setting.

---

default
Resets the command to its default setting of disabled.

---

event-based-charging
Enables event-based charging.

---

override session-mode { per-sub-session | per-subscriber }

Overrides the session-mode configured through the CLI command “require ecs credit-control session-mode per-subscriber” in Global Configuration mode so that different APN can operate in different modes. For example, one APN can be configured to work in per-subscriber mode, while another in per-sub-session mode.
This keyword is used to switch between subscriber level Gy and sub-session level Gy.
**Important:** This CLI can be changed on the fly. The modified values will be reflected only in the new subscriber session.

The `no` command removes the override CLI and makes the APN fall back to the configuration specified through the CLI command “`require ecs credit-control session-mode per-subscriber`”.

**Usage**

Use this command to configure the credit-control client parameters for this APN. This configuration should be enabled to report UE’s PLMN, timezone and ULI changes through Event-based-Gy session. In the event that both Gy Online charging and Gy event reporting are enabled, the P-GW shall send only CCR-Update requests to the OCS and shall not send CCR-Event requests. With the inclusion of this keyword `override session-mode` ... in 14.1 release, it is possible to seamlessly change the configuration from bearer level to APN level and vice-versa without requiring a system reboot.

**Example**

The following command enables event-based Gy support for the current APN:

```
credit-control-client event-based-charging
```
credit-control-group

Configures the credit control group to be used for subscribers who use this APN.

**Product**
- GGSN
- ACS
- P-GW
- SAEGW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > APN Configuration

```bash
configure > context context_name > apn apn_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-apn)#
```

**Syntax**

```bash
credit-control-group cc_group_name

no credit-control-group
```

**Usage**

Use this command to configure the credit control group for this APN.
Creating different credit control groups enables applying different credit control configurations (DCCA dictionary, failure-handling, session-failover, Diameter endpoint selection, etc.) to different subscribers on the same system.
Without credit control groups, only one credit control configuration is possible on a system. All the subscribers in the system will have to use the same configuration.

**Example**

The following command configures a credit control group named `testgroup12` for the current APN:

```bash
credit-control-group testgroup12
```
**daf-pdp-type**

By configuring this command P-GW/GGSN can set different behavior of assigning PDN Type and return cause code when request for ipv4v6 PDN with DAF bit False is received.

**Product**
GGSN
P-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > APN Configuration
`configure > context context_name > apn apn_name`
Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-apn)#
```

**Syntax**

```
daf-pdp-type { ipv4 | ipv6 } cause-code { network-preference | single-address-bearer-only }
```

**daf-pdp-type**

Configures PDP type for requested IPv4v6 PDN with Dual Address Flag zero. Default PDP type is IPv6.

**ipv4**

Configures PDP type for this APN to be IPv4.

**ipv6**

Configures PDP type for this APN to be IPv6

**ipv6**

Configures PDP type for this APN to be IPv6.

**cause-code**

Configures GTP cause code for requested IPv4v6 PDN with Dual Address Flag zero. Default GTP cause code is single-address-bearer-only.

**network-preference**

New PDP type due to network preference.

**single-address-bearer-only**

New PDP type due to single address bearer only.
Usage

By configuring this command P-GW/GGSN can set different behavior of assigning PDN Type and return cause code when request for ipv4v6 PDN with DAF bit False is received. If this command is not configured P-GW/GGSN it uses the default option of assigning ipv6 pdn type with return cause of ‘New PDN Type due to single address bearer only’.

Example

The following command configures PDP type and GTP cause code for requested IPv4v6 PDN due to network preference.

\[ \text{daf-pdp-type ipv4 cause-code network-preference} \]
data-tunnel mtu

Configures the Maximum Transmission Unit (MTU) for data sent on the IPv6 tunnel between the P-GW and the mobile node.

**Product**
P-GW
SAEGW

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > APN Configuration

```
configure > context context_name > apn apn_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-apn)#
```

**Syntax**

```
data-tunnel mtu
```

**default**

```
data-tunnel mtu
```

**default**

```
data-tunnel mtu
```

Returns the command to the default value of 1500.

```
data-tunnel mtu
```

**bytes**

```
data-tunnel mtu
```

Specifies the MTU for the IPv6 tunnel between the P-GW and the mobile node. `bytes` must be an integer between 1280 and 2000. Default: 1500

**Usage**

Use this command to set the MTU for data traffic on the IPv6 tunnel between the P-GW and the mobile node.

**Example**

The following command sets the MTU for IPv6 data traffic to 1400 bytes:

```
data-tunnel mtu 1400
```
data-tunneling ignore df-bit

Controls the handling of the DF (Don't Fragment) bit present in the user IPv4/IPv6 packet for tunneling used for the Mobile IP data path.

Product
GGSN
P-GW
SAEGW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > APN Configuration

configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-apn)#

Syntax

[ default | no ] data-tunneling ignore df-bit

- default
  Restores the data-tunneling parameter to its default setting of disabled.

- no
  Disables this option. The DF bit in the tunneled IP packet header is not ignored during tunneling. This is the default setting.

- ignore df-bit
  Ignores the DF bit in the tunneled IP packet header during tunneling. This is the default setting.

Usage

Use this command to configure a user so that during Mobile IP tunneling the DF bit is ignored and packets are fragmented.

If this feature is enabled, and fragmentation is required for the tunneled user IPv4/IPv6 packet, then the DF bit is ignored and the packet is fragmented. Also the DF bit is not copied to the outer header.

In the GGSN, this command also affects the other L3 tunneling options, IP-in-IP and GRE, but does not affect L2TP tunneling.

Example

To enable fragmentation of a subscriber's packets over a MIP tunnel even when the DF bit is present, enter the following command:

data-tunneling ignore df-bit
dcca origin endpoint

This command is obsolete. To configure the Diameter Credit Control Origin Endpoint, in the Credit Control Configuration Mode, use the `diameter origin endpoint` command.
**dcca peer-select**

Specifies the Diameter credit control primary and secondary host for credit control.

**Product**
- GGSN
- ACS
- P-GW
- SAEGW

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration > Context Configuration > APN Configuration
  - `configure > context context_name > apn apn_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-apn)#
```

**Syntax**

```
dcca peer-select peer host_name [ realm realm_name ] [ secondary-peer host_name ]
no dcca peer-select
```

**Usage**

Use this command to select a Diameter credit control peer and realm.

**Syntax**

```dcca peer-select peer host_name [ realm realm_name ] [ secondary-peer host_name ]
no dcca peer-select```

**no**

Removes the previously configured Diameter credit control peer selection.

**host_name**

Specifies a unique name for the peer as an alphanumeric string of 1 through 63 characters that allows punctuation marks.

**realm realm_name**

Specifies the realm as an alphanumeric string of from 1 through 127 characters that allows punctuation marks. The realm may typically be a company or service name.

**secondary-peer host_name**

Specifies a back-up host that is used for fail-over processing as an alphanumeric string of from 1 through 63 characters. When the route-table does not find an AVAILABLE route, the secondary host performs fail-over processing.
Caution: This configuration completely overrides all instances of diameter peer-select that have been configured within the Credit Control Configuration Mode for an Active Charging Service.

Example

The following command selects a Diameter credit control peer named test and a realm of companyx:

```bash
dcca peer-select test realm companyx
```
**dhcp context-name**

Configures the name of the context on the system in which Dynamic Host Control Protocol (DHCP) functionality is configured.

**Product**
- GGSN
- P-GW
- SAEGW

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration > Context Configuration > APN Configuration

```bash
configure > context context_name > apn apn_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-apn)#
```

**Syntax**

```
[ no ] dhcp context-name name
```

- **no**
  - Removes a previously configured context name.

- **name**
  - Specifies the name of a context configured on the system in which one or more DHCP services are configured. `name` is an alphanumeric string of 1 through 79 characters that is case sensitive.

**Usage**

If the APN is to support dynamic address assignment via DHCP (either the proxy or relay mode), this parameter must be configured to point the APN to the name of a pre-configured context on the chassis in which one or more DHCP services are configured.

The `configure` command can be used to identify a single DHCP service instance within the specified context to use to facilitate the address assignment.

**Example**

The following command configures the APN to look for DHCP services in a context called `dhcp-ctx`:

```
dhcp context-name dhcp-ctx
```
dhcp lease-expiration-policy

Configures the system’s handling of PDP contexts whose DHCP assigned IP lease has expired.

Product

GGSN
P-GW
SAEGW

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > Context Configuration > APN Configuration
configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-apn)#

Syntax

dhcp lease-expiration-policy { auto-renew | disconnect }
default dhcp lease-expiration-policy

default
Restores the dhcp lease-expiration-policy parameter to its default setting of auto-renew.

auto-renew
Configures the system to automatically renew an IP address’ lease when it is about to expire for PDP contexts facilitated by the APN. Default: Enabled

disconnect
Configures the system to automatically release the PDP context when the lease for the IP address associated with that context expires. Default: Disabled

Usage

Use this command to specify the action the system is to take when leases for IP addresses for PDP contexts that it are currently facilitated by the current APN are about to expire.

Example

The following command causes the system to release PDP contexts associated with the current APN when the lease for their DHCP-assigned IP address expires:

dhcp lease-expiration-policy disconnect
dhcp service-name

Configures the name of a specific DHCP service to use when dynamically assigning IP addresses to PDP contexts using the Dynamic Host Control Protocol.

**Product**
- GGSN
- P-GW
- SAEGW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > APN Configuration

`configure > context context_name > apn apn_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-apn)#
```

**Syntax**

```
[ no ] dhcp service-name service_name
```

- **no**
  - Removes a previously configured DHCP service name.

- **service_name**
  - Configures the name of the DHCP service instance that is to be used by the current APN for the dynamic assignment of IP addresses to PDP contexts. The name can be an alphanumeric string of 1 through 63 characters that is case sensitive.

**Usage**

Use this command to specify a pre-configured DHCP service instance that is to be used by the APN for IP address assignment when the Dynamic Host Control Protocol is used.

The name of the context in which the desired DHCP service is configured must be specified by the `dhcp context-name` command.

**Example**

The following command instructs the APN to use a DHCP service called `dhcp1`:

```
dhcp service-name dhcp1
```
dhcpv6 context-name

Configures the name of the context on the system in which DHCPv6 functionality is configured. If a DHCPv6 service is configured in the APN, this DHCPv6 context name is used to get an address.

**Product**
GGSN
P-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > APN Configuration

```bash
configure > context context_name > apn apn_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-apn)#
```

**Syntax**

```
dhcpv6 context-name context_name
```

[ no ] dhcp context-name

```
no
```

Removes a previously configured context name.

```
context_name
```

Specifies the name of a context configured on the system in which one or more DHCPv6 services are configured. `context_name` is an alphanumeric string of 1 through 79 characters that is case sensitive.

**Usage**

If the APN is to support dynamic address assignment via DHCPv6, this parameter must be configured to point the APN to the name of a pre-configured context on the chassis in which one or more DHCPv6 services are configured.

The command can be used to identify a single DHCPv6 service instance within the specified context to use to facilitate the address assignment.

**Example**

The following command configures the APN to look for DHCPv6 services in a context called `dhcpv6-ctx`:

```
dhcpv6 context-name dhcpv6-ctx
```
**dhcpv6 service-name**

Specifies which DHCPV6 service to use, if the alloc-type is configured as dhcpv6-client or dhcpv6-relay.

**Product**
GGSN
P-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > APN Configuration
configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

```
/context_name]host_name(config-apn)#
```

**Syntax**

```
[ no ] dhcpv6 service-name service_name
```

- **no**
  
  Removes a previously configured DHCPv6 service name.

- **service_name**

  Configures the name of the DHCPv6 service instance that is to be used by the current APN for the dynamic assignment of IPv6 addresses to PDP contexts. The name can be an alphanumeric string of 1 through 63 characters that is case sensitive.

**Usage**

Use this command to specify a pre-configured DHCPv6 service instance that is to be used by the APN for IPv6 address assignment when the Dynamic Host Control Protocol is used.

The name of the context in which the desired DHCP service is configured must be specified by the `dhcpv6 context-name` command.

**Important:** Only one DHCPv6 service can be configured for an APN

**Example**

The following command instructs the APN to use a DHCPv6 service called `dhcpv6_svc`:

```
dhcp service-name dhcpv6_svc
```
dns

Configures the Domain Name Service (DNS) servers that will be used by the APN for PPP.

Product
GGSN
P-GW
SAEGW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > APN Configuration

configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-apn)#

Syntax

dns { primary | secondary } { address }

no dns { primary | secondary } [ dns_address ]

no
Deletes a previously configured DNS server.

primary
Configures the primary DNS server for the APN.

secondary
Configures the secondary DNS server for the APN. Only one secondary DNS server can be configured.

address
Configures the IP address of the DNS server expressed in IPv4 dotted-decimal notation.
Default: primary = 0.0.0.0, secondary = 0.0.0.0

dns_address
Specifies the IP address of the DNS server to remove, expressed in IPv4 dotted-decimal notation.

Usage
DNS servers are configured on a per-APN profile basis. This allows each APN profile to use specific servers in processing PDP contexts.
The configured DNS IP addresses are relayed to the subscriber within IPCP if the PDP type is PPP, or as PCOs (Protocol Configuration Options) if the PDP type is IP.
The DNS can be specified at the APN level in APN configuration as well as at the Context level in Context configuration mode with `ip name-servers` command, or it can be received from AAA server. When DNS is requested in PCO configuration, the following preference will be followed for DNS value:

1. DNS Values received from LNS have the first preference.
2. DNS values received from RADIUS Server has the second preference.
3. DNS values locally configured with APN has the third preference.
4. DNS values configured at context level with `ip name-servers` command has the last preference.

**Important:** The same preference would be applicable for the NBNS (NetBIOS Name Service) servers to be negotiated via ICPC (Initial Connection Protocol Control) with the LNS (L2TP Network Server).

**Example**

The following commands configure a primary DNS server address of 192.168.100.3 and a secondary DNS server address of 192.168.100.4:

```bash
dns primary 192.168.100.3

dns secondary 192.168.100.4
```
**ehrpd-access**

Configures the P-GW to exclude IPv6 traffic from being delivered to UEs, accessing PDNs from the eHRPD network that do not have IPv6 capabilities.

**Product**
P-GW
SAEGW

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > APN Configuration
`configure > context context_name > apn apn_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-apn)#
```

**Syntax**

```
[ default | no ] ehrpd-access drop-ipv6-traffic
```

| [ default | no ] | ehrpd-access drop-ipv6-traffic |
|-----------------|--------------------------------|
| Resets this command to its default setting of disabled. |

**drop-ipv6-traffic**

Excludes IPv6 traffic from being delivered to UEs, accessing PDNs from the eHRPD network that do not have IPv6 capabilities.

**Usage**

Use this command to exclude IPv6 traffic from being delivered to UEs on the eHRPD network that do not have IPv6 capabilities.
emergency-apn

Configures this APN as an emergency APN for Voice over LTE (VoLTE) based E911 support.

Product
GGSN
P-GW
SAEGW

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > APN Configuration

configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-apn)#

Syntax

[ default | no ] emergency-apn

[ default | no ]

Resets this command to its default setting of disabled.

Usage

Use this command to configure this APN as an emergency APN for VoLTE based E911 support. With this support, a UE is able to connect to an emergency PDN and make Enhanced 911 (E911) calls while providing the required location information to the Public Safety Access Point (PSAP). E911 is a telecommunications-based system that is designed to link people who are experiencing an emergency with the public resources that can help. This feature supports E911-based calls across the LTE and IMS networks. In a voice over LTE scenario, the subscriber attaches to a dedicated packet data network (PDN) called EPDN (Emergency PDN) in order to establish a voice over IP connection to the PSAP. Both signaling and RTP media flow over a dedicated emergency bearer. Additionally, different than normal PDN attachment that relies on AAA and PCRF components for call establishment, the EPDN attributes are configured locally on the P-GW, which eliminates the potential for emergency call failure if either of these systems is not available.
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**
Use this command to return to the parent configuration mode.
firewall policy

Enables or disables Stateful Firewall support for the APN.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > APN Configuration

```
configure > context context_name > apn apn_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-apn)#
```

**Syntax**

```
firewall policy firewall
{ default | no } firewall policy
```

- **no**
  Disables Stateful Firewall support for this APN.

- **default**
  Configures the default setting for Stateful Firewall support.
  Default: Disabled

**Usage**

Use this command to enable or disable Stateful Firewall support for this APN.

**Important:** This command is only available in StarOS 8.0. In StarOS 8.1 and later, this configuration is available in the ACS Rulebase Configuration Mode.

**Important:** Unless Stateful Firewall support for this APN is enabled using this command, firewall processing for this APN is disabled.

**Important:** If firewall is enabled, and the rulebase has no firewall configuration, Stateful Firewall will cause all packets to be discarded.

**Example**

The following command enables Stateful Firewall support for an APN:

```
firewall policy firewall-required
```
The following command disables Stateful Firewall support for an APN:

```
no firewall policy
```
fw-and-nat policy

Specifies the Firewall-and-NAT policy to be used for subscribers who use this APN.

Product

eWAG
PSF
NAT

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > Context Configuration > APN Configuration
configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-apn)#

Syntax

fw-and-nat policy fw_nat_policy

{ default | no } fw-and-nat policy

default

Configures the default setting.
Default: The default Firewall-and-NAT policy configured in the rulebase is used for subscribers who use this APN.

no

Disables Firewall and NAT for the APN.

fw_nat_policy

Specifies the Firewall-and-NAT policy for the APN as an alphanumeric string of 1 through 63 characters. Note that this policy will override the default Firewall-and-NAT policy configured in the ACS rulebase.

Usage

Use this command to configure the Firewall-and-NAT policy for the APN. Note that the policy configured in the subscriber mode will override the default policy configured in the ACS rulebase. If a policy is not configured in the subscriber mode, the default policy configured in the ACS rulebase will be used.

Important: This command is customer-specific and is only available in StarOS 8.1.
**Important:** This customer-specific command must be used to configure the Policy-based Firewall-and-NAT feature.

**Example**

The following command configures a Firewall-and-NAT policy named `standard` for the APN:

```
fw-and-nat policy standard
```
**gsm-qos negotiate**

Enables negotiation of the QoS Reliability Class attribute based on the configuration provided for Service Data Unit (SDU) Error Ratio and Residual Bit Error Ratio (BER) attributes in the APN.

**Product**
- GGSN
- P-GW
- SAEGW

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration > Context Configuration > APN Configuration
- `configure > context context_name > apn apn_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-apn)#
```

**Syntax**

```
gsm-qos negotiate sdu-error-ratio sdu-error-ratio-code [ residual-ber residual-ber-code ]

```

- **no**
  - Disables negotiation of the QoS Reliability Class attribute.

- **sdu-error-ratio sdu-error-ratio-code**
  - Enables the negotiation of the QoS Reliability Class attribute based on Service Data Unit (SDU) Error Ratio attributes. `sdu-error-ratio-code` corresponds to distinct SDU Error ratio values within an integer range of 1 to 7.

- **residual-ber residual-ber-code**
  - Enables the optional configuration of negotiation of the QoS Reliability Class attribute based on Residual Bit Error Ratio (BER) attributes. `residual-ber-code` corresponds to distinct Residual Bit Error Ratio values within an integer range of 1 to 9.

**Usage**

This command configures the QoS attribute Reliability Class to be negotiated based on the configuration provided for SDU Error Ratio and Residual BER attributes. The derived Reliability Class and the configured values for SDU Error Ratio and Residual BER are sent back in CPC and UPC response. The mapping for `sdu-error-ratio-code` is as follows:

<table>
<thead>
<tr>
<th>Code</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>10-2</td>
</tr>
</tbody>
</table>
Residual BER needs to be specified when SDU Error Ratio is set to codes 1, 2, 3 or 7 (Or, SDU Error Ratio is intended to be set to a value greater than $5 \times 10^{-4}$), for determining the Reliability Class QoS attribute. Otherwise, the Residual BER value received in the Create PDP context request QoS (or UPC request) would be used. The mapping for `residual-ber-code` is as follows:

<table>
<thead>
<tr>
<th>Code</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$5 \times 10^{-2}$</td>
</tr>
<tr>
<td>2</td>
<td>$10^{-2}$</td>
</tr>
<tr>
<td>3</td>
<td>$5 \times 10^{-3}$</td>
</tr>
<tr>
<td>4</td>
<td>$4 \times 10^{-3}$</td>
</tr>
<tr>
<td>5</td>
<td>$10^{-3}$</td>
</tr>
<tr>
<td>6</td>
<td>$10^{-4}$</td>
</tr>
<tr>
<td>7</td>
<td>$10^{-5}$</td>
</tr>
<tr>
<td>8</td>
<td>$10^{-6}$</td>
</tr>
<tr>
<td>9</td>
<td>$6 \times 10^{-8}$</td>
</tr>
</tbody>
</table>

**Example**

The following commands configures the negotiation of QoS attribute Reliability Class based on Service Data Unit (SDU) Error Ratio 3 attributes in the APN:

```
gsm-qos negotiate sdu-error-ratio 3
```
**gtpp group**

Enables a configured GTPP server group to an APN for CGF accounting functionality.

---

**Important:** In releases prior to 11.0, only one GTPP group is allowed to be configured per APN. Releases 11.0 through 15.0, this CLI can be used to configure up to a maximum of 32 GTPP groups.

---

**Product**

- GGSN
- P-GW
- SAEGW

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > APN Configuration  
`configure > context context_name > apn apn_name`

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-apn)#`

**Syntax**

```
gtpp group  group_name [ accounting-context ac_context_name ]

default gtpp group

no gtpp group  group_name
```

`no`

Removes all the configured GTPP groups for the specific APN.

```
group_name
```

Specifies the name of server group that is used for authentication/accounting for specific APN. `group_name` must be an alphanumeric string of 1 to 63 characters. It must be identical to the one configured earlier within the same APN context.

---

**Important:** In Release 11.0 and later, if you have mistakenly configured a GTPP group, you should remove the initially configured group and configure the new desired group. However, in Releases prior to 11.0, there is no need to remove the incorrect configuration; instead you can directly reconfigure the desired GTPP group.

---

**Important:** If a GTPP group entry is invalid, this GTPP group will be ignored and the next valid GTPP group in the APN will be used. If no valid GTPP group exists, then the default GTPP group in the accounting context specified by the GGSN service will be used.
accounting-context ac_context_name

Specifies the name of an accounting context on the system that processes accounting for PDP contexts
handled by this GGSN service for accounting to specific APN.

ac_context_name must be an alphanumeric string of 1 through 79 characters that is case sensitive.
Note that if an accounting context is not specified here, the system uses the GGSN service context or the
context configured by the accounting context command in the GGSN Service Configuration mode.

Usage

This feature provides the GTPP server configurables under a GTPP group node. Instead of having a single list
of servers per context, this feature configures multiple server groups within a context and applies individual
an GTPP server group for subscribers in that context. Each server group consists of a list of CGF (Charging
Group Function) accounting servers.
In case no GTPP group is applied for the said APN or default APN template, then the default GTPP server
group available at the context level is applicable for accounting of a specific APN.

Important: When multiple GTPP groups are applied to the same APN, the load will be shared across these
GTPP groups. Sessions for this APN will use all the configured GTPP groups in a round robin fashion.

Once a GTPP group is selected for a subscriber session, the GTPP group will never change under any
circumstances. A request is initially sent to primary CGF server configured in that group. When the primary
fails to respond, the request is sent to secondary CGF server.
The process of failover from primary to secondary is per the 3GPP standards. Multiple GTPP groups
configuration is actually supported only for load sharing of sessions within an APN and not used for failover.
When all CGFs are down in a GTPP group, the requests are archived either in hard disk or main memory
depending on whether or not streaming is enabled.

Example

The following command applies a previously configured GTPP server group named star1 to an APN within
the specific context:

    gtppp group star1

The following command disables the applied GTPP server group for the specific APN:

    no gtppp group star1
gtpp secondary-group

Enables or associates a preconfigured secondary GTPP server group to an APN for CGF (Charging Group Function) accounting functionality. By default it is disabled.

Product
GGSN
P-GW
SAEGW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > APN Configuration

configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-apn)#

Syntax

```
gtpp secondary-group group_name [ accounting-context actt_ctxt_name ]
[ default | no ] gtpp secondary-group group_name
```

**default**
Default: Enabled
Restores the default mode for secondary GTPP group for APN template.

**no**
Disables the configured/associated GTPP secondary group for specific APN.

**group_name**
Specifies the name of secondary GTPP server group that is used as an alternate for the primary GTPP group associated with a specific APN for storage of GTPP messages. `group_name` must be an alphanumeric string of 1 through 63 characters. It must be the same name as configured earlier within the same APN context.

**accounting-context actt_ctxt_name**
Specifies the name of an accounting context on the system that processes accounting for PDP contexts handled by this GGSN service for accounting to a specific APN. `actt_ctxt_name` specifies the name of the context to be used for accounting as an alphanumeric string of 1 through 79 characters that is case sensitive. Note that if an accounting context is not specified here, the system uses the GGSN service context or the context configured by the `accounting context` command in the GGSN Service Configuration mode.

Usage
Use this feature to provide the secondary GTPP server group support for an APN.
When the secondary GTPP group is configured with this command, the GTPP messages will also be mirrored to the secondary servers. This secondary group configuration is ignored, if the configured group_name is the same as the primary group. It will also be ignored, if the configured GTPP group_name and/or accounting context ac_context_name is invalid. In such cases, the call will be established successfully (unlike the primary group configuration where the call drops). In the absence of a configured ac_context_name context, the GGSN service context is chosen by default. The secondary group messages are low priority and thus are purged when there is no room for the new messages.

For more information on GTPP group, refer the description of the gtpp group command.

**Example**

The following command applies a previously configured GTPP server group named star2 to as secondary GTPP group to an APN within the specific context:

```
gtpp secondary-group star2
```

The following command disables the applied secondary GTPP server group for the specific APN:

```
no gtpp secondary-group star2
```
idle-timeout-activity

Configures a session idle-timeout to be reset with uplink packets only, or with both uplink and downlink packets.

**Product**
GGSN
P-GW
SAEGW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > APN Configuration

```
configure > context context_name > apn apn_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-apn)#
```

**Syntax**

```
[ no ] idle-timeout-activity ignore-downlink

default idle-timeout-activity
```

- **default**
  Sets or restores the command to the default setting.

- **ignore-downlink**
  Sets the system to ignore the downlink traffic for consideration as activity for idle-timeout.

**Usage**

If `idle-timeout-activity ignore-downlink` is configured, the downlink (network to subscriber) traffic will not be used to reset the idle-timeout. Only uplink (subscriber to network) packets will be able to reset the idle-timeout.

By default, **ignore-downlink** is negated by the `no` command so downlink traffic is also used to reset the idle-timeout.

**Example**

The following command causes both uplink and downlink traffic to reset a session idle-timeout:

```
default idle-timeout-activity
```

The following command causes the session idle-timeout to be reset with only uplink packets:

```
idle-timeout-activity ignore-downlink
```
**ikev2 tsr**

Configures the Traffic Selector responder (TSr) negotiation behavior during IKEv2 Security Association (SA) establishment.

**Product**
PDG/TTG

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > APN Configuration

```
configure > context context_name > apn apn_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-apn)#
```

**Syntax**

```
[ default ] ikev2 tsr { wildcard | user-specified }
```

- **default**
  Specifies the default behavior, which is wildcard TSr negotiation.

- **wildcard**
  Specifies that during TSr negotiation, the PDG/TTG always returns an any-to-any IP address range, an any-to-any port range, and allows any protocol, irrespective of the traffic selector ranges received from the UE. This is the default behavior.

- **user-specified**
  Specifies that during TSr negotiation, the PDG/TTG responds to each UE request with the UE-specified IP address ranges. This enables split tunneling on the PDG/TTG, and enables the UE to tunnel only a specified traffic range to the PDG/TTG and send other traffic directly out the WLAN.

**Usage**

Use this command to specify the TSr negotiation behavior on the PDG/TTG.

**Example**

The following command enables user-specified TSr negotiation on the PDG/TTG:

```
ikev2 tsr user-specified
```
**ims-auth-service**

Applies an IMS (IP Multimedia Subsystem) authorization service to a subscriber through APN for Gx interface support and functionality.

**Product**
GGSN
P-GW
SAEGW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > APN Configuration
```
configure > context context_name > apn apn_name
```
Entering the above command sequence results in the following prompt:
```
[context_name] host_name(config-apn) #
```

**Syntax**
```
[ no ] ims-auth-service auth_service_name
```

- `no`
  Disables the applied IMS authorization service for a specific APN.

- `auth_service_name`
  Specifies the name of the IMS authorization service name that is used for Gx interface authentication for a specific APN. `auth_service_name` must be an alphanumeric string of 1 through 63 characters preconfigured within the same context as this APN.

**Usage**
This feature provides the IMS authorization service configuration for Gx interface in IMS service node.

**Example**
The following command applies a previously configured IMS authorization service named `gx_interface1` to an APN within the specific context:
```
ims-auth-service gx_interface1
```
The following command disables the applied IMS authorization service `gx_interface1` for the specific APN:
```
no ims-auth-service gx_interface1
```
**ip access-group**

Configures an IPv4/IPv6 access group for the current APN profile.

**Product**
- ACS
- eWAG
- GGSN
- P-GW
- SAEGW

**Privilege**
Security Administrator, Administrator

**Mode**
`Exec > Global Configuration > Context Configuration > APN Configuration`  
`configure > context context_name > apn apn_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-apn)#
```

**Syntax**

```
ip access-group acl_group_name [ in | out ] [ fallback-enabled ]

[ no ] ip access-group acl_group_name [ in | out ]
```

<table>
<thead>
<tr>
<th>no</th>
</tr>
</thead>
<tbody>
<tr>
<td>Removes a previously configured IPv4/IPv6 access group association.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>acl_group_name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the name of the IPv4/IPv6 access group. <code>acl_group_name</code> is a previously configured ACL group expressed as an alphanumeric string of 1 to 79 characters.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>in</th>
<th>out</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default: both (in and out)</td>
<td></td>
</tr>
<tr>
<td>Specifies the access-group as either inbound or outbound by the keywords <code>in</code> and <code>out</code>, respectively.</td>
<td></td>
</tr>
</tbody>
</table>

**Usage**

Use this command to apply a single IPv4/IPv6 access control list to multiple subscribers via this APN for inbound or outbound IPv4/IPv6 traffic.
If no traffic direction is specified, the selected access control list will be applied to both directions.

**Example**

The following command associates the `sampleipv4Group` access group with the current APN profile for both inbound and outbound access.

```
ip access-group sampleipv4Group
```
The following command removes the outbound access group flag for `sampleipv4Group`.

```
no ip access-group sampleipv4Group out
```
**ip address alloc-method**

Configures the method by which this APN will obtain IP addresses for PDP contexts.

**Product**

GGSN
P-GW
SAEGW

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > APN Configuration

```plaintext
configure > context context_name > apn apn_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-apn)#
```

**Syntax**

```plaintext
ip address alloc-method { dhcp-proxy [ allow-deferred ] [ prefer-dhcp-options ] | dhcp-relay | local [ allow-deferred ] | no-dynamic [ allow-deferred ] ) [ allow-user-specified ]
```

**default ip address allocation-method**

- **default**
  
  Restores the APN ip parameters to the following default settings.

- **dhcp-proxy**
  
  Default: Disabled
  
  Configures the APN to assign an IP address received from a DHCP server.

  **Important:** If this option is used, the system’s DHCP parameters must be configured.

- **dhcp-relay**
  
  Configures the APN to forward DHCP packets received from the MS to a DHCP server. Default: Disabled

  **Important:** If this option is used, the system’s DHCP parameters must be configured.

- **local**
  
  Configures the APN to allocate IP addresses from a pool configured in the destination context on the system. Default: Enabled
**Important:** If this option is used, the name of the IP address pool from which to allocate addresses must be configured using the `ip address pool-name` command. If no pool name is specified, the system will attempt to allocate an address from any public pool configured in the destination context.

**no-dynamic**
Disables the dynamic assignment of IP addresses to PDP contexts using this APN. Default: Disabled
If a PDP context needing an IP address is received by an APN with this option enabled, it will be rejected with a cause code of 220 (Unknown PDP address or PDP type).

**prefer-dhcp-options**
If this keyword is specified with `dhcp-proxy` for IP address allocation configuration, the GGSN will prefer DHCP-supplied parameters over values provided by AAA server or by local configuration. This keyword controls the following parameters:
- primary and secondary Domain Name Server (DNS) addresses
- primary and secondary NetBIOS Name Server (NBNS) addresses
These values will be sent out in the PCO IE of a GTP Create PDP Response Message whenever the MS Requests them in A Create PDP Request Message.
Default: Disabled

**Important:** This keyword is available only with `dhcp-proxy` ip allocation method as this functionality is implemented only for GGSN acting as DHCP proxy.

By default, this functionality is disabled. Hence, DNS and NBNS values received from a DHCP server will not be considered by the GGSN.

**allow-deferred**
Enables support for P-GW deferred address allocation. Default: Disabled

**allow-user-specified**
Enables support for PDP contexts requesting the use of specific (static) addresses. Default: Enabled

**Important:** If this option is not enabled, PDP contexts requesting the use of a static address will be rejected with a cause code of 220 (Unknown PDP address or PDP type).

**Usage**
Use this command to configure the method by which the APN profile will assign IP addresses to PDP contexts.
When the PDP context is being established and the APN name is determined, the system will examine the APN’s configuration profile. Part of that procedure is determining how to handle IP address allocation. The figure in the Example section below displays the process used by the system to determine how the address should be allocated.

**Example**
The following command configures the APN to dynamically assign an address from a DHCP server and reject PDP sessions with static IP addresses:
**ip address alloc-method dhcp-proxy**

The following command configures the APN to reject sessions requesting dynamically assigned addresses and only allow those with static addresses:

**ip address alloc-method no-dynamic allow-user-specified**

The following figure provides the IP address allocation process:
Figure 3. IP Address Allocation Process

1. System rejects session with cause code 220 (DCH, Unknown PDP address or PDP type)
2. Is a user-specified IP address provided?
   - Yes: Is allow-user-specified option enabled?
     - Yes: Address available in locally configured static pool?
       - Yes: Use IP address specified by user
     - No: No
   - No: No
3. Is authentication required?
   - Yes: IP address provided by authentication server?
     - Yes: Does IP address exist in a configured static pool?
       - Yes: Use assigned IP address
     - No: No
   - No: IP address pool name provided by authentication server?
     - Yes: Does pool name match a configured static pool?
       - Yes: Use IP address from specified pool
       - No: No
     - No: No
4. Is local allocation method enabled?
   - Yes: Is pool name configured for ip address pool name command?
     - Yes: Does pool name match a configured private pool?
       - Yes: Use IP address from specified public pool
       - No: System rejects session with cause code 220 (DCH, Unknown PDP address or PDP type)
     - No: No
   - No: No
5. Is dhcp-proxy allocation method enabled?
   - Yes: Assign IP address from block received from DHCP server
   - No: No
6. Is dhcp-relay-agent option enabled?
   - Yes: System negotiates IP address of 0.0.0.0 with MS
   - No: System receives DHCP packets from MS and forwards them to DHCP server

System rejects session with cause code 220 (DCH, Unknown PDP address or PDP type)
ip address pool

Configures the name of an IP address pool configured on the system from which to assign an address for a PDP context.

Product
GGSN
P-GW
SAEGW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > APN Configuration
configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-apn)#

Syntax

[ no ] ip address pool name pool_name

no

Removes a previously configured pool name.

pool_name

Specifies the name of the pool configured on the system from which an IP address will be assigned. The name is expressed as an alphanumeric string of 1 through 31 characters that is case sensitive.

Usage

If the ip address alloc-method command is configured to allow the assignment of IP addresses from a local pool configured on the system. It command instructs the system as to which pool should be used. The pool specified by this command must be a pool configured in the destination context on the system. Please refer to the ip pool command in the Context Configuration Mode Commands chapter for information on configuring IP address pools.

Multiple APNs can use the same IP address pool if required. In addition, this command could be issued multiple times to allow a single APN to use different address pools.

⚠️ Caution: From 14.0 onward for configuration of multiple IP pool in an APN, GGSN expects Framed-IP-Address and Framed-Pool from RADIUS.

⚠️ Caution: In pre-release 14.0, the maximum number of IP pools in an APN is 16 for static and dynamic type of pool. From 14.0 onward this limit has been changed for static address allocation to 1 and out of the maximum 16 pools which can be configured under a particular APN, the first IP pool should be a static pool, which is the only working static pool from an APN.

Example
The following command configures the system to use a pool named `private_pool1` for address allocation:

```
ip address pool private_pool1
```
**ip address pool-exhaust-action**

Configures the behavior to accept/reject a call if the IPv4 address pool is exhausted.

**Product**
- GGSN
- P-GW
- SAEGW

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration > Context Configuration > APN Configuration

```
configure > context context_name > apn apn_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-apn)#
```

**Syntax**

```
ip address pool-exhaust-action { ipv6-accept | ipv6-reject }
```

- **ipv6-accept**
  
  GGSN/P-GW will not reject the call; follows the standard behavior of allocating the available IP address.

- **ipv6-reject**
  
  Enables rejecting a call if GGSN/P-GW cannot allocate the IPv4 address for PDN type IPv4v6.

**Usage**

As per the standard behavior, when a UE sends a Create Request to GGSN/P-GW with PDN type IPv4v6, it should allocate both IPv4 and IPv6 address to the UE. If GGSN/P-GW fails to allocate the IPv4 address due to IP pool exhaustion, then it allocates only IPv6 address and changes the PDN Type to IPv6 and the call continues. In order to control this behavior, this CLI has been introduced; when configured, the following behavioral scenarios will be in place:

- CLI executed with `ipv6-reject` option will reject a call if GGSN/P-GW cannot allocate the IPv4 address for PDN type IPv4v6.
- CLI executed with `ipv6-accept` option will not reject a call and follow the standard behavior.

**Example**

The following command will reject a call if IPv4 type address allocation is not possible by GGSN/P-GW:

```
ip address pool-exhaust-action ipv6-reject
```
ip context-name

Configures the name of the destination context to use for subscribers accessing this APN.

Product
GGSN
P-GW
SAEGW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > APN Configuration

Syntax

[ no ] ip context-name ctx_name

- no
  Removes a previously configured context name.

- ctx_name
  Specifies the name of the context through which subscriber data traffic will be routed. ctx_name must be an alphanumeric string from 1 to 79 characters.

Usage
Use this command to specify the name of a destination context configured on the system through which to route all subscriber data traffic. This context will be used for subscribers accessing this APN. If no name is specified, the system will use the context in which the APN is configured as the destination context. When the APN is used to support Mobile IP functionality, this command is used to indicate the context in which the FA (foreign Agent) service is configured. If no name is specified, the context in which the GGSN service facilitating the subscriber PDP context is used.

Example
The following command configures the system to route subscriber traffic for the APN through a context called ispl:

    ip context-name ispl
**ip header-compression**

Configures IP packet header compression parameters for this APN.

**Product**
- GGSN
- P-GW
- SAEGW

**Privilege**
- Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > APN Configuration
```plaintext
configure > context context_name > apn apn_name
```
Entering the above command sequence results in the following prompt:
```
[context_name]host_name(config-apn)#
```

**Syntax**
```
ip header-compression vj
```
```
default ip header-compression
```
```
o ip header-compression
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Disables Van-Jacobson header compression.</td>
</tr>
<tr>
<td>no</td>
<td>Disables Van-Jacobson header compression.</td>
</tr>
<tr>
<td>vj</td>
<td>Enables Van-Jacobson header compression for IP packets. Default: Enabled</td>
</tr>
</tbody>
</table>

**Usage**
IP header compression reduces packet header overhead resulting in more efficient utilization of available bandwidth.

**Example**
The following command disables packet header header compression for the APN:
```
no ip header-compression
```
ip hide-service-address

Renders the IP address of the GGSN unreachable from mobile stations (MSs) using this APN. This command is configured on a per-APN basis.

Product
GGSN
P-GW
SAEGW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > APN Configuration

\[\text{configure} > \text{context} \ context\_name \ > \text{apn} \ apn\_name\]

Entering the above command sequence results in the following prompt:

\[\text{context\_name}\_host\_name(config-apn)\#\]

Syntax

\[[\text{default} | \text{no}] \ ip \ hide-service-address\]

\[\text{default}\]

\text{Does not allow the mobile station to reach the GGSN IP address using this APN.}\n
\[\text{no}\]

\text{Allows the mobile station to reach the GGSN IP address using this APN.}\n
Usage

This hides the GGSN IP address from the mobile station for security purposes.

Example

The following command allows the GGSN’s IP address to be viewed by the mobile station:

\[\text{no ip hide-service-address}\]
**ip local-address**

Configures the local-side IP address of the subscriber's point-to-point connection.

**Product**
- GGSN
- P-GW
- SAEGW

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration > Context Configuration > APN Configuration
- `configure > context context_name > apn apn_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-apn)#
```

**Syntax**

```
ip local-address ip_address
no ip local-address
```

- **no**
  - Removes a previously configured IP local-address.

- **ip_address**
  - Specifies an IP address configured in a destination context on the system through which a packet data network can be accessed. `ip_address` must be expressed in IPv4 dotted-decimal notation.

**Usage**

This parameter specifies the IP address on the system that the MS uses as the remote-end of the PPP connection. If no local address is configured, the system uses an unnumbered scheme for local-side addresses.

**Example**

The following command configures a local address of 192.168.1.23 for the MS:

```
ip local-address 192.168.1.23
```
ip multicast discard

Configures the IP multicast discard packet behavior.

Product
GGSN
P-GW
SAEGW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > APN Configuration
configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-apn)#

Syntax

[ default | no ] ip multicast discard

- default
Restores the APN IP parameters to the default multicast settings, which is to discard PDUs.

- no
Removes a previously configured IP multicast discard.

Usage
This command specifies if IP multicast discard is enabled or disabled.

Example
The following command enables IP multicast discard for an APN:

   ip multicast discard
**ip source-violation**

Enables or disables packet source validation for the current APN.

**Product**
- GGSN
- P-GW
- SAEGW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > APN Configuration

`configure > context context_name > apn apn_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-apn)#
```

**Syntax**

```
ip source-violation { ignore | check [ drop-limit limit ] } [ exclude-from-accounting ]
default ip source-violation
```

`default`

Restores the APN ip parameters to the default settings `check` enabled, `drop-limit` 10.

`ignore`

Default: Disabled
Disables source address checking for the APN.

`check [ drop-limit limit ]`

Default: Enabled, limit = 10
Enables the checking of source addresses received from subscribers for violations.
A `drop-limit` can be configured to set a limit on the number of invalid packets that can be received from a subscriber prior to their session being deleted. `limit` can be configured to any integer value between 0 and 1000000. A value of 0 indicates that all invalid packets will be discarded but the session will never be deleted by the system.

`exclude-from-accounting`

Default: Disabled
Excludes the packets identified with IP source violation from the statistics generated for accounting records.

**Usage**

Source validation is useful if packet spoofing is suspected or for verifying packet routing and labeling within the network.
Source validation requires the source address of received packets to match the IP address assigned to the subscriber (either statically or dynamically) during the session.

Example

The following command enables source address validation for the APN and configures a drop-limit of 15:

```
ip source-violation check drop-limit 15
```
**ip user-datagram-tos copy**

Controls the copying of the IP ToS octet value from user IPv4/IPv6 datagrams into the IP header of GTP tunnel encapsulations.

**Product**
- GGSN
- P-GW
- SAEGW

**Privilege**
- Security Administrator, Administrator

**Mode**

```
Exec > Global Configuration > Context Configuration > APN Configuration
configure > context context_name > apn apn_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-apn)#
```

**Syntax**

```
[ default | no ] ip user-datagram-tos copy
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Sets the default behavior of this command. By default this function is disabled.</td>
</tr>
<tr>
<td>no</td>
<td>Removes the preconfigured parameter for this command.</td>
</tr>
</tbody>
</table>

**Usage**

This command enables or disables the copying of the ToS byte from the inner IP header to the outer IP header for an RP connection.

When this function is enabled, the SGSN can detect the special ToS marking in the outer IP header of GTP tunnel packets and identify certain packets as control messages.
ipv6 access-group

Configures the IPv6 access group for the current APN profile which applies a single Access Control List (ACL) to multiple subscribers via the APN for IPv6 traffic.

**Product**
- GGSN
- ACS
- P-GW
- SAEGW

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration > Context Configuration > APN Configuration

```
configure > context context_name > apn apn_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-apn)#
```

**Syntax**

```
ipv6 access-group group_name [ in | out ] [ fallback-enabled ]
```

```[ no ] ipv6 access-group group_name [ in | out ]```

```
no
```

Removes a previously configured IPv6 ACL applied to a particular APN for IPv6 traffic. If at least one of the two \{ in | out \} options is not selected for the ACL that will be removed, the ACL will be removed for both directions.

```
group_name
```

Specifies the name of the IPv6 access group as an alphanumeric string of 1 through 79 characters.

```
in | out
```

Default: both (in and out)

Specifies the access-group as either inbound or outbound by the keywords in and out, respectively.

If no direction is supplied in the base command, the specified IPv6 access control list will be applied to both directions.

**Usage**

Use this command to apply a single IPv6 access control list to multiple subscribers via an APN for inbound or outbound IPv6 traffic.

If no traffic direction is specified, the selected access control list will be applied to both traffic directions.

**Example**
The following command associates the `sampleipv6Group` access group with the current APN profile for both inbound and outbound access:

```bash
ipv6 access-group sampleipv6Group
```

The following removes the outbound access group flag for `sampleipv6Group`:

```bash
no ipv6 access-group sampleipv6Group out
```
ipv6 address alloc-method

Controls the IPv6 address allocation method for a particular APN.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > APN Configuration

configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-apn)#

Syntax

ipv6 address alloc-method { dhcpv6-proxy [allow-prefix-delegation] | local | no-dynamic } [ allow-user-specified ]

[ default ] ipv6 address alloc-method

default
Configures the default address allocation method which is “local”.

dhcpv6-proxy
Configures the IPv6 address from DHCP server for the APN.

allow-prefix-delegation
Configures the APN to allow DHCPv6 prefix-delegation.

local
Configures the IPv6 address from the local pool configured.

no-dynamic
Configures the IPv6 address as indicated by the authentication server.

allow-user-specified
When any of the above three options is specified with allow-user-specified, the static IP address provided by UE takes priority and allocated/configured.

Usage
With the support of DHCPv6 and dual PDP IPv4v6, the separate allocation methods are required for IPv4 and IPv6. Earlier the IPv6 address was allocated through locap pool or RADIUS Returned, but with the new options: local, no-dynamic, and DHCPv6-proxy, the IPv6 address allocation can be done for a particular
APN. The static address allocation can be enabled by the use of `allow-user-specified` keyword with the above three options.

From 15.0 onward the support of prefix delegation for DHSCv6 is added to assign a network address prefix to a user site, configuring the user’s router with the prefix to be used for each interface it is attached to. This is one of the methods for delegating IPv6 address prefixes to an IPv6 subscriber’s network.

**Example**

The following command provides an example of allocating the IP address from DHCP server:

```
ipv6 address alloc-method dhcpv6-proxy allow-user-specified
```

The following commands configure the prefix-delegation for DHCPv6 with 52 bit length:

```
ipv6 address alloc-method dhcpv6-proxy allow-prefix-delegation ipv6 address prefix-delegation-len 52
```
ipv6 address prefix-delegation-len

Configures the supported prefix length to 48/52/56 bit length per-APN for DHCPv6 prefix-delegation support.

Product
All

Privilege
Security Administrator, Administrator

Syntax

[ no ] ipv6 address prefix-delegation-len { 48 | 52 | 56 }

no

Removes the configured prefix-delegation length to allow DHCPv6 prefix delegation.

Usage

Use this command to configure the length of prefix (48/52/56) to allow with DHCPv6 prefix delegation.

Example

The following command sets the allowed prefix length to 52 bit for DHCPv6 prefix delegation support:

ipv6 address prefix-delegation-len 52
ipv6 address pool-exhaust-action

Configures the behavior to accept/reject a call if the IPv6 address pool is exhausted.

Product
GGSN
P-GW
SAEGW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > APN Configuration
configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-apn)#

Syntax

ipv6 address pool-exhaust-action { ipv4-accept | ipv4-reject }

ipv4-accept

GGSN/P-GW will not reject the call; follows the standard behavior of allocating the available IP address.

ipv4-reject

Enables rejecting a call if GGSN/P-GW cannot allocate the IPv6 address for PDN type IPv4v6.

Usage

As per the standard behavior, when a UE sends a Create Request to GGSN/P-GW with PDN type IPv4v6, it should allocate both IPv4 and IPv6 address to the UE. If GGSN/P-GW fails to allocate the IPv6 address due to IP pool exhaustion, then it allocates only IPv4 address and changes the PDN Type to IPv4 and the call continues. In order to control this behavior, this CLI has been introduced; when configured, the following behavioral scenarios will be in place:

- CLI executed with ipv4-reject option will reject a call if GGSN/P-GW cannot allocate the IPv6 address for PDN type IPv4v6.
- CLI executed with ipv4-accept option will not reject a call and follow the standard behavior.

Example

The following command will reject a call if IPv6 type address allocation is not possible by GGSN/P-GW:

ipv6 address pool-exhaust-action ipv4-reject
ipv6 dns

Configures primary and secondary IPv6 Domain Name Service (DNS) servers.

**Product**

GGSN
P-GW
SAEGW

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > APN Configuration

configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-apn)#

**Syntax**

```
[ no ] ipv6 dns { primary | secondary } { ipv6_dns_address }
```

- **no**
  
  Deletes a previously configured DNS server.

- **primary**
  
  Configures the IPv6 address of primary DNS server for the APN.

- **secondary**
  
  Configures IPv6 address of the secondary DNS server for the APN. Only one secondary DNS server can be configured.

- **ipv6_dns_address**
  
  The IP address of the DNS server entered using IPv6 colon-separated-hexadecimal notation.

**Usage**

DNS servers are configured on a per-APN profile basis. This allows each APN profile to use specific servers in processing PDP contexts.

The DNS can be specified at the APN level in APN configuration as well as at the Context level in Context configuration mode with **ip name-servers** command, or it can be received from AAA server.

When DNS is requested in PCO configuration, the following preference will be followed for DNS value:

1. DNS Values received from LNS have the first preference
2. DNS values received from RADIUS Server has the second preference
3. DNS values locally configured with APN has the third preference
4. DNS values configured at context level with **ip name-servers** command has the last preference.
**Important:** The same preference would be applicable for the NBNS (NetBIOS Name Service) servers to be negotiated via ICPC (Initial Connection Protocol Control) with the LNS (L2TP Network Server).

**Example**

The following command provides an example of setting the primary DNS server:

```plaintext
ipv6 dns primary fe80::c0a8:a04
```
**ipv6 egress-address-filtering**

Enables or disable IPv6 egress address filtering. This function filters out packets not meant for the mobile interface ID. The GGSN records the source interface ID of all the packets received from the mobile node. When packets sent to the mobile node are received, the destination interface ID is compared against the list of recorded interface IDs and with the local interface-ID assigned to the MS during IPv6CP. If no match is found, the packet is dropped.

**Product**
- GGSN
- P-GW
- SAEGW

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration > Context Configuration > APN Configuration
- configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-apn)#
```

**Syntax**

```
[ no ] ipv6 egress-address-filtering
```

- **no**
  - Disables IPv6 egress address filtering.

**Usage**

Used to filter packets that arrive from the internet to a particular site.

**Example**

The following command provides an example disabling egress address filtering:

```
no ipv6 egress-address-filtering
```
**ipv6 initial-router-advt**

Creates an IPv6 initial router advertisement interval for the current APN.

**Product**
- GGSN
- P-GW
- SAEGW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > APN Configuration

```
configure > context context_name > apn apn_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-apn)#
```

**Syntax**

```
ipv6 initial-router-advt { interval int_value | num-advts num_value }
[ default ] ipv6 initial-router-advt { interval | num-advts }
```

- **default**
  Resets interval or num-advts to their default setting.

- **interval int_value**
  Specifies the time interval (in milliseconds) when the initial IPv6 router advertisement is sent to the mobile node as an integer from 100 through 16000. Default: 3000ms

- **num-advts num_value**
  Specifies the number of initial IPv6 router advertisements sent to the mobile node as an integer from 1 through 16. Default: 3

**Usage**
This command is used to set the advertisement interval and the number of advertisements. Using a smaller advertisement interval increases the likelihood of router being discovered more quickly when it first becomes available.

**Example**
The following command specifies the initial ipv6 router interval to be 2000ms:

```
ipv6 initial-router-advt interval 2000
```
### l3-to-l2-tunnel address-policy

Configures the address allocation/validation policy, when subscriber L3 (IPv4/IPv6) sessions are tunneled using an L2 tunneling protocol, such as L2TP.

**Product**
- GGSN
- P-GW
- SAEGW

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration > Context Configuration > APN Configuration
- `configure > context context_name > apn apn_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-apn)#
```

**Syntax**

```
l3-to-l2-tunnel address-policy { alloc-only | alloc-validate | no-alloc-validate }
default l3-to-l2-tunnel address-policy
```

- **default**
  - Restores the layer 3-to-layer 2 tunnel address policy parameter to the default setting of validation with no allocation.

- **alloc-only**
  - Specifies that the system locally allocates and validates subscriber addresses. Default: Disabled

- **alloc-validate**
  - Specifies that the system allocates addresses when IP addresses are dynamically assigned. The system does not validate the address specified by the subscriber. Default: Disabled

- **no-alloc-validate**
  - Specifies that the system does not allocate or validate subscriber addresses locally for such sessions; it passes the address between remote tunnel terminator to the mobile node. Default: Enabled

**Usage**

This command can be useful for MIP HA sessions tunneled from the system using L2TP tunnels, or GGSN PDP contexts of type IP tunneled using L2TP to a remote LNS.

**Example**

The following command configures the system to locally allocate and validate subscriber addresses:

```
l3-to-l2-tunnel address-policy alloc-only
```
loadbalance-tunnel-peers

Configures how tunnel-peers are selected for this APN.

Product
GGSN
P-GW
SAEGW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > APN Configuration
configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:
[context_name]host_name(config-apn)#

Syntax
loadbalance-tunnel-peers { balanced | prioritized | random }
default loadbalance-tunnel-peers

default
Restores the loadbalance-tunnel-peers parameter to the default setting of random.

balanced
Tunnel-peer selection is made without regard to prioritization, but in a sequential order that balances the load across the total number of peer nodes available. Default: Disabled

prioritized
Tunnel-peer selection is made based on the priority configured for the peer. Default: Disabled

random
Tunnel-peer selection is random in order. Default: Enabled

Usage
Use this command to configure the load-balancing algorithm that defines how the tunnel-peers are selected by the APN when multiple peers are configured in the APN.

Example
The following command sets the APN to connect to tunnel-peers in a sequential order:

load-balancing balanced
**long-duration-action detection**

Sets the detection of a session that exceeds the long duration timer and sends notification.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > APN Configuration

`configure > context context_name > apn apn_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-apn)#
```

**Syntax**

```
long-duration-action detection

default long-duration-action
```

```
default
Restores the long-duration-action parameter to its default setting of detection.
```

```
long-duration-action detection

Detects long duration sessions and sends SNMP TRAP and CORBA notification. This is the default behavior. Default: Enabled
```

**Usage**

Use this command to detect a session that exceeds the limit set by the long duration timer. Refer to the `timeout idle` and `timeout long-duration` commands for information on setting the long duration timer.

**Example**

Use the following command to enable detecting the session that exceeds the long duration timer:

```
long-duration-action detection
```
long-duration-action disconnection

Specifies what action is taken when the long duration timer expires.

Product: All
Privilege: Security Administrator, Administrator
Mode: Exec > Global Configuration > Context Configuration > APN Configuration

configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-apn)#

Syntax

long-duration-action disconnection [ suppress-notification ] [ dormant-only ] +

---

long-duration-action disconnection

Detects a long duration session and disconnects the session after sending SNMP TRAP and CORBA notification. Default: Disabled

---

suppress-notification

Suppress the SNMP TRAP and CORBA notification after detecting and disconnecting a long duration session. Default: Disabled

---

dormant only

Disconnects the dormant sessions after long duration timer and inactivity time with idle time-out duration expires. It sends the SNMP TRAP and CORBA notification after disconnecting a long duration session. Default: Disabled

Usage

Use this command to determine what action is taken when a session exceeds the limit set by the long duration timer.
Refer to the timeout idle and timeout long-duration command for information on setting the long duration timer.

Example

Use the following command to enable disconnecting sessions that exceed the long duration timer:

    long-duration-action disconnection

Use the following command to disconnect the session that exceed the long duration timer without sending SNMP TRAP and CORBA notification:

    long-duration-action disconnection suppress-notification
Use the following command to disconnect the session that exceed the long duration timer and also inactivity timer for idle time-out duration and send SNMP TRAP and CORBA notification:

```plaintext
long-duration-action disconnection dormant-only
```

Use the following command to disconnect the session that exceed the long duration timer and also inactivity timer for idle time-out duration without sending any SNMP TRAP and CORBA notification. If the session is idle and the session-idle-time >= inactivity time the session gets disconnected. Even if session is idle when the long-duration timed-out and session-idle time < inactivity time the timer value is reset to idle-timeout time.

```plaintext
long-duration-action disconnection dormant-only suppress-notification
```
mbms bmsc-profile

Applies a configured Broadcast-Multicast Service Center (BM-SC) profile to subscribers through APN for Multimedia Broadcast Multicast Service (MBMS) support and functionality.

Product
GGSN
P-GW
SAEGW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > APN Configuration
configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-apn)#

Syntax

mbms bmsc-profile name bmsc_profile_name

[ default | no ] mbms bmsc-profile

default
Applies the default BMSC profile to the subscribers through the APN.

no
Deletes a previously associated BM-SC profile with this APN.

name bmsc_profile_name

Specifies a name for the BM-SC profile already configured in BMSC configuration mode.
bmsc_profile_name is an alphanumeric string of 1 through 79 characters that may contain dots (.) and/or dashes (-).

Usage

Use this command to associate a configured BM-SC profile to use for MBMS contexts with this APN for MBMS feature support.
For more information on BM-SC profile configuration, refer to the BMSC Profile Configuration Mode Commands chapter.
This command also configures the specific BM-SC profile to use for Internet Group Management Protocol (IGMP) JOIN requests received from PDP contexts with this APN.

Example

Following command applies a previously configured BM-SC profile named bm_sc_1 to an APN within the specific context.
mbms bmsc-profile name bm_sc_1
mbms bearer timeout

Configures the session timeout values for the Multimedia Broadcast Multicast Service (MBMS) bearer contexts with this MBMS APN.

Product
GGSN
P-GW
SAEGW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > APN Configuration
configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-apn)#

Syntax

mbms bearer timeout { absolute | idle } time
[ default | no ] mbms bearer timeout { absolute | idle }

default
Sets the default value for the followed option for MBMS bearer context timeout.

no
Returns the timeout parameter to its default setting. If neither the absolute or idle keywords are used in conjunction with this keyword, both timeout options will be returned to their default settings.

absolute
Configures the absolute maximum time (in seconds) an MBMS bearer context may exist in any state (active or idle). Default: Disabled

idle
Default: Disabled
Configures the maximum amount of time (in seconds) an MBMS bearer context may be idle.

time
time can be any integer value between 0 and 4294967295. A time of 0 disables timeouts for this APN. Default: 0

Usage
Use this command to limit the amount of time that an MBMS bearer context session can remain connected.
Example

The following commands enables an absolute time timeout of 60000 seconds for MBMS bearer context:

```
mbms bearer timeout absolute 60000
```
mbms ue timeout

Configures the session timeout values for the Multimedia Broadcast Multicast Service (MBMS) user equipment (UE) contexts with this MBMS APN.

Product
GGSN
P-GW
SAEGW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > APN Configuration
configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-apn) #

Syntax

mbms ue timeout absolute time

[ default | no ] mbms ue timeout absolute

default
Set the default value for the followed option for MBMS UE context timeout.

no
Returns the timeout parameter to its default setting. If neither the absolute or idle keywords are used in conjunction with this keyword, both timeout options will be returned to their default settings.

absolute time
Configures the absolute maximum time (in seconds) an MBMS UE context may exist in any state (active or idle). time can be any integer value between 0 and 4294967295. A time of 0 disables timeouts for this APN. Default: 0

Usage
Use this command to limit the amount of time that an MBMS UE context session can remain connected.

Example
The following commands enables an absolute time timeout of 60000 seconds for MBMS UE context:

mbms bearer timeout absolute 60000
mediation-device

Enables the use of a mediation device and specifies the system context to use for communicating with the device.

**Product**
GGSN
P-GW
SAEGW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > APN Configuration

```plaintext
configure > context context_name > apn apn_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-apn)#
```

**Syntax**

```plaintext
mediation-device [ context-name context_name ] [ delay-GTP-response ] [ no-early-PDUs ] [ no-interims ] +
[ default | no ] mediation-device
```

+  
Indicates that more than one of the options can be specified with a single execution of the command.

**default**
Changes the mediation device to no context-name configured and restores the mediation device’s default properties.

**no**
Deletes the mediation-device configuration.

**context-name context_name**

Configures the mediation VPN context for this APN as an alphanumeric string of 1 through 79 characters that is case sensitive. If not specified, the mediation context is the same as the destination context of the subscriber. Default: The subscriber’s destination context.

**delay-GTP-response**
When enabled, delays the CPC response until an Accounting Start response is received from the mediation device. Default: Disabled

**no-early-pdus**
Specifies that the system delays PDUs from the MS until a response to the GGSN accounting start request is received from the mediation device. The PDUs are queued, not discarded. Default: Disabled
If “no-early-PDUs” is enabled, the chassis does not send uplink/downlink data from/to a MS until it receives the Acct-Rsp Start for the same from the mediation device. On receiving the Acct-Rsp, pending PDUs are forwarded. The chassis buffers up to two PDUs per call. As soon as the third PDU comes, the buffering is disabled and all the PDUs are forwarded for that call.

Configures the system to queue up to two PDUs until the mediation device returns a response to the system's accounting START request per 3GPP standards. On receiving the Accounting response message, the system forwards the subsequent PDUs without discarding any of the packets.

**Important:** For StarOS 10.0 and earlier releases, the system buffers up to four PDUs and queues or discards the remaining PDUs.

**Important:** For StarOS 11.0 and later releases, the system is configured so that none of the PDUs are discarded.

```bash
going mediatio
```

Disables sending interims to the mediation server. Default: Disabled

**Important:** Different commands are used to disable RADIUS interims for RADIUS accounting and mediation accounting. To disable RADIUS interims for mediation accounting, use the following command: `mediation-device context-name context_name no-interims`. To disable RADIUS interims for RADIUS accounting, use the following command: `accounting-mode radius-diameter no-interims`.

**Usage**

This command enables mediation device support for the APN. Mediation devices can be either deep-packet inspection servers or transaction control servers.

Keywords to this command can be used in combination to each other, depending on configuration requirements.

**Example**

The following command enables mediation device support for the APN and uses the protocol configuration located in an system context called `ggsn1`:

```bash
  mediation-device context-name ggsn1
  mediation-device context-name ggsn1 no-interims no-early-pdus
  mediation-device no-early-pdus no-interims
  mediation-device no-interims no-early-pdus
```

The following command enables mediation device support for the APN and uses the protocol configuration located in the subscribers destination context:

```bash
  mediation-device
```
**mobile-ip home-agent**

Configures the IP address of the home agent (HA) used by the current APN to facilitate subscriber Mobile IP sessions.

**Product**
- GGSN
- FA
- P-GW
- SAEGW

**Privilege**
- Security Administrator, Administrator

**Mode**
```
Exec > Global Configuration > Context Configuration > APN Configuration
```
```
configure > context context_name > apn apn_name
```
Entering the above command sequence results in the following prompt:
```
[context_name]host_name(config-apn)#
```

**Syntax**
```
mobile-ip home-agent ip_address [ alternate ]
```
```
no mobile-ip home-agent ip_address alternate
```
```
default mobile ip home-agent
```
```
default
```
Restores the APN mobile-ip parameters to the default setting, no HA address defined.
```
no
```
Removes a previously configured HA address.
```
```
ip_address
```
Specifies the IP address of the HA expressed in IPv4 dotted-decimal notation.
```
```
alternate
```
Designates this Mobile IP HA as the alternate that will be used in the event of a fail-over.

**Usage**
If the APN is configured to support Mobile IP for all PDP contexts it is facilitating, this command specifies the IP address of the HA that is to be used.

**Example**
The following command configures an HA IP address of 192.168.1.15:
```
mobile-ip home-agent 192.168.1.15
```
mobile-ip min-reg-lifetime-override

Specifies the minimum registration timer to override the platform-wide default on an enterprise basis. This feature is associated with 4G LTE scenarios employing Network Mobility (NEMO) routing.

**Product**

P-GW

HA

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > APN Configuration

```
configure > context context_name > apn apn_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-apn)#
```

**Syntax**

```
mobile-ip min-reg-lifetime-override { seconds | infinite }

default mobile-ip min-reg-lifetime-override

no mobile-ip min-reg-lifetime-override
```

- **default**
  
  Sets the minimum registration time to 600 seconds.

- **no**
  
  Deletes the registration interval entered via this command.

- **seconds**
  
  Specifies the minimum registration interval in seconds as an integer from 1 through 65534. Default = 600

- **infinite**
  
  Sets the minimum registration interval as “infinite” (forever) for this subscriber.

**Usage**

Specify the minimum registration timer to override the platform-wide default on an enterprise basis. With this command, NEMO traffic could be re-routed symmetrically to an alternate carrier within the specified number of seconds following a failure on the primary communication path.

**Example**

The following command sets the minimum registration override interval to 900 seconds:

```
mobile-ip min-reg-lifetime-override 900
```
mobile-ip mn-aaa-removal-indication

Configures the system to remove various information elements when relaying Registration Request messages to the HA.

**Product**
GGSN
FA
P-GW
SAEGW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > APN Configuration

```
configure > context context_name > apn apn_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-apn)#
```

**Syntax**

```
[ default | no ] mobile-ip mn-aaa-removal-indication
```

- **default**
  Sets the default setting for mobile IP MN-AAA-Removal-Indication.

- **no**
  Disables this functionality. This is the default setting.

**Usage**

When this functionality is enabled, the MN-FA challenge and MN-AAA authentication extensions are removed when relaying a Registration Request (RRQ) to the HA.
**mobile-ip mn-ha-hash-algorithm**

Designates the encryption algorithm to use for Hash-based Message Authentication Code (HMAC).

**Product**
GGSN
P-GW
SAEGW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > APN Configuration

```
configure > context context_name > apn apn_name
```
Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-apn)#
```

**Syntax**

```
mobile-ip mn-ha-hash-algorithm { hmac-md5 | md5 | rfc2002-md5 }
```

```
default mobile-ip mn-ha-hash-algorithm
```

```
default
Designates the default encryption algorithm to use.
```

```
hmac-md5 | md5 | rfc-2002-md5
Default: hmac-md5
The encryption algorithms that may be used.
```

**Usage**
Provides security by encrypting the data.

**Example**
The following command sets encryption for md5:

```
mobile-ip mn-ha-hash-algorithm md5
```
mobile-ip mn-ha-shared-key

Configures the subscriber MobileNode-Home Agent (MN-HA) shared key.

**Product**
- GGSN
- P-GW
- SAEGW

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration > Context Configuration > APN Configuration
  
  configure > context context_name > apn apn_name

  Entering the above command sequence results in the following prompt:

  
  [context_name]host_name(config-apn)#

**Syntax**

```
mobile-ip mn-ha-shared-key key
```

`no mobile-ip mn-ha-shared-key`

  `no`

  Disables this functionality. This is the default setting.

  `key`

  Specifies the subscriber MN-HA shared key as either an alphanumeric string or a hexadecimal number sequence beginning with “0x”. The string or sequence consists of 16 to 127 characters.

**Usage**

Configures a shared key for the APN.

**Example**

The following command configures a shared key as the alphanumeric string `sfd23408imi9yn`:

```
mobile-ip mn-ha-shared-key sfd23408imi9yn
```
mobile-ip mn-ha-spi

Configures the Mobile IP Security Parameter Index (SPI).

Product
GGSN
P-GW
SAEGW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > APN Configuration
configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-apn)#

Syntax
mobile-ip mn-ha-spi spi_number
no mobile-ip mn-ha-spi

no
Disables this functionality. This is the default setting.

spi_number
Specifies the SPI as an integer from 256 through 4294967295.

Usage
Configures an SPI for the APN.

Example
The following command configures an SPI of 15111111111111111111111111111111:

    mobile-ip mn-ha-spi 15111111111111111111111111111111
mobile-ip required

Enables support for Mobile IP functionality for all PDP contexts facilitated by the current APN.

Product
- GGSN
- FA
- P-GW
- SAEGW

Privilege
- Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > APN Configuration

configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-apn)#

Syntax

[ default | no ] mobile-ip required

- default
  Applies the default setting for mobile-ip for the APN. Default is disabled.

- no
  Disables mobile-ip for the APN.

Usage

Mobile IP functionality for IP PDP contexts is only supported at the APN-level. This command enables or disables Mobile IP support for the APN.

When Mobile IP is performed, the system authenticates the subscriber and the Mobile IP FA.

If this option is enabled, the system deletes all PDP contexts attempting to access the APN for which a Mobile IP session can not be established.
mobile-ip reverse-tunnel

Configures the system to support reverse-tunneling for Mobile IP sessions facilitated by the current APN.

Product
- GGSN
- FA
- P-GW
- SAEGW

Privilege
- Security Administrator, Administrator

Mode
`Exec > Global Configuration > Context Configuration > APN Configuration`
```
configure > context context_name > apn apn_name
```
Entering the above command sequence results in the following prompt:
```
[context_name]host_name(config-apn)#
```

Syntax
```
[ default | no ] mobile-ip reverse-tunnel
```
- **default**
  Designates the default reverse tunnel for the APN. The default is enabled.
- **no**
  Disables this functionality.

Usage
Use this command to enable support for Mobile IP reverse tunneling for the APN. Reverse tunneling is enabled by default.
nai-construction

Configures the Network Access Identifier (NAI) construction parameters on a per-APN basis only, rather than by per-aaa-group when constructed NAI authentication is enabled.

Product
GGSN
P-GW
SAEGW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > APN Configuration

configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-apn)#

Syntax

nai-construction { imsi | msisdn } [ override-null-username ] [ encrypted password encrypt_password | use-shared-secret-password | password password ]

no nai-construction

no
Disables the NAI construction at the APN level.

imsi
Enables NAI construction using IMSI for authentication for a user. GGSN constructs NAI using IMSI when no user-name is received. This is the default setting. Default: Enabled

msisdn
Enables NAI construction using Mobile Station International ISDN Number (MSISDN) for authentication for a user. GGSN constructs NAI using MSISDN when no user-name is received.

override-null-username
Enables NAI construction using IMSI/MSISDN for authentication for a user or when empty user name is received.

encrypted password
Specifies an encrypted password is to be used for this NAI-constructed user. string is an alphanumeric string of 0 through 63 characters.
password
Configures the authentication user-password for this NAI-constructed user. `password` is an alphanumeric string of 0 through 63 characters.

use-shared-secret-password
Specifies use of the RADIUS authentication shared secret password for this NAI-constructed user.

Usage
NAI-construction defines the behavior for construction at the APN level. If defined for a particular APN, this command works independently and overwrites the behavior of `aaa constructed-nai` defined at the context level for calls involving this APN.

Note that NAI construction using IMSI or MSISDN, where either no user name is received or a blank user name is received for authentication, is applicable only when NAI constructed authentication is enabled using the `aaa nai-construction authentication` command in Context Configuration Mode.

Example
The following command enables NAI-construction using IMSI as the authentication type with an encrypted password:

```
nai-construction imsi encrypted password s1289sf980333jwwdo97342
```
## nbns

Configures and enables use of NetBios Name Service (NBNS) for the APN.

### Product
- GGSN
- P-GW
- SAEGW

### Privilege
- Security Administrator, Administrator

### Mode
- Exec > Global Configuration > Context Configuration > APN Configuration
  ```
  configure > context context_name > apn apn_name
  ```
  Entering the above command sequence results in the following prompt:
  ```
  [context_name]host_name(config-apn)#
  ```

### Syntax

```
[ no ] nbns { primary | secondary } IP_address
```

- **no**
  Removes/disables use of a previously configured NetBios Name Service.

- **primary**
  Designates primary NBNS server. Must be followed with an IPv4 address in dotted-decimal notation.

- **secondary**
  Designates secondary/failover NBNS server. Must be followed with an IPv4 address in dotted-decimal notation.

- **IP_address**
  Specifies the IP address in IPv4 dotted-decimal notation.

### Usage
This command specifies NBNS parameters. The NBNS option is present for both pdp type IP and pdp type PPP for GGSN. The system can be configured to use NetBios Name Service for the APN.

### Example
The following command configures the APN’s NetBios Name Service to primary IP 192.168.1.15.

```
nbns primary 192.168.1.15
```
network-behind-mobile

Allows enabling/disabling the Network Behind Mobile Station (NBMS) for the APN.

**Product**
- GGSN
- P-GW
- SAEGW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > APN Configuration

```
configure > context context_name > apn apn_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-apn)#
```

**Syntax**

```
network-behind-mobile ( max-addresses-behind-mobile max_addrs | max-subnets max_subnets )
[ default | no ] network-behind-mobile
```

---

**default**

Enables the default settings for this function. It enables NBMS with max-subnets as 10 and max-addresses-
behind-mobile as 16,777,214 default values.

---

**no**

Disables the network behind mobile station functionality on the APN.

---

**max-addresses-behind-mobile max_addrs**

Configures the maximum number of addresses that are allowed in a single Network/subnet Behind MS.

`max_addrs` must be an integer from 1 through 16,777,214.

Default: 16,777,214

---

**max-subnets max_subnets**

Specifies the maximum number of subnets that can be enabled for a call in the APN.

`max_subnets` must be an integer from 1 through 16.

Default: 10

---

**Usage**

Use this command to enable or disable NBMS for the APN.

---

**Example**

The following command enables NBMS and allows a maximum of 16 routes to be installed on the APN
wherein maximum 268,435,454 host addresses are allowed in each network:
network-behind-mobile max-subnets 16
nexthop-forwarding-address

Configures the next hop forwarding address for the APN.

Product

GGSN
P-GW
SAEGW

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > Context Configuration > APN Configuration

configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-apn)#

Syntax

nexthop-forwarding-address ip_address

no nexthop-forwarding-address

no

Disables this function. This is the default setting.

ip_address

Specifies the IP address of the nexthop forwarding address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

Ensure the route is available for this nexthop address and its directly connected host. Use of an arbitrary address can cause a routing loop within the host and lead to dropped packets.

Usage

Use this command to configure the next hop forwarding address for the APN.

Example

The following command configures the next hop forwarding address to 10.1.1.1:

nexthop-forwarding-address 10.1.1.1
npu qos

Configures an NPU QoS priority queue for packets facilitated by the APN.

**Product**

GGSN
P-GW
SAEGW

**Privilege**

Security Administrator, Administrator\/

**Mode**

Exec > Global Configuration > Context Configuration > APN Configuration

```
configure > context context_name > apn apn_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-apn)#
```

**Syntax**

```
npu qos traffic priority { best-effort | bronze | derive-from-packet-dscp | gold | silver |

default npu qos traffic priority

  default
  Configures the default NPU QoS traffic priority.

  traffic priority { best-effort | bronze | derive-from-packet-dscp | gold | silver }

  best-effort: Assigns the best-effort queue priority. This is the lowest priority.
  bronze: Assigns the bronze queue priority. This is the third-highest priority.
  derive-from-packet-dscp: Specifies that the priority is to be determined from the DSCP (Differentiated Services Code Point) field in the packet's TOS octet. Default: Enabled
  gold: Assigns the gold queue priority. This is the highest priority.
  silver: Assigns the silver queue priority. This is the second-highest priority.
```

**Usage**

This command is used in conjunction with the Network Processing Unit (NPU) Quality of Service (QoS) functionality.

The system can be configured to determine the priority of a subscriber packet either based on the configuration of the APN, or from the differentiated service (DS) field in the packet's TOS octet (representing the differentiated service code point (DSCP) value).

Refer to the GGSN Administration Guide for additional information on NPU QoS functionality.

**Example**

The following command configures the APN’s priority queue to be **gold**:

```
npu qos traffic priority gold
```
outbound

Configures the APN host username and password.

Product
GGSN
P-GW
SAEGW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > APN Configuration

configure > context context_name > apn apn_name

 Entering the above command sequence results in the following prompt:

[context_name]host_name(config-apn)#

Syntax

outbound { [ encrypted ] password pwd | username name }

no outbound password | username

no

Removes previously configured outbound information for the APN.

encrypted

The encrypted keyword is intended only for use by the chassis while saving configuration scripts. The system displays the encrypted keyword in the configuration file as a flag that the variable following the password keyword is the encrypted version of the plain text password. Only the encrypted password is saved as part of the configuration file.

password pwd

Specifies the password to use for session authentication as an alphanumeric string of 1 through 132 characters that is case sensitive.

username name

Specifies the username to use for session authentication as an alphanumeric string of 1 to 127 characters that is case sensitive.

Usage

This command can be used to provide a username and password for authentication when the subscriber does not supply one in accordance with 3GPP standards. In addition, it can be used to create a PPP session when using L2TP to tunnel IP PDP contexts.

If only a username is specified using this command, the password is determined based on the setting of the aaa constructed-nai command in the Context Configuration mode. That command is also used to...
determine the password if an outbound username and password are configured for the APN when the imsi-auth keyword is specified for the authentication command in this mode.

Example

The following commands configures an APN username of *isp1* and a password of *secRet123*.

```plaintext
outbound username isp1
outbound password secRet123
```
**p-cscf**

Enables use of locally configured Proxy Call Session Control Function (P-CSCF) addresses or a Fully Qualified Domain Name (FQDN).

**Product**
- P-GW
- SAEGW

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration > Context Configuration > APN Configuration

```
configure > context context_name > apn apn_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-apn)#
```

**Syntax**

In StarOS V14.x and earlier:

```
p-cscf { fqdn fqdn | primary [ ip IPv4_address | ipv6 IPv6_address ] | secondary [ ip IPv4_address | ipv6 IPv6_address ] }
```

```
```

In StarOS V15.0 and later:

```
p-cscf { fqdn fqdn | priority address_priority [ ip IPv4_address | ipv6 IPv6_address ] }
```

```
no p-cscf { fqdn fqdn | priority address_priority [ ip | ipv6 ] }
```

**no**

Disables use of previously configured P-CSCF addresses or FQDN.

```
fqdn fqdn
```

Configures the P-CSCF FQDN server name for the APN as an alphanumeric string of 1 through 256 characters.

```
primary [ ipIPv4_address | ipv6 IPv6_address ]
```

Specifies the primary P-CSCF address for the APN.

- `IPv4_address` must be expressed in IPv4 dotted-decimal notation.
- `IPv6_address` must be expressed in IPv6 colon-separated-hexadecimal notation.

```
secondary [ ip IPv4_address | ipv6 IPv6_address ]
```

Specifies the secondary P-CSCF address for the APN.

- `IPv4_address` must be expressed in IPv4 dotted-decimal notation.
- `IPv6_address` must be expressed in IPv6 colon-separated-hexadecimal notation.
priority address_priority [ ip IPv4_address | ipv6 IPv6_address ]

Specifies the priority for P-CSCF address for the APN.
address_priority is an integer from 1 to 3. 1 is the highest priority.
IPv4_address must be expressed in IPv4 dotted-decimal notation.
IPv6_address must be expressed in IPv6 colon-separated-hexadecimal notation.

Usage
Use this command to specify the P-CSCF addresses or FQDN server name associated with this APN.

Example
The following command enables a P-CSCF with the primary IPv4 address 10.2.3.4 for the APN:

   p-cscf primary ip 10.2.3.4

The following command enables a P-CSCF with FQDN server name pcscfalias1.ind.pun.cisco.com for the APN:

   p-cscf fqdn pcscfalias1.ind.pun.cisco.com

The following command enables a P-CSCF with the IPv4 address 10.2.3.4 at the highest priority of 1 for the APN:

   p-cscf priority 1 ip 10.2.3.4
pco-options

This command controls the sending of customized PCO (Protocol Configuration Options) options in the network to MS GTP messages and configures APN to include link MTU in PCO IE.

**Product**
P-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > APN Configuration

```
configure > context context_name > apn apn_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-apn)#
```

**Syntax**

```
pco-options { customl [ ue-requested ] | link-mtu bytes }

{ default | no } pco-options [ customl | link-mtu ]
```

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>customl</code></td>
<td>Enable sending of customized PCO options in the network to MS messages; send customized PCO options to all UEs regardless of support.</td>
</tr>
<tr>
<td><code>ue-requested</code></td>
<td>Enable sending of customized PCO options in the network to MS messages for “UE-Requeste d” mode; send PCO to only UEs that request customized PCO options.</td>
</tr>
<tr>
<td><code>link-mtu bytes</code></td>
<td>Configures APN to include link MTU in PCO IE, if it is requested by UE. When UE sends IPv4 Link MTU Size PCO request during Initial attach/ Standalone PDN connection, then the S-GW/SGSN/HSGW sends the same transparently in Create Session Request, Create/Update PDP Context Request, or PBU to P-GW, GGSN, or PMIP-PGW. Create Session Response, Create/ Update PDP Context Response/ PBA will be sent with latest configured MTU size PCO value in APN. If UE is in outbound roaming, then default value (1500) will be provided in the MTU size PCO. <code>bytes</code> must be an integer from 1280 to 2000. Default: 1500</td>
</tr>
<tr>
<td><code>default</code></td>
<td>Disable sending of customized PCO options in the network to MS messagesand/or sets the link MTU PCO to 1500 bytes.</td>
</tr>
<tr>
<td><code>no</code></td>
<td>Do not send customized PCO options to any UEs and/or sets the link MTU PCO to 1500 bytes.</td>
</tr>
</tbody>
</table>
**Usage**

Use this command to enable or disable sending of customized PCO options in the network to MS GTP messages and configure link MTU size PCO value.

**Important:** Configure custom PCO values in `pco-custom1` command in *ACS Charging Action Configuration Mode*.

**Example**

The following command enables sending customized PCO options to all UEs regardless of support:

```
pco-options custom1
```

The following command disables sending of customized PCO options in the network to MS messages and sets the link MTU PCO to 1500 bytes:

```
default pco-options
```
**pdn-behavior**

Configures specific PDN behavior.

**Product**
P-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > APN Configuration

```configure > context context_name > apn apn_name```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-apn)#
```

**Syntax**

```pdn-behavior { custom1 | ims }```

```
[ default | no ] pdn-behavior
```

- **default | no**
  
  Configures APN as “Normal”.

- **custom1**
  
  Configures APN as a Custom1 (well-known) APN. Re-auth Requested reason code returned for PDN disconnect.

- **ims**
  
  Configures APN as an IMS APN. Re-auth Requested reason code returned for PDN disconnect.

**Usage**

Use this command to configure specific PDN behavior.

**Example**

The following command configures APN as an IMS APN which returns reason code Re-auth Requested for PDN disconnect:

```
pdn-behavior ims
```
**pdp-type**

Configures the type of PDP contexts that are supported by this APN.

**Product**
- GGSN
- P-GW
- SAEGW

**Privilege**
- Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > APN Configuration

`configure > context context_name > apn apn_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-apn)#
```

**Syntax**

```
pdp-type { ipv4 [ ipv6 ] | ipv6 [ ipv4 ] | ppp }
```

**default pdp-type**

```
default
```

Configures the default PDP type, IPv4, for the APN.

```
ipv4 [ ipv6 ]
```

Enables support for IPv4 PDP contexts. Also enables support for IPv6 if the IPv6 optional keyword is entered in this command. Default: Enabled

**Important:** Entering both IPv4 and IPv6 in either order enables support for both.

```
ipv6 [ ipv4 ]
```

Enables support for IPv6 PDP contexts. Also enables support for IPv4 if the IPv6 optional keyword is entered in this command. Default: Disabled

**Important:** Entering both IPv4 and IPv6 in either order enables support for both.

```
PPP
```

Enables support for PPP PDP contexts. Default: Disabled
Usage

IP PDP context types are those in which the MS is communicating with a PDN such as the Internet or an intranet using IP. PPP PDP contexts are those in which PPP or PPP Network Control Protocol (NCP) frames from the MS are either terminated at, or forwarded by the GGSN. If a session specifies a PDP type that is not supported by the APN, the system rejects the session with a cause code of 220 (DCH, Unknown PDP address or PDP type).

⚠️ Caution: For the IPv6 calls to work, the destination context must have at least one IPv6 interface configured.

Example

The following command configures the APN to support PPP context types:

```
pdp-type ppp
```
**permission**

Enables or disables the ability to use authorized services for the current APN.

**Product**
- P-GW
- SAEGW
- GGSN

**Privilege**
- Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > APN Configuration

```bash
configure > context context_name > apn apn_name
```

Entering the above command sequence results in the following prompt:

```
[context_name] host_name(config-apn)#
```

**Syntax**

```
[ no ] permission { nemo }
```

**Usage**
Use this command to enable support for NEMO or PMIPv6 functionality on the APN. These options are disabled by default.

**Example**
The following command enables NEMO functionality:

```
permission nemo
```

The following command disables NEMO functionality:

```
no permission nemo
```
policy

Configures the Mobile IPv6 policy to set the action to be taken when IPv4/IPv6 subscriber packets need to be tunneled and the encapsulated packets exceed the tunnel maximum transmission unit (MTU).

Product

P-GW
SAEGW

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > Context Configuration > APN Configuration

`configure > context context_name > apn apn_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-apn)#
```

Syntax

```
policy ipv6 tunnel mtu exceed { fragment [ inner ] | notify-sender }
[ default | no ] policy ipv6 tunnel mtu exceed
```

```default```

IPv6: System will do a Path MTU (PMTU) discovery and send “ICMPv6 Packet Too Big” to the original sender if the subscriber packet exceeds MTU after encapsulation.

IPv4: System will do an outer IPv6 fragmentation if the packet exceeds MTU after encapsulation.

```no```

Disables this functionality.

```ipv6 tunnel mtu exceed { fragment [ inner ] | notify-sender }```

`fragment`: System will do an outer IPv6 fragmentation if the subscriber packet exceeds MTU after encapsulation.

`inner`:

IPv6: System will do a PMTU discovery and send “ICMPv6 Packet Too Big” to the original sender if the subscriber packet exceeds MTU after encapsulation.

IPv4: If packet will exceed tunnel MTU after encapsulation, based on DF bit and ignore-DF config, the original IPv4 packet will be fragmented and then encapsulated so that it will not exceed MTU, or ICMP Error will be sent if IPv4 packet fragmentation is not allowed.

`notify-sender`:

IPv6: System will do a PMTU discovery and send “ICMPv6 Packet Too Big” to the original sender if subscriber packet exceeds MTU after encapsulation.

IPv4: System will do an outer IPv6 fragmentation if packet exceeds MTU after encapsulation.
Usage

This command sets the Mobile IPv6 policy for the action to be taken when IPv4/IPv6 subscriber packets need to be tunneled and the encapsulated packets exceed tunnel MTU size.

Example

The following command causes the system to do outer IPv6 fragmentation if the subscriber packet exceeds MTU after encapsulation:

```
policy ipv6 tunnel mtu exceed fragment
```
**ppp**

Configures the Point-to-Point Protocol (PPP) options for the current APN.

**Product**
- GGSN
- P-GW
- SAEGW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > APN Configuration

`configure > context context_name > apn apn_name`

Entering the above command sequence results in the following prompt:

```
<context_name>host_name(config-apn)#
```

**Syntax**

```plaintext
ppp { data-compression { protocols protocols | mode modes } | keepalive seconds | min-compression-size min_octets | mtu max_octets }

default ppp { data-compression protocols | keepalive | min-compression-size | mtu }

no ppp { data-compression protocols | keepalive seconds | mtu }
```

---

**default**

Configures the default PPP parameters for the specified APN.

---

**no**

Resets the option specified to its default setting.

---

**data-compression { mode modes | protocols protocols}**

Configures the data compression or the compression protocol to use for the APN. Default: all protocols enabled

- **mode modes**: Sets the compression mode to one of the following:
  - **normal**: Packets are compressed using the packet history for automatic adjustment and for best compression.
  - **stateless**: Each packet is compressed individually.

- **protocols protocols**: Sets the compression protocol to one of the following:
  - **deflate**: DEFLATE algorithm
  - **mppc**: Microsoft Point-to-Point Compression
  - **stac**: STAC LZS algorithm
**keepalive seconds**

Specifies the frequency of sending the Link Control Protocol (LCP) keep alive messages. `seconds` must be either 0 or an integer from 5 through 14400. The special value 0 disables the keep alive messages entirely. Default: 30

**min-compression-size min_octets**

Specifies the smallest packet to which compression may be applied as an integer from 0 through 2000. Default: 128

**mtu max_octets**

Specifies the maximum transmission unit (MTU) for packets accessing the APN as an integer from 100 through 2000. Default: 1500

**Important:** The MTU refers to the PPP payload which excludes the two PPP octets. Therefore, an MTU of 1500 corresponds to the 3GPP standard MTU of 1502 for GTP packets with PPP payloads.

**Usage**

Adjust packet sizes and compression to improve bandwidth utilization. Each network may have unique characteristics such that determining the best packet size and compression options may require system monitoring over an extended period of time.

**Example**

The following command configures the `ppp data-compression mode` for the APN to be `stateless`:

```
ppp data-compression mode stateless
```

The following command configures an MTU of 500 for the APN:

```
ppp mtu 500
```
**proxy-mip**

Configures support for Proxy Mobile IP functionality for the APN.

**Product**
- GGSN
- FA
- P-GW
- SAEGW

**Privilege**
- Security Administrator, Administrator

**Mode**
```
Exec > Global Configuration > Context Configuration > APN Configuration

configure > context context_name > apn apn_name
```

Entering the above command sequence results in the following prompt:
```
[context_name]host_name(config-apn)#
```

**Syntax**
```
[ default | no ] proxy-mip { required | null-username static-homeaddr }
```

- **default**
  Configures the default proxy MIP setting for the specified APN

- **no**
  Disables this functionality.

- **required**
  Default: Disabled.
  Enables proxy-mip for all subscribers using this APN.

- **null-username static-homeaddr**
  Configures handling of RRQ to enable the acceptance without an NAI extension in this APN. Default: Disabled

**Usage**
This command requires that Proxy Mobile IP functionality be performed for all PDP contexts facilitated by the APN.
When Proxy Mobile IP is performed, the system performs subscriber authentication but not Mobile IP FA authentication. It can be configured to handling of RRQ without NAI extension in an APN.
More information about Proxy Mobile IP support for the GGSN can be found in the *GGSN Administration Guide*.

**Example**
The following command causes the system to support Proxy Mobile IP for all PDP contexts facilitated by the APN:

```
proxy-mip required
```

The following command will enable the accepting of RRQ without NAI extensions in this APN.

```
proxy-mip null-username static-homeaddr
```
**qos negotiate-limit**

Configure the QoS profile to provide the peak and committed data rate limits that the GGSN assigns to the APN. The GGSN sends the QoS profile to the SGSNs in response to GTP Create/Update PDP Context requests for traffic shaping and policing functionality.

**Product**
- GGSN
- P-GW
- SAEGW

**Privilege**
- Security Administrator
- Administrator

**Mode**
- Exec > Global Configuration > Context Configuration > APN Configuration
- `configure > context context_name > apn apn_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-apn) #
```

**Syntax**

```

no qos negotiate-limit direction { downlink | uplink } [ qci qci_val ]
```

**no**
Disables the QoS Profile for the APN.

**direction { downlink | uplink }**

- `downlink`: Apply the specified limits and actions to the downlink (to-Gn direction).
- `uplink`: Apply the specified limits and actions to the uplink (to-Gi direction).

**qci qci_val**

`qci_val` is the QoS Class Identifier (QCI) for which the negotiate limit is being set. QCI ranges from 1 to 9. If no qci-val is configured, it will be handled as an undefined-qci (same as undefined-qos class).

**committed-data-rate bps**

Default: See the *Usage* section for this command
The committed data rate (guaranteed-data-rate) in bps (bits per second).

`bps` must be an integer from 1 through 16000000 for the downlink direction or 1 through 8640000 for the uplink direction. The value must also correspond to one of the permitted values identified the tables below. If a non-permitted value is entered for this parameter, the system rounds the value to the nearest lower supported value, except in the case where value is less than 1,000 bps. In this case, the system rounds the value to 1,000 bps. In addition, if the configured committed rate is lower than the value configured for the peak-data-rate, the system uses the configured peak rate for this parameter.
**Important:** System measurements for this value exclude the GTP and outer packet headers. In addition, some traffic classes have both a committed rate and a peak rate, while other traffic classes have just a peak rate. If a committed rate is not applicable (such as, the traffic class is background or interactive), an error occurs if this option is configured. If the committed-rate is applicable (such as, the traffic class is conversational or streaming), the values supplied by the SGSN are used if this option is not configured.

**peak-data-rate bps**

Default: See the Usage section for this command

Specifies the peak data-rate for the subscriber in bps (bits per second).

*bps* must be an integer from 1 through 16000000 for the downlink direction or 1 through 8640000 for the uplink direction. The value must also correspond to one of the permitted values identified in the tables below.

If a non-permitted value is entered for this parameter, the system rounds the value to the nearest lower supported value, except in the case where value is less than 1,000 bps. In this case, the system rounds the value to 1,000 bps.

**Usage**

This command configures the APN quality of service (QoS) profile. This feature enables configuring and enforcing bandwidth limitations on individual PDP contexts of a particular traffic class. Traffic classes are defined in 3GPP TS 23.107 and are negotiated during PDP context activation. Bandwidth enforcement is configured and enforced independently for the downlink and the uplink directions.

The profile information is sent to the SGSN(s) in response to GTP Create/Update PDP Context Request messages. If the QoS profile requested by the SGSN is lower than the configured QoS profile configured, the profile requested by the SGSN is used. If the QoS profile requested by the SGSN is higher, the configured rates are used.

Note that the values for the uplink/downlink committed-data-rate and peak-data-rate parameters are exchanged in the GTP messages between the GGSN and the SGSN. Therefore, the values used may be lower than the configured values. When negotiating the rate with the SGSN(s), the system convert this to a value that is permitted by GTP as shown in the tables below.

**Table 15. Permitted Values for Committed and Peak Data Rates in GTP Messages**

<table>
<thead>
<tr>
<th>Value (bps)</th>
<th>Increment Granularity (bps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>From 1000 to 63,000</td>
<td>1,000 (e.g. 1000, 2000, 3000, ... 63000)</td>
</tr>
<tr>
<td>From 64,000 to 568,000</td>
<td>8,000 (e.g. 64000, 72000, 80000, ... 568000)</td>
</tr>
<tr>
<td>From 57,600 to 8,640,000</td>
<td>64,000 (e.g. 576000, 640000, 704000, ... 8640000)</td>
</tr>
<tr>
<td>From 8,700,000 to 16,000,000</td>
<td>100,000 bps (e.g. 8700000, 8800000, 8900000, ... 16000000)</td>
</tr>
</tbody>
</table>

The command can be entered multiple times to specify different combinations of direction and class. If this command is not configured at all, the GGSN does not perform traffic policing or QoS negotiation with the SGSN.

Additional information on the QoS traffic shaping functionality is located in the *System Administration Guide*.

**Default Values:**

**Example**

The following command sets an uplink peak data rate of 128000 bps for QoS negotiation limit:
qos negotiate-limit direction uplink peak-data-rate 128000
qos rate-limit

Configures the action on a subscriber traffic flow that violates or exceeds the peak/committed data rate under traffic policing functionality.

Product
- GGSN
- P-GW
- SAEGW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > APN Configuration
configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-apn)#

Syntax

qos rate-limit direction { downlink | uplink } [ qci qci_val ] [ burst-size { bytes | auto-readjust [ duration dur ] } ] [ exceed-action { drop | lower-ip-precedence | transmit } ] [ violate-action { drop | lower-ip-precedence | shape [ transmit-when-buffer-full ] | transmit } ] [ violate-action { drop | lower-ip-precedence | shape [ transmit-when-buffer-full ] | transmit } ] [ exceed-action { drop | lower-ip-precedence | transmit } ] 

no qos rate-limit direction { downlink | uplink } [ qci qci_val ]

no

Disables the QoS data rate limit configuration for the APN.

Important: When no Qos Profile is configured, the system defaults to using the information provided by the SGSN.

qos rate-limit direction { downlink | uplink }

downlink: Apply the specified limits and actions to the downlink (the Gn direction).
uplink: Apply the specified limits and actions to the uplink (the Gi direction).

qci qci_val

qci_val is the QoS Class Identifier (QCI) for which the negotiate limit is being set. QCI ranges from 1 to 9. If no qci-val is configured, it will be handled as an undefined-qci (same as undefined-qos class).

burst-size { bytes | auto-readjust [ duration dur ] }

Default: See Usage section for this command.
The burst size allowed, in bytes for peak data rate and committed data rate.
bytes must be an integer from 1 through 6000000.

**Important:** It is recommended that the minimum value of this parameter be configured to the greater of the following two values: 1) three times greater than packet MTU for the subscriber connection, OR 2) 3 seconds worth of token accumulation within the “bucket” for the configured peak-data-rate. In addition, if the committed-data-rate parameter is specified, the burst-size is applied to both the committed and peak rates.

The `auto-readjust [ duration dur ]` keyword provides the option to calculate the Burst size dynamically while configuring the rate-limit. Whenever this keyword is enabled to calculate burst size, the GGSN QoS negotiated rate is enforced for this calculation. Whenever there is a change in the rates (due to a QoS update), the burst sizes will be updated accordingly. This keyword also provides two different burst sizes. One burst size for peak rate and another for committed rate. By default this keyword is disabled.

`duration dur` describes the duration of burst in seconds. If duration is not specified this keyword will use 1 second as default value.

`dur` must be an integer between 1 through 30.

**Important:** Traffic Shaping is not supported on the GGSN, P-GW, or SAEGW.

The action to take on the packets that exceed both the committed-data-rate and the peak-data-rate. The following actions are supported:

- **drop**: Drop the packet.
- **lower-ip-precedence**: Transmit the packet after lowering the IP precedence.
- **transmit**: Transmit the packet.

The action to take on the packets that exceed the committed-data-rate but do not violate the peak-data-rate. The following actions are supported:

- **drop**: Drop the packet.
- **lower-ip-precedence**: Transmit the packet after lowering the ip-precedence.
- **transmit**: Transmit the packet.

**Important:** This command is not intended for bearer level policing.
Important: If the exceed/violate action is set to “lower-ip-precedence”, this command may override the configuration of the `ip qos-dscp` command in the GGSN Service Configuration mode for packets from the GGSN to the SGSN. In addition, the GGSN service `ip qos-dscp` command configuration can override the APN setting for packets from the GGSN to the Internet. Therefore, it is recommended that this command not be used in conjunction with this action.

The command can be entered multiple times to specify different combinations of direction and class. If this command is not configured at all, the GGSN does not perform traffic policing or QoS negotiation with the SGSN. (It accepts all of the SGSN-provided values for the PDP context.)

To calculate the burst size dynamically, an optional keyword `auto-readjust [ duration dur ]` is provided with the `burst-size` keyword. By default, the burst size is fixed if defined in bytes with this command. Regardless of the rate being enforced, burst-size is fixed as set by the `burst-size bytes` parameter.

The `auto-readjust [ duration dur ]` keyword enables variable burst size depending on the rate being enforced. The system calculates burst size using a per token bucket algorithm calculation as \( T = B/R \), where \( T \) is the time interval, \( B \) is the burst size and \( R \) is the Rate being enforced. It also provides different burst size for Peak and Committed data rate-limiting.

If the `auto-readjust` keyword is not used, a fixed burst size must be defined which will be applicable for peak data rate and committed data rate regardless of the rate being enforced.

If the `auto-readjust` keyword is provided without specifying the duration, a default duration of 1 second will be used for burst size calculation.

Example

The following command lowers the IP precedence when the committed-data-rate and the peak-data-rate are violated in uplink direction:

```
qos rate-limit direction uplink violate-action lower-ip-precedence
```
qos-renegotiate

This keyword is obsolete.
**qos traffic-police**

This command is obsolete. This functionality is now supported through `qos negotiate-limit` and `qos rate-limit` commands.

**Mode**

Exec > Global Configuration > Context Configuration > APN Configuration

```bash
configure > context context_name > apn apn_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-apn)#
```
radius

This command is obsolete.
radius group

This command is obsolete.
radius returned-framed-ip-address

Sets the policy whether or not to reject a call when the RADIUS server supplies 255.255.255.255 as the framed IP address and the MS does not supply an address.

Product
GGSN
P-GW
SAEGW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > APN Configuration

configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-apn)#

Syntax

radius returned-framed-ip-address 255.255.255.255-policy { accept-call-when-ms-ip-not-supplied | reject-call-when-ms-ip-not-supplied }

default radius returned-framed-ip-address 255.255.255.255-policy

default
Set the policy to its default of rejecting calls when the RADIUS server does not supply a framed IP address and the MS does not supply an address.

{ accept-call-when-ms-ip-not-supplied | reject-call-when-ms-ip-not-supplied }

accept-call-when-ms-ip-not-supplied: Accept calls when the RADIUS server does not supply a framed IP address and the MS does not supply and address.
reject-call-when-ms-ip-not-supplied: Reject calls when the RADIUS server does not supply a framed IP address and the MS does not supply an address.

Usage
Use this command to set the behavior in the APN when the RADIUS server supplies 255.255.255.255 as the framed IP address and the MS does not supply an address.

Example
Use the following command to set the APN to reject calls when the RADIUS server does not supply a framed IP address and the MS does not supply an address:

radius returned-framed-ip-address 255.255.255.255-policy reject-call-when-ms-ip-not-supplied
radius returned-username

Configures the username that is returned in accounting messages. If the username is not available in the Protocol Configuration Options (PCO), the RADIUS returned username is preferred to the constructed username (imsi@apn, msisdn@apn, or outbound username).

### Product
- GGSN
- P-GW
- SAEGW

### Privilege
Security Administrator, Administrator

### Mode
Exec > Global Configuration > Context Configuration > APN Configuration

```
configure > context context_name > apn apn_name
```

Entering the above command sequence results in the following prompt:

```
/context_name>host_name(config-apn)#
```

### Syntax

```
radius returned-username { override-constructed-username | prefer-constructed-username }
```

**default radius returned-username**

```
default
```

The default value for the RADIUS returned-username is prefer-constructed-username. The constructed username (imsi@apn, msisdn@apn) will be used.

**Important:** If the username is available in the PCO, that username will be used regardless of the setting for this command (radius returned-username).

- **override-constructed-username**
  - If the RADIUS server returns a username in the Access-Accept message and that username is not available in the Protocol Configuration Options (PCO), the new username from the RADIUS server will be used.

- **prefer-constructed-username**
  - If the username is not available in the PCO, a constructed username (imsi@apn, msisdn@apn) will be used regardless of the username from the RADIUS server. This is the default.

### Usage

Use this command to configure the username that is returned in accounting messages

### Example

Following command sets the default value for the RADIUS returned-username is prefer-constructed-username [constructed username (imsi@apn, msisdn@apn)]:

```
```

default radius returned-username
restriction-value

Configures the level of restriction to ensure controlled co-existence of the Primary PDP Contexts.

Product

GGSN
P-GW
SAEGW

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > Context Configuration > APN Configuration
configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-apn)#

Syntax

restriction-value value

[ default | no ] restriction-value

default | no

Default: no restriction-value
Entering either default or no restriction-value sets the internal value to zero (0) so that connection to any APN is allowed.

value

Specifies a unique number that identifies the type of network supported for primary PDP contexts facilitated by this APN. The following values are supported:

- 1: Value used for Wireless Application Protocol (WAP) or Multimedia Messaging Service (MMS) type of networks. This corresponds to APN type public-1.
- 2: Value used for Internet or Packet-Switched Public Data Network (PSPDN) type of networks. This corresponds to APN type public-2.
- 3: Value used for corporate customers who use MMS. This corresponds to APN type private-1.
- 4: Value used for corporate who do not use MMS. This corresponds to APN type private-2.

Usage

Restricts the ability to have connections to public access and certain private APNs as required by the APN configuration. Also allows co-existence of the Primary PDP Contexts in a controlled manner.
It does not restrict the total number of Primary PDP Contexts for the user. It also configures a method for preventing hackers in the public domain from using the UE as a router.
Access is provided based on the following rules:

- If value = 1, then PDP contexts with restriction values of 0, 1, 2, and/or 3 are allowed
If \( value = 2 \), then PDP contexts with restriction values of 0, 1 and/or 2 are allowed

If \( value = 3 \), then PDP contexts with restriction values of 0 and/or 1 are allowed

If \( value = 4 \), then PDP contexts with no restriction values are allowed

If \texttt{default} or \texttt{no} syntax is entered, then no PDP contexts have restriction

In the event that a Maximum APN Restriction value is received from the SGSN as part of a PDP Context Create (CPCR) or Update (UPCR) message, the GGSN allows the request based on the following matrix:

- If maximum = 0, then allow connection to any APN
- If maximum = 1, then allow APN Restriction values of 0, 1, 2, and/or 3
- If maximum = 2, then allow APN Restriction values of 0, 1 and/or 2
- If maximum = 3, the allow APN Restriction values of 0 and/or 1
- If maximum = 4, then always reject
- If maximum = anything else, then allow all APN Restriction values (1, 2, 3, and/or 4)

Refer to 3GPP 23.060 version 6.9.0 for more information.

**Example**

The following command sets the restriction value of the APN to 2:

```
restriction-value 2
```
secondary ip pool

This command specifies a secondary IP pool to be used as backup pool for Network Address Translation (NAT).

**Important:** This command is license dependent. For more information please contact your Cisco account representative.

**Product**
NAT

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > APN Configuration

```
configure > context context_name > apn apn_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-apn)#
```

**Syntax**

```
secondary ip pool pool_name

no secondary ip pool
```

- **no**
  - Removes the previous secondary IP pool configuration.

- **pool_name**
  - Specifies the secondary IP pool name.
  - `pool_name` must be an alphanumeric string of 1 through 31 characters.

**Usage**

Use this command to configure a secondary IP pool for NAT subscribers, which is not overwritten by the RADIUS supplied list. The secondary pool configured will be appended to the RADIUS supplied IP pool list / APN provided IP pool list whichever is applicable during call setup.

**Example**

The following command configures a secondary IP pool named `test123`:

```
secondary ip pool test123
```
**selection-mode**

Configures the level of verification that will be used to ensure a mobile station’s subscription to use this APN.

**Product**
- GGSN
- P-GW
- SAEGW

**Privilege**
- Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > APN Configuration

```bash
configure > context context_name > apn apn_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-apn)#
```

**Syntax**

```bash
selection-mode { chosen-by-sgsn | sent-by-ms | subscribed } +
```

**default selection-mode**

```
default
```
Sets the default selection mode as “subscribed”.

```
chosen-by-sgsn
```
Default: Disabled
The MS’s subscription will not be verified and the APN will be provided by the SGSN.

```
sent-by-ms
```
Default: Disabled
The MS’s subscription will not be verified and the APN will be provided by the MS.

```
subscribed
```
Default: Enabled
The MS’s subscription will be verified by the SGSN.

```
+
```
More than one of the above keywords can be entered within a single command.

**Usage**

Use this command to specify the level of verification that will be used to ensure a MS’s subscription to use this APN. This setting must match the corresponding setting on the SGSN. If the two settings are not identical, the GGSN rejects the session with a cause code of 201 (D1H, User authentication failed).
Example

The following command specifies that the MS’s subscription will not be verified and that the APN name will be supplied by the SGSN:

```
selection-mode chosen-by-sgsn
```
timeout

Configures the session timeout values for this APN.

Product
GGSN
P-GW
SAEGW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > APN Configuration

configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-apn)#

Syntax

timeout { absolute | qos-renegotiate } time

[ default | no ] timeout [ absolute | qos-renegotiate ]

default

Set the default value for the followed option.

no

Returns the timeout parameter to its default setting. If neither the absolute or idle keywords are used in conjunction with this keyword, both timeout options will be returned to their default settings.

absolute

Configures the absolute maximum time a session may exist in any state (active or idle).

qos-renegotiate

This keyword is obsolete.

time

Default:

- absolute = 0 (Disabled)
- qos-renegotiation = 300

Measured in seconds, the time can be configured to any integer value between 0 and 4294967295. A time of 0 disables timeouts for this APN.
**Usage**

Use this command to limit the amount of time that a subscriber session can remain connected or as a QoS renegotiation dampening timer.

**Example**

The following commands enable an absolute time timeout of 60000 seconds:

```
timeout absolute 60000
```
timeout bearer-inactivity

This command configures the bearer inactivity timer and the threshold value of the traffic through an APN. The bearer inactivity timer can also be configured to exclude default bearer/primary bearer from monitoring bearer inactivity.

Product
GGSN
P-GW
SAEGW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > APN Configuration
configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-apn)#

Syntax

In StarOS 15.0 and later releases:

```
timeout bearer-inactivity dur_seconds volume-threshold { downlink | total | uplink } bytes
```

```
timeout bearer-inactivity exclude-default-bearer
```

[ default | no ] timeout bearer-inactivity

In StarOS 14.x and earlier releases:

```
timeout bearer-inactivity dur_seconds volume-threshold total bytes
```

[ default | no ] timeout bearer-inactivity

---

**default**

Sets the bearer inactivity timer to disabled mode.

---

**no**

Removes the configured bearer inactivity timer values and traffic threshold limit.

---

**timeout**

Specifies that a bearer time out value will be configured for this APN.

---

**dur_seconds**

Specifies the timeout duration in seconds to check inactivity on the bearer.

In StarOS 15.0 releases:

`dur_seconds` must be an integer value from 900 to 2592000 (15 minutes to 720 hours). The minimum configurable value of bearer inactivity timer was reduced from 3600 seconds to 900 seconds.
In StarOS 14.x and earlier releases:
`dur_seconds` must be an integer value from 3600 through 2592000.

**volume-threshold**
This keyword sets the volume threshold in bytes to check the low activity on the bearer.

**downlink**
Threshold value of the downlink data traffic in a bearer.

**total**
Specifies that the total of both uplink and downlink data will be used as a volume threshold.

**uplink**
Threshold value of the uplink data traffic in a bearer.

**bytes**
`bytes` must be an integer value from 1 through 4294967295.

**exclude-default-bearer**
Ignore bearer inactivity handling for default/primary bearer.

**Usage**
Use this command to configure the bearer inactivity timer and the threshold value of the traffic through an APN. This enables the deletion of bearers experiencing less data traffic than the configured threshold value. Bearer inactivity timer is started only when time and volume threshold is configured.

**Important:** Only one threshold is allowed to be configured per APN which is to monitor total, uplink, or downlink traffic.

The bearer inactivity timer can also be configured to exclude default bearer/primary bearer from monitoring bearer inactivity.

**Example**
The following command enables the inactivity time on the bearer with a timeout duration of 7200 seconds and the total traffic volume of 256000 bytes in uplink and downlink directions as thresholds:

```
timeout bearer-inactivity 7200 volume-threshold total 256000
```
timeout emergency-inactivity

Configures the emergency session inactivity-timeout for this APN. The APN must be configured as an emergency APN for Voice over LTE (VoLTE) E911 support.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > APN Configuration
configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:
[context_name]host_name(config-apn)#

Syntax

timeout emergency-inactivity seconds
[ default | no ] timeout emergency-inactivity

default | no

Indicates the timeout specified is to be returned to its default behavior. If no specific timeout is specified, then all are set to their default behavior.

seconds

Default: 0 (disabled)
Specifies the timeout duration, in seconds, to check inactivity on the emergency session.
seconds must be an integer value from 1 through 3600.

Usage

Use this command to set the emergency session inactivity-timeout for this APN.
At reception of an IP CAN Session Modification Request triggered by the Policy and Charging Rules Function (PCRF) for an IP-CAN (IP Connectivity Access Network) session serving an IMS emergency session that removes all PCC rules with a QCI other than the default bearer QCI and the QCI used for IMS signalling, the Policy and Charging Enforcement Function (PCEF) shall start a configurable inactivity timer (to enable PSAP Callback session). When the configured period of time expires, the PCEF shall initiate an IP-CAN Session Termination Request for the IP-CAN session serving the IMS Emergency session. If a PCRF-Initiated IP-CAN Session Modification Request provides new PCC rule(s) with a QCI other than the default bearer QCI and the QCI used for IMS signalling, the PCEF shall cancel the inactivity timer.
Refer to the emergency-apn command in this chapter for additional information.

Example

The following command sets the emergency inactivity timeout duration to 450 seconds.

    timeout emergency-inactivity 450
timeout idle

Configures the idle timeout duration for the long duration timer associated with a subscriber session.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > APN Configuration

configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-apn)#

Syntax

timeout idle idle_dur

[ default | no ] timeout idle

default | no

Indicates the timeout specified is to be returned to its default behavior. If no specific timeout is specified, then all are set to their default behavior.

idle_dur

Default: 0
Designates the maximum duration of the session (in seconds). After expiry the system considers the session as dormant or idle and terminates the session.
idle_dur must be an integer value in the range from 0 through 4294967295.
The special value 0 disables the timeout specified.

Usage

Use this command to set the idle time duration for subscriber session to determine the dormant session. Refer to the long-duration-action detection and long-duration-action disconnection command in this chapter for additional information.

Example

Following command sets the idle timeout duration to 450 seconds.

    timeout idle 450
timeout idle micro-checkpoint-periodicity

Enables configuration of periodic idle seconds micro checkpoint timer on a per-APN basis.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > APN Configuration

`configure > context context_name > apn apn_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-apn)#
```

**Syntax**

```
timeout idle idle_dur [ micro-checkpoint-periodicity time_in_seconds ]
[ default | no ] timeout idle
```

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>`default</td>
<td>no`</td>
</tr>
<tr>
<td><code>idle_dur</code></td>
<td>Designates the maximum duration of the session (in seconds). After expiry, the system considers the session as dormant or idle and terminates the session. <code>idle_dur</code> must be an integer value in the range from 0 through 4294967295. Default: 0 The special value 0 disables the timeout specified.</td>
</tr>
<tr>
<td><code>micro-checkpoint-periodicity time_in_seconds</code></td>
<td>Configures periodic idle seconds micro checkpoint timer on a per-APN basis. Idle seconds micro checkpoints are sent at the configured regular intervals to the standby chassis; otherwise, they are sent at intervals of 10 seconds, which is the default value. <code>time_in_seconds</code> must be an integer value in the range from 0 through 4294967295. Default: 10</td>
</tr>
</tbody>
</table>

**Important:** Micro-checkpoint-periodicity value should be less than idle timeout value.

**Usage**

Use this command to set the idle time duration and micro-checkpoint-periodicity timer for subscriber session to determine the dormant session.

**Example**
Following command sets the idle timeout duration to 10 seconds and micro-checkpoint-periodicity to 15 seconds.

```
timeout idle 10 micro-checkpoint-periodicity 15
```
timeout long-duration

Configures the long duration timeout and inactivity duration for subscriber sessions.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > APN Configuration

`configure > context context_name > apn apn_name`

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-apn)#`

**Syntax**

```
timeout long-duration ldt_timeout [ inactivity-time inact_timeout ]
```

```
no timeout long-duration
```

**no**

Indicates the timeout specified is to be returned to its default behavior. If no specific timeout is specified then all timeouts are set to their default behavior.

**ldt_timeout**

Default: 0

Designates the maximum duration of the session (in seconds) before the system automatically reports/terminates the session.

Specifies the maximum amount of time (in seconds) before the specified timeout action is initiated.

`ldt_timeout` must be an integer value in the range from 0 through 4294967295.

The special value 0 disables the timeout specified.

**inactivity-time** `inact_timeout`

Specifies the maximum amount of time (in seconds) before the specified session is marked as dormant.

`inact_timeout` must be an integer value in the range from 0 through 4294967295.

The special value 0 disables the inactivity time specified.

**Usage**

Use this command to set the long duration timeout period and inactivity timer for subscriber sessions. Reduce the idle timeout to free session resources faster for use by new requests.

Refer to the `long-duration-action detection` and `long-duration-action disconnection` commands in this chapter for additional information.

**Example**

The following command sets the long duration timeout duration to 300 seconds and the inactivity timer for subscriber session to 45 seconds.
timeout long-duration 300 inactivity-time 45
tpo policy

The Traffic Performance Optimization (TPO) in-line service is not supported in this release.
**tunnel address-policy**

This command specifies the address allocation/validation policy for all tunneled calls (IP-IP, IP-GRE) except L2TP calls. This means that GGSN IP address validation could be disabled for specified incoming calls.

**Product**

GGSN
P-GW
SAEGW

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > APN Configuration

`configure > context context_name > apn apn_name`

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-apn)#`

**Syntax**

```
tunnel address-policy { alloc-only | alloc-validate | no-alloc-validate }
```

default tunnel address-policy

```
default
```

- Resets the tunnel address-policy to alloc-validate.

```
alloc-only
```

- IP addresses are allocated locally and no validation is done.

```
alloc-validate
```

- Default.
The VPN Manager allocates and validates all incoming IP addresses from a static pool of IP addresses.

```
no-alloc-validate
```

- No IP address assignment or validation is done for calls arriving via L3 tunnels. Incoming static IP addresses are passed. This allows for the greatest flexibility.

**Usage**

This command supports scalable solutions for Corporate APN deployment as many corporations handle their own IP address assignments. In some cases this is done to relieve the customer or the mobile operators from the necessity of reconfiguring the range of IP addresses for the IP pools at the GGSN.

For calls coming through L2TP tunnels, the command `l3-to-l2-tunnel address policy` as defined in the APN Configuration mode, will be in effect.

**Example**

This command supports scalable solutions for Corporate APN deployment as many corporations handle their own IP address assignments. In some cases this is done to relieve the customer or the mobile operators from the necessity of reconfiguring the range of IP addresses for the IP pools at the GGSN.
Use the following command to reset the IP address validation policy to validate against a static pool of address:

```
default tunnel address-policy
```

Use the following command to disable all IP address validation for calls coming through tunnels:

```
tunnel address-policy no-alloc-validate
```
tunnel gre

Configures Generic Routing Encapsulation (GRE) tunnel parameters between the GGSN and an external gateway for the APN.

Product
GGSN
P-GW
SAEGW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > APN Configuration

configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-apn)#

Syntax

tunnel gre peer-address peer_address local-address local_addr [ preference num ]

no tunnel gre peer-address peer_address

no

Disables GRE tunneling for the APN.

peer-address peer_address

Specifies the IP address of the external gateway terminating the GRE tunnel.
peer_address must be expressed in dotted decimal notation.

local-address local_addr

Specifies the IP address of the interface in the destination context of the GGSN originating the GRE tunnel.
local_addr must be expressed in IPv4 dotted-decimal notation.

preference num

Default: 1
This option can be used to assign a preference to the tunnel.
preference can be configured to any integer value from 1 to 128.

Important: Only one GRE tunnel per APN is supported. Therefore, the preference should always be set to “1”.

Usage

Subscriber IP payloads are encapsulated with IP/GRE headers and tunneled by the GGSN to an external gateway.
Example

The following command configures the system to encapsulate subscriber traffic using GRE and tunnel it from a local address of 192.168.1.100 to a gateway with an IP address of 192.168.1.225:

```plaintext
tunnel gre peer-address 192.168.1.225 local-address 192.168.1.100 preference 1
```
tunnel ipip

Configures IP-in-IP tunnelling parameters between the GGSN and an external gateway for the APN.

Product
GGSN
P-GW
SAEGW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > APN Configuration
configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-apn) #

Syntax

tunnel ipip peer-address peer_address local-address local_addr [ preference num ]

no tunnel ipip

Disables IP-in-IP tunneling for the APN.

peer-address peer_address
 Specifies the IP address of the external gateway terminating the IP-in-IP tunnel.
 peer_address must be expressed in IPv4 dotted-decimal notation.

local-address local_addr
 Specifies the IP address of the interface in the destination context of the GGSN originating the IP-in-IP tunnel.
 local_addr must be expressed in IPv4 dotted-decimal notation.

preference num
 Default: 1
 If multiple tunnels will be configured, this option can be used to assign a preference to the tunnel.
 preference can be configured to any integer value from 1 to 128.

Usage
 Subscriber IP payloads are encapsulated with IP-in-IP headers and tunneled by the GGSN to an external gateway.

Example
 The following command configures the system to encapsulate subscriber traffic using IP-in-IP and tunnel it from a local address of 192.168.1.100 to a gateway with an IP address of 192.168.1.225:
tunnel i pip peer-address 192.168.1.225 local-address 192.168.1.100 preference 1
tunnel ipsec

This command configures sessions for the current APN to use an Internet Protocol Security (IPSec) tunnel based on the IP pool corresponding to the subscribers assigned IP address.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > APN Configuration

```
configure > context context_name > apn apn_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-apn)#
```

**Syntax**

```
[ no ] tunnel ipsec use-policy-matching-ip-pool
```

<table>
<thead>
<tr>
<th>no</th>
</tr>
</thead>
</table>
| Disables the use of the IPSec policy that matches the IP pool that the assigned IP address relates to.

**Usage**

Use this command to set the APN to use an IPSec policy that is assigned to the IP pool that the subscribers assigned IP address relates to.

**Example**

The following command enables the use of the policy that matches the IP pool address:

```
tunnel ipsec use-policy-matching-ip-pool
```
tunnel l2tp

Configures Layer 2 Tunnelling Protocol (L2TP) parameters between the GGSN and an external gateway for the APN.

**Product**
- GGSN
- P-GW
- SAEGW

**Privilege**
- Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > APN Configuration

```plaintext
configure > context context_name > apn apn_name
```

Entering the above command sequence results in the following prompt:

```
[context_name] host_name(config-apn) #
```

**Syntax**

```plaintext
tunnel l2tp [ peer-address ins-address [ [ encrypted ] secret l2tp_secret ] [ preference num ] [ tunnel-context name ] [ local-address ip-address ] [ crypto-map map_name { [ encrypted ] isakmp-secret crypto_secret } ] [ local-hostname hostname ]

no tunnel [ peer-address ins-address]
```

**no**

Disables L2TP, or secure L2TP tunneling for the APN if a specific peer-address is not specified, or, if a peer-address is specified, this keyword removes the peer-address configuration from the APN.

**peer-address ins-address**

Specifies the IP address of the LNS node that the LAC service connects to.

*ins-address* must be expressed in IPv4 dotted-decimal notation.

---

**Important:** A maximum of four LNS peers can be configured per APN.

**encrypted**

This keyword is intended only for use by the system while saving configuration scripts. The system displays the encrypted keyword in the configuration file as a flag that the variable following the secret keyword is the encrypted version of the plain text secret. Only the encrypted secret is saved as part of the configuration file.

**secret l2tp_secret**

Specifies the shared secret (password) between the L2TP Access Concentrator (LAC) service (configured on the system) and the LNS node.

*l2tp_secret* must be an alphanumeric string of 1 through 127 characters and is case sensitive.
**preference num**

Default: 1

Specifies the preference of the tunnel if the LAC service communicates with multiple LNS nodes. preference can be configured to any integer value from 1 to 128.

**tunnel-context name**

Specifies the name of the destination context on the system in which the LAC service(s) is configured. name must be an alphanumeric string of 1 through 79 characters and is case sensitive.

**Important:** If this option is not configured, the system will attempt to determine the name of the destination context from the ip context-name parameter configured for the APN.

**local-address ip-address**

Specifies the IP address of an interface that is bound to a LAC service. This is a mechanism to dictate which LAC service to use to facilitate the subscriber’s L2TP session.

address is the IP address of the interface in IPv4 dotted-decimal notation.

**Important:** If the address configured does not exist or is not bound to a LAC service, the system will automatically choose a LAC service to use.

**local-hostname hostname**

This keyword configures LAC-Hostname to be used for the communication with the LNS peer for this APN. When Tunnel parameters are not received from the RADIUS server, Tunnel parameters configured in APN are considered for the LNS peer selection. When APN Configuration is selected, local-hostname configured with the “tunnel l2tp” command in the APN for the LNS peer will be used as a LAC Hostname.

**Important:** For this configuration to take effect allow aaa-assigned-hostname command, which is used to configure LAC-Hostname based on the “Tunnel-Client-Auth-ID” attribute received from the RADIUS server, needs to be configured in the LAC Service Configuration mode.

hostname is name of the local host for the LNS peer and must be an alphanumeric string of 1 through 127 characters.

When Tunnel parameters are not received from the RADIUS Server, Tunnel parameters configured in APN will be considered for the LNS peer selection. When APN Configuration is selected, the local hostname hostname configured with this command in the APN for the LNS peer will be used as a LAC Hostname.

**crypto-map map_name { [ encrypted ] secret crypto_secret }**

Configures the IPSec crypto-map policy that is to be associated with this L2TP tunnel configuration for secure L2TP.

map_name is the name of a crypto-map policy configured on the system expressed as an alphanumeric string of 1 through 127 characters and is case sensitive.

encrypted is intended only for use by the system while saving configuration scripts. The system displays the encrypted keyword in the configuration file as a flag that the variable following the secret keyword is the encrypted version of the plain text secret. Only the encrypted secret is saved as part of the configuration file.

secret specifies the secret associated with the crypto-map policy. crypto_secret can be from 0 to 255 bytes.
Usage

This command can be used to configure the GGSN to tunnel subscriber traffic to one or more peer LNSs using L2TP or L2TP with IPSec.

When using L2TP, the system functions as a L2TP access Concentrator (LAC) and tunnels traffic to a peer L2TP Network Server (LNS). LAC functionality is supported through the configuration of LAC Services defined in destination contexts configured on the system.

When using crypto-map policies, the system functions in the same fashion as with L2TP, with the exception that the encapsulated L2TP traffic is further encrypted using IPSec. IPSec functionality is supported through the definition of crypto maps configured in the same destination context as the LAC services.

A maximum of four LNS peers can be configured per APN. If no peer is specified, the system will use the LAC Service(s) configured in the same destination context as the APN.

Example

The following command configures L2TP support for the APN. It configures the APN to tunnel traffic to an LNS with an IP address of 192.168.1.50 through a LAC service bound to an interface with an IP address 192.168.1.201 configured in a destination context on the system called pdn1. The shared secret between the system and the LNS is 5496secRet. This will be the only LNS configured so the default preference of 1 will not be changed.

```
tunnel l2tp peer-address 192.168.1.50 secret 5496secRet tunnel-context pdn1 local-address 192.168.1.201
```
**virtual-apn gdcr**

Defines which APN (Gn or virtual) is used in charging records.

**Product**
- eWAG
- GGSN
- IPSG
- P-GW
- SAEGW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > APN Configuration
`configure > context context_name > apn apn_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-apn)#
```

**Syntax**

```
virtual-apn gcdr apn-name-to-be-included { Gn | virtual }
```

**default virtual-apn gcdr apn-name-to-be-included**

```
default
```

Returns the CDR related parameters to the default values.

```
gcdr apn-name-to-be-included { gn | virtual }
```

Defines which APN is to be sent in charging records (CDR):
- **Gn**: Use the Gn APN name received in the Create PDP Context Request message from SGSN or the S5 APN name received in the PDN Connectivity Request from MME.
- **virtual**: Use the virtual APN selected by the GGSN/P-GW. This is the default.

**Usage**

Defines which APN is to be sent in charging records (CDR), either the APN received in the Create PDP Context Request from the SGSN, or the APN received in the PDN Connectivity Request from the MME.

**Example**
The following command configures the gateway to use the APN supplied by the SGSN or MME.

```
virtual-apn gcdr apn-name-to-be-included gn
```
virtual-apn preference

Defines one or more criteria used to redirect a call received on a particular APN to another APN.

Product
- GGSN
- eWAG
- IPSG
- P-GW
- SAEGW

Privilege
- Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > APN Configuration
configure > context context_name > apn apn_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-apn)#

Syntax

virtual-apn preference priority apn apn_name [ access-gw-address { ip_address | ip_address/mask } | bearer-access-service service_name | cc-profile cc_profile_index [ rat-type { eutran | gan | geran | hspa | utran | wlan } ] | domain domain_name | mcc mcc_number | mnc mnc_number | cc-profile cc_profile_index ] | [ msin-range from msin_range_from to msin_range_to ] | [ rat-type { eutran | gan | geran | hspa | utran | wlan } ] | muisdn-range from misisdn_start_range to misisdn_to_range [ rat-type { eutran | gan | geran | hspa | utran | wlan } ] | roaming-mode { home | roaming | visiting } ]

no virtual-apn preference priority

no

Removes a previously configured “virtual” APN.

preference priority

Specifies the order in which the referenced APNs are compared by the system.
priority specifies the order and can be configured to any integer value from 1 (highest priority) to 1000 (lowest priority).

apn apn_name

Specifies the name of an alternative APN configured on the system that is to be used for PDP contexts or PDN connections with matching properties.
apn_name is the name of the alternative APN expressed as an alphanumeric string of 1 through 62 alphanumeric characters and is case insensitive. It may also contain dots (.) and/or dashes (-).
access-gw-address { ip_address | ip_address/mask }

Specifies the Access Gateway (SGSN/SGW/Other) IP address.

*ip_address* must be an IPv4 address in dotted-decimal or an IPv6 address in colon-separated-hexadecimal notation.

*ip_address/mask* must be an IPv4 address in dotted-decimal or an IPv6 address in colon-separated-hexadecimal notation with network-host mask separation.

bearer-access-service service_name

Specifies the Bearer Access Service (GGSN/P-GW/Other) name. This service name is unique across the context.

*service_name* must be an alphanumeric string of 1 through 63 characters.

For eWAG and IPSG, this option is not supported in this release.

cr-profile cc_profile_index

Specifies the charging characteristics (CC)-profile index.

*cc_profile_index* must be an integer from 1 to 15.

For eWAG and IPSG, this option is not supported in this release.

domain domain_name

Specifies the domain name (realm). This is compared with the domain name portion of subscriber’s username (user@domain).

*domain_name* must be an alphanumeric string of 1 through 79 characters, is case sensitive and can contain all special characters.

For eWAG and IPSG, this option is not supported in this release.

mcc mcc_number mnc mnc_number

**mcc**: Specifies the mobile country code (MCC) portion of the PLMN’s identifier.

*mcc_number* is the PLMN MCC identifier and can be configured to any 3-digit integer value between 100 and 999.

**mnc**: Specifies the mobile network code (MNC) portion of the PLMN’s identifier.

*mnc_number* is the PLMN MNC identifier and can be configured to any 2- or 3-digit integer value between 00 and 999.

For eWAG and IPSG, this option is not supported in this release.

msin-range from msin_range_from to msin_range_to

This option is supported only for the GGSN.

Specifies the IMSI MSIN range.

*msin_range_from* is the start prefix of the IMSI MSIN range and can be configured between 0 and 9999999999.

*msin_range_to* is the end prefix of the IMSI MSIN range and can be configured as a string of size 1 to 10 digits between 0 and 9999999999.

*msin-range* should follow the following rules:

- Start prefix (such as *msin_range_from*) and end prefix (such as *msin_range_from*) must be of the same length.
- Total length of mcc + mnc + msin-range <= 15 digits.
- For a given combination of mcc + mnc + msin-range (start-end prefix), overlapping range is not allowed.
**msisdn-range from msisdn_start_range to msisdn_to_range**

Specifies the MSISDN range.

- **msisdn_start_range** is the starting MSISDN number which is a string of size 2 to 15 and its value ranges between 00 and 999999999999999.
- **msisdn_to_range** is the ending MSISDN number which is also a string of size 2 to 15 and its value ranges between 00 and 999999999999999.

For eWAG, this keyword is not supported in this release.

**rat-type { eutran | gan | geran | hspa | utran | wlan }**

The type of the Radio Access Technology (RAT).

The available options include:

- **eutran**
- **gan**
- **geran**
- **hspa**
- **utran**
- **wlan**

For eWAG, the rat-type keyword is not supported in this release.

**roaming-mode { home | roaming | visiting }**

Supports separate PDP context or PDN connection processing for roaming, visiting, and home subscribers.

For eWAG and IPSG, this option is not supported in this release.

---

**Usage**

This command simplifies the configuration process for mobile operators allowing them to provide subscribers with access to a large number of packet data networks, characterized by APN templates, while only having to configure a small number of APNs on the HLR.

Each “virtual” APN is a reference, or a link, to an alternate APN configured on the system. Each reference is configured with a rule that subscriber PDP contexts or PDN connections are compared against and a priority that dictates the comparison order.

**GGSN**

The references works as follows:

1. A Create PDP Context Request message is received by the GGSN. The message specifies an APN configured in the HLR.
2. The GGSN determines whether its own matching APN configuration contains “virtual” APN references.
3. The system determines the priority of the references and compares the associated information pertaining to the PDP context against the configured rules.
4. If the rule matches, the parameters in the APN specified by the reference are applied to the PDP context. If not, the rules in the reference with the next highest priority are compared against the PDP context. This occurs until a match is found. If none of the references match, then the parameters within the current APN are applied to the PDP context.

The GGSN supports a maximum of 1023 Virtual APN mapping configurations in a system. A single Gn APN can be configured with up to 1000 mapping rules. Multiple Gn APNs are supported - each requiring Virtual APN mapping configurations. The limit imposed is that the total virtual APN mappings across all Gn APNs should not exceed 1023.
The functionality provided by this command can also be used to restrict access to particular APNs. To restrict access based on a particular criteria (domain name, mcc/mnc, etc.), the “virtual” APN reference should refer to an APN that is not configured on the system and contains the desired rule. All calls matching the configured rule would then be denied with a reason code of 219 (DBH), Missing or Unknown APN.

eWAG
For eWAG, in this release only the access-gw-address Virtual APN configuration option is supported. For information on how virtual APN configuration can be used in eWAG deployments, refer to the Enhanced Wireless Access Gateway Administration Guide.

IPSG
For IPSG, in this release only the following Virtual APN configuration options are supported:

• access-gw-address (RADIUS client in the case of IPSG)
• msisdn-range from msisdn_start_range to msisdn_to_range
• rat-type

All these attributes are sent in access-request in Auth-Proxy mode or Acct-Start in other modes to trigger Virtual APN selection.

The functionality provided by this command can also be used to restrict access to particular APNs. To restrict access based on a particular criteria (domain name, mcc/mnc, etc.), the “virtual” APN reference should refer to an APN that is not configured on the system and contains the desired rule. All calls matching the configured rule would then be denied with a reason code of 219 (DBH), Missing or Unknown APN.

P-GW/SAEGW
The Virtual APN feature allows a carrier to use a single APN to configure differentiated services. The APN that is supplied by the MME is evaluated by the P-GW in conjunction with multiple configurable parameters. Then, the P-GW selects an APN configuration based on the supplied APN and those configurable parameters. APN configuration dictates all aspects of a session at the P-GW. Different policies imply different APNs. After basic APN selection, however, internal re-selection can occur based on the following parameters:

• S-GW address: access-gw-address
• Service name: bearer-access-service
• Call control profile index: cc-profile
• Domain name part of username (user@domain): domain
• MCC-MNC of IMSI: mcc mcc_number mnc mnc_number
• MSISDN range: msisdn-range from msisdn_start_range to msisdn_to_range
• Subscriber type: rat-type

In StarOS v12.x and earlier, the P-GW supports a maximum of 1024 Virtual APNs in a system. In StarOS v14.0 and later, the P-GW supports a maximum of 2048 Virtual APNs in a system.

The functionality provided by this command can also be used to restrict access to particular APNs. To restrict access based on a particular criteria (domain name, mcc/mnc, etc.), the “virtual” APN reference should refer to an APN that is not configured on the system and contains the desired rule. All PDN connections matching the configured rule would then be denied with a reason code of 219 (DBH), Missing or Unknown APN.

Example
The following commands configure two “virtual” APNs, priority 1 references the bigco APN with a domain rule of bigco.com, priority 2 references the bigtown APN with a mobile country code rule of 100 and a mobile network code rule of 50.

```
virtual-apn preference 1 apn bigco domain bigco.com
virtual-apn preference 2 apn bigtown mcc 100 mnc 50 msin-range from 4000000000 to 4999999999
```
virtual-apn preference 3 apn bigco.com access-gateway-address
192.168.62.2

virtual-apn preference 4 apn bigco.co.kr access-gateway-address
192.168.60.2/24
Chapter 24
APN Profile Configuration Mode

The APN Profile configuration mode defines a set of parameters controlling the SGSN or MME behavior when a specific APN is received or no APN is received in a Request. An APN profile is a key element in the Operator Policy feature and an APN profile is not used or valid unless it is associated with an APN and this association is specified in an operator policy (see the Operator Policy Configuration Mode Commands).

Essentially, an APN profile is a template that consists of a set of APN-specific commands that may be applicable to one or more APNs. When a subscriber requests an APN that has been identified in a selected operator policy, the set of commands in the associated APN profile will be applied. The same APN profile can be associated with multiple APNs and multiple operator policies.

The SGSN and the MME each support a total of 1,000 APN profile configurations per SGSN/MME; up to 50 APN profiles can be associated with a single operator policy. For additional SGSN limit information, refer to Engineering Rules in the SGSN Administration Guide.

Mode

Exec > Global Configuration > APN Profile Configuration

configure > apn-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(apn-profile-profile_name)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
address-resolution-mode

Identifies the address resolution mode for this APN profile. This command is specific to the SGSN.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > APN Profile Configuration

`configure > apn-profile profile_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(apn-profile-profile_name)#
```

**Syntax**

```
address-resolution-mode { fallback-for-dns | local }
```

**default address-resolution-mode**

```
default
```

Resets the configuration to the default value, that is, `fallback-for-dns`.

```
fallback-for-dns
```

Instructs the system to try DNS resolution. If the DNS query fails, the SGSN will use locally configured addresses, if they have been configured. The `pgw-address` configured under `apn-profile` will be treated as fallback for `dns-address` and will be used only after `dns` failure.

Default: enabled

```
local
```

Instructs the system to only use locally configured addresses and not to use DNS query.

Default: disabled

**Usage**

Use this command to specify the DNS query or local address resolution for this APN profile.

**Example**

The following command sets the address resolution mode to use local addresses *only if* the DNS query fails:

```
address-resolution-mode fallback-for-dns
```
**apn-resolve-dns-query**

Command enables the SGSN to send Straightforward Name Authority Pointer (SNAPTR) type DNS query for APN resolution on a per APN basis.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > APN Profile Configuration
configure > apn-profile profile_name
Entering the above command sequence results in the following prompt:

```
[local]host_name(apn-profile-profile_name)#
```

**Syntax**

```
apn-resolve-dns-query snaptr
remove apn-resolve-dns-query snaptr
```

```
remove

Removes the DNS SNAPTR function from the configuration.
```

**Usage**

SNAPTR filters based on the EPC-capability of the user equipment (UE). Use this command to enable SNAPTR type DNS query for APN resolution for 3G subscribers with EPC subscription. Configuration in this mode promotes control of this feature per APN. By default, this functionality is not enabled.

**Example**

Enable the SGSN to select a PGW during APN resolution:

```
apn-resolve-dns-query snaptr
```
associate sgw-paging-profile

This command allows the association of an SGW Paging Profile with an APN profile on the S-GW.

**Product**
S-GW

**Privilege**
Administrator, Security Administrator

**Mode**
Exec > Global Configuration > APN Profile Configuration

```configuration
configure > apn-profile profile_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(apn-profile-profile_name)#
```

**Syntax**

```plaintext
[ remove ] associate sgw-paging-profile three-tuple
```

- **remove**
  Removes the S-GW Paging Profile from the APN Profile.

- **associate sgw-paging-profile three-tuple**
  Associates an SGW Paging Profile with an APN profile on the S-GW. S-GW Paging Profiles are configured in Global Configuration Mode with the `sgw-paging-profile three-tuple` command.

**Usage**

Use this command to associate an S-GW paging profile with an APN profile on the S-GW.

**Example**

This example associates an S-GW paging profile with an APN profile on the S-GW.

```plaintext
associate sgw-paging-profile three-tuple
```
**CC**

Configures the charging characteristics (CC) for this APN profile.

**Product**
- SGSN
- S-GW
- SAEGW

**Privilege**
- Security Administrator, Administrator

**Mode**

Exec > Global Configuration > APN Profile Configuration

```
configure > apn-profile profile_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(apn-profile-profile_name)#
```

**Syntax**

```
cc { local-value-for-scdrs behavior bit_value profile index_bit | prefer { hlr-value-for-scdrs | local-value-for-scdrs } }
```

```
remove cc { local-value-for-scdrs | prefer }
```

---

**remove**

Removes the charging characteristics configuration from this APN profile.

```
local-value-for-scdrs behavior bit_value profile index_bit
```

Sets the value of the behavior bits and profile index for the charging characteristics for S-CDRs locally, when the Home Location Register (HLR) does not provide these values.

If the HLR provides the charging characteristics with behavior bits and profile index, and the operator wants to ignore what the HLR provides, then specify the `prefer local-value-for-scdrs` keyword with this command.

- `bit_value`: must be a hexadecimal value between 0x0 and 0xFFF.
- `index_bit`: must be an integer from 1 through 15.

Some of the index values are predefined according to 3GPP standard:

- *1* for hot billing
- *2* for flat billing
- *4* for prepaid billing
- *8* for normal billing

Defaults: `bit_value = 0x0; index_bit = 8`

```
prefer { hlr-value-for-scdrs | local-value-for-scdrs }
```

Specify what charging characteristic settings the system will use for S-CDRs.
• **hlr-value-for-scdrs**: instructs the system to use charging characteristic settings received from the HLR for S-CDRs.

• **local-value-for-scdrs**: instructs the profile preference to only use locally configured/stored charging characteristic settings for S-CDRs.

Default: *hlr-value-for-scdrs*

---

### Usage

Use this command to specify the charging characteristic for S-CDRs -- either from the HLR or locally from the SGSN.

These charging characteristics parameters for S-CDRs and M-CDRs are also configurable in the Call-Control Profile configuration mode. When CC parameters are specified in both types of profiles, then:

- For generation of M-CDRs, the parameters configured in the Call-Control Profile configuration mode will take precedence.

- For generation of S-CDRs, the parameters configured in the APN Profile configuration mode will take precedence.

### Example

The following command configures the APN profile to instruct the SGSN not to use charging characteristic settings received from the HLR for S-CDR generation:

```
cc prefer hlr-value-for-scdrs
```
**dedicated-bearers**

Configures the MME to either accept or reject dedicated GBR and Non-GBR bearers.

**Product**
MME

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > APN Profile Configuration
```
configure > apn-profile profile_name
```
Entering the above command sequence results in the following prompt:
```
[local]host_name(apn-profile-profile_name)#
```

**Syntax**
```
dedicated-bearers { gbr { accept | reject } | non-gbr { accept | reject } }  
[ remove ] dedicated-bearers { gbr | non-gbr }
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>dedicated-bearers</strong></td>
<td>Configures the MME to accept or reject dedicated GBR and Non-GBR bearers.</td>
</tr>
<tr>
<td><strong>remove</strong></td>
<td>Removes the configuration, returning the system to the default setting where the MME accepts GBR or Non-GBR dedicated bearers.</td>
</tr>
<tr>
<td><strong>gbr</strong> { accept</td>
<td>reject }</td>
</tr>
<tr>
<td><strong>non-gbr</strong> { accept</td>
<td>reject }</td>
</tr>
</tbody>
</table>

**Usage**
The MME differentiates GBR and Non-GBR dedicated bearers as follows: GBR Bearers - QCI value ranges from 1 to 4; Non-GBR bearers - QCI value ranges from 5-9.
In the case of a UE-initiated Bearer Resource Allocation Reject, the ESM cause “EPS QOS not accepted” is used and the corresponding bearer allocation reject MME statistic is incremented.
In the case of a Create Bearer Request Reject, the EGTP cause “Service denied” is used and the corresponding EGTP statistic is incremented.
**Note:** Handling of multiple bearers in a Create Bearer request from S-GW for Partial accept/reject of GBR/Non-GBR dedicated bearers is a current limitation.

**Example**
The following commands configure the MME to reject both GBR and Non-GBR dedicated bearers:
```
dedicated-bearers gbr reject

dedicated-bearers non-gbr reject
```
description

Defines a descriptive string relevant to the specific APN profile.

Product

MME
SGSN
S-GW
SAEGW

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > APN Profile Configuration

configure > apn-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(apn-profile-profile_name)#

Syntax

description description

remove description

remove

Removes the configured description from this APN profile.

description

Specifies a description for this APN profile as an alphanumeric string of 1 through 100 characters. The string may include spaces, punctuation, and case-sensitive letters if the string is enclosed in double quotation marks (").

Usage

Define information that identifies this particular APN profile.

Example

Indicate that APN profile apnprof1 is to be used for customers in Saudi Arabia and that the profile was created on April 10th of 2010:

description “apnprof1 defines APNs for customers in Saudi Arabia (4/10/10).”
**direct-tunnel**

Defines the permission for direct tunnel establishment by GGSNs. This command is specific to the SGSN.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > APN Profile Configuration

```
configure > apn-profile profile_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(apn-profile-profile_name)#
```

**Syntax**

```
direct-tunnel not-permitted-by-ggsn
remove direct-tunnel
```

---

**remove**

Removes the direct tunnel establishment configuration from this APN profile.

---

**not-permitted-by-ggsn**

Specifies that a direct tunnel is not permitted by the GGSN when resolved by this APN.

Default: disabled.

---

**Usage**

Use this command to enable/disable the permission for establishment of direct tunnels between an RNC and a GGSN.

**Example**

The following command instructs the SGSN not to permit establishment of a direct tunnel with a GGSN:

```
direct-tunnel not-permitted-by-ggsn
```

dns-extn

Takes an offset group of digits from the MSISDN and appends the digits to the DNS query string to create a new APN intended to assist roaming subscribers to use the local GGSN.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > APN Profile Configuration
configure > apn-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(apn-profile-profile_name)#

Syntax

dns-extn { charg-id { binary | decimal | hexadecimal } | lac-rac | msisdn start-offset start_digits end-offset end-digits | rnc-id [ charg-id { binary | decimal | hexadecimal } ] }
remove dns-extn { charg-id | lac-rac | msisdn | rnc-id [ charg-id ] }

charg-id { binary | decimal | hexadecimal }

Instructs the SGSN to take the profile index value of the charging characteristics, from the PDP subscription record (selected during APN selection) and include the profile index value in the APN name prior to sending out DNS queries. The operator can also specify the format (binary, decimal or hexadecimal) for the CC information to be included.

lac-rac

Enables the SGSN to append geographical information to the APN string that is being sent in the DNS query. This information is used during the DNS query process to select the geographically closest GGSN.

msisdn start-offset start_digits end-offset end-digits

Defines an offset group of digits from the MSISDN and appends the digits to create a new APN DNS query string that is intended to assist roaming subscribers to use the local GGSN.

• start_digits is an integer from 1 through 14 that identifies the position of the first digit in the MSISDN to start the offset.

• end_digits is an integer from 2 through 15 that identifies the position of the last digit in the MSISDN to be part of the offset.

rnc-id [ charg-id { binary | decimal | hexadecimal } ]

Instructs the SGSN to include the ID of the calling RNC in the APN DNS query string. Optionally, the profile index value of the charging characteristics can be inserted into the APN name prior to sending out DNS queries. As well, the operator can specify the format (binary, decimal or hexadecimal) for the CC information to be included.
Usage

With this command, the APN in the DNS query string, used for querying the GGSN address, can be appended with additional information, such as

- digits from the MSISDN
- LAC/RAC info
- RNC-ID
- profile index from the charging characteristics information (SCHAR)

This additional information allows some customization of the DNS query string to facilitate selecting a specific (usually local or nearest) GGSN.

For example, roaming subscribers using a specific APN may want to be directed to a specific GGSN. This can be achieved by having an operator policy for roaming subscribers associated with an APN profile that includes a configuration specifying certain digits, from the MSISDN or geographical information from the LAC/RAC, be appended to the APN. This is then used as the DNS query string.

In addition, the operator must configure appropriate DNS entries to enforce the selection of the required GGSN. After appending the MSISDN digits to the DNS query string, the string will have the form:

\[ \text{ni.<digits>}.mnc*.mcc*.gprs \]

After appending the LAC/RAC information to the DNS query string, the string will have the form:

\[ <\text{apn_network_id}>.\text{racAAAA.lacBBBB}.<\text{apn_operator_id}> \]

where the AAAA and BBBB are Hex-coded digits (less than 4 significant digits and one or more zero (“0”) digits will be inserted to the left side of the Hex to fill the 4-digit coding).

After appending the charging characteristic (SCHAR) information, the DNS string will take the following form:

\[ <\text{apn_network_id}>.<\text{profile_index}>.<\text{apn_operator_id}> \]

The profile index in the following example has an integer value 10:

\[ \text{quicknet.com.uk.1010.mnc234.mcc027.gprs} \]

If the RNC-ID information is configured to be a part of the APN name, and if inclusion of the profile index of the charging characteristics information is also enabled before the DNS query is sent, the profile index is included after the included RNC-ID and the DNS APN name will appear in the following form:

\[ <\text{apn_network_id}>.<\text{rnc_id}>.<\text{profile_index}>.<\text{apn_operator_id}> \]

Once the DNS extension is defined, the selected extension is applicable when either the wildcard APN feature or the default APN feature are configured and used.

The information is appended to the DNS query and the actual APN string sent to the GGSN will not be modified in any way.

Example

A sample MSISDN is ‘112233445566778’ and a sample APN NI (network identifier) is ‘wap98.testnetz.ca’.

The following command instructs the SGSN to create a new APN with digits pulled from the MSISDN and appended to the APN:

\[ \text{msisdn start-offset 3 end-offset 9} \]

The resulting APN DNS query string would have appended 7 digits (2233445) to the APN NI so that it would appear something like \text{wap98.testnetz.ca.2233445.MNC009.MCC262.GPRS}.

Enable inclusion of geographical information in the APN string used for the DNS query to locate the closest GGSN:

\[ \text{lac-rac} \]

In the following example, the DNS query for a subscriber using RNC 0321 with the profile index of value 8 would appear as:

\[ \text{quicknet.com.uk.0321.1000.mnc234.mcc027.gprs} \]
end

Exits the current configuration mode and returns to the Exec mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

end

**Usage**

Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Use this command to return to the parent configuration mode.
gateway-address

Configures the IPv4 or IPv6 address of the GGSN supporting the APN associated with this APN profile. Also, use this command to create a secondary pool of GGSNs. This command is specific to the SGSN.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > APN Profile Configuration
configure > apn-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(apn-profile-profile_name)#

Syntax

gateway-address ip_address { priority priority | weight weight [ secondary-pool ] }

no gateway-address ip_address

no
Disables the GGSN address configured in this APN profile.

ip_address
Specifies the IP address for the GGSN in IPv4 dotted-decimal or IPv6 colon-separated notation.

priority priority
Specifies the priority, for the configured GGSN address, to be considered during address selection. If the highest priority GGSN fails to respond, the next priority level GGSN is selected. priority is an integer from 1 through 100. Note that the lower integer has the higher priority, so that 1 is the highest priority.

weight weight [ secondary-pool ]
Specifies the weight (preference) assigned to a GGSN to facilitate load balancing. weight is an integer from 1 to 100 where 1 is the least preferred and 100 is the most preferred.
If a weight is assigned to an address, then load balancing (of primary CPC requests) depends on the weight value. For example:

GGSN1 172.16.130.1 weight 30 and GGSN2 172.16.130.3 weight 70

With this configuration, 30% of the activation requests for this APN will go to GGSN1 and 70% of the requests will go to GGSN2. Also note that the sum of the weights does not need to be 100. The calculation of weight percentiles is carried out proportionately, so the following configuration will also yield the same 30% - 70% results:

GGSN1 172.16.130.1 weight 6 and GGSN2 172.16.130.3 weight 14
**secondary-pool**

This optional keyword allows the operator to enable multiple GGSN pools by assigning the GGSN to a secondary pool of GGSNs. The selection algorithm for GGSNs in a secondary pool is weight-based.

**Usage**

Use this command to define priority or load balancing to be applied during GGSN selection. A maximum of 16 GGSN address can be configured for this APN profile. Also use this command to setup GGSN pools - primary and secondary pools with up to 16 GGSNs in each pool. By default, GGSNs will always be selected from the primary pool. However, working in tandem with the `ggsn-fail-retry-timer` command configuration (SGTP service configuration mode) which enables the local DNS feature, some of the primary GGSNs can be temporarily blacklisted if they become unavailable or overburdened.

**Example**

Set a GGSN address with a secondary priority level:

```
  gateway-address 123.123.123.2 priority 2
```

Add a GGSN to the secondary GGSN pool and define selection weighting of 7th:

```
  gateway-address 198.168.138.8 weight 7 secondary-pool
```
gtp

Enables or disables the GTPC private extension for the Overcharging Protection feature. This command is specific to the SGSN.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > APN Profile Configuration

configure > apn-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(apn-profile-profile_name)#

Syntax

[ remove ] gtp private-extension loss-of-radio-coverage send-to-ggsn [ send-to-peer-sgsn ]

remove
Disables the inclusion of the GTPC private extension, thereby disabling the Overcharging Protection feature.

private-extension loss-of-radio-coverage send-to-ggsn
Instructs the SGSN to set a proprietary GTPC private extension (in the LORC Intimation IEs) in the event of loss of radio coverage (LORC). These private extensions are only understood by a GGSN with an Overcharging Protection license.
The mandatory loss-of-radio-coverage send-to-ggsn keyword set instructs the SGSN to forward the private extension flag to the GGSN in the event of a loss of radio coverage (LORC).

send-to-peer-sgsn
This optional keyword instructs the SGSN to also forward the LORC private extension to the peer SGSN.

Usage
gtp private-extension is one of the two commands required to enable the Overcharging Protection feature. The second command sets the RANAP cause code in the Iu Release to enable the SGSN to detect the LORC state of the MS/UE. This second command is configured in the IuPS service and is explained in the IuPS Service Configuration Mode chapter.

When there is a loss of coverage and the Overcharging Protection feature is enabled with the gtp private-extension command, the SGSN includes the proprietary private extension in the GTP LORC Intimation IE messages. This LORC IE is also included in UPCQ, DPCQ, and SGSN Context Response GTP messages. Refer to the SGSN Administration Guide for additional information regarding the Overcharging Protection feature.

Example
Use the following command to have the SGSN send the GGSN the GTPC private extension in the LORC Intimation IE:
gtp private-extension loss-of-radio-coverage send-to-ggsn
idle-mode-acl

Configures a group of access control lists (ACLs) that define rules to apply to downlink data destined for UEs in an idle mode.

**Product**
- S-GW
- SAEGW

**Privilege**
- Administrator

**Mode**
- Exec > Global Configuration > APN Profile Configuration
- `configure > apn-profile profile_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(apn-profile-profile_name)#
```

**Syntax**

```
[ remove ] idle-mode-acl { ipv4 | ipv6 } access-group acl_name
```

- **remove**
  - Removes the specified ACL name from the access group.

- `{ ipv4 | ipv6 } access-group acl_name`
  - Specifies the ACL type to add to the access group.
    - **ipv4**: Specifies that an IPv4 ACL is being added to the access group.
    - **ipv6**: Specifies that an IPv6 ACL is being added to the access group.

- `access-group acl_name` specifies the name of the ACL being added to the access group as an existing IPv4 or IPv6 ACL name expressed as an alphanumeric string of 1 through 47 characters.

**Usage**

Use this command to create a group of ACLs that contain rules to apply to data sent to UEs that are currently in idle mode.

IPv4 ACLs are configured through the Context Configuration Mode using the `ip access-list` command.

IPv6 ACLs are configured through the Context Configuration Mode using the `ipv6 access-list` command.

**Example**

The following command configures the APN profile to use an IPv4 ACL named `acl-3-permit` to apply rules to downlink data sent to UEs that are currently in idle mode:

```
idle-mode-acl ipv4 access-group acl-3-permit
```
**ip**

Defines the IP parameters for this APN profile.

**Product**
- SGSN
- S-GW
- SAEGW

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > APN Profile Configuration

```
configure > apn-profile profile_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(apn-profile-profile_name)#
```

**Syntax**

```
ip { qos-dscp { { downlink | uplink } { background forwarding | conversational forwarding | interactive traffic-handling-priority priority forwarding | streaming forwarding } + } | source-violation { deactivate [ all-pdp | exclude-from accounting | linked-pdp | tolerance-limit ] | discard [ exclude-from-accounting ] | ignore } default ip { qos-dscp { downlink | uplink } | source-violation }

no ip qos-dscp { downlink | uplink } { background | conversational | interactive | streaming } +
```

---

**Important:** All parameters not specifically configured will be included in the configuration with default values.

---

**default**

Resets the configuration to the default values.

**no**

Disables the specified IP QoS-DSCP mapping.

**qos-dscp**

Configures the Differentiated Services Code Point (DCSP) marking to be used for sending packets of a particular 3GPP QoS class.

**downlink | uplink**

Configures the packets for either downlink (network to subscriber) or uplink (subscriber to network) direction. downlink and uplink configuration must include one or more of the following:

- **background** - Configures the DSCP marking to be used for packets of sessions subscribed to 3GPP background class. Must be followed by a DSCP marking
• **conversational** - Configures the DSCP marking to be used for packets of sessions subscribed to 3GPP conversational class. Must be followed by a DSCP marking.

• **interactive** - Configures the DSCP marking to be used for packets of sessions subscribed to different traffic priorities in the 3GPP interactive class. Must be followed by a traffic handling priority (THP): 1, 2, or 3.

• **streaming** - Configures the DSCP marking to be used for packets of sessions subscribed to 3GPP streaming class. Must be followed by a DSCP marking.

---

**DSCP marking options**

Downlink and uplink must include a DSCP forwarding marking; supported options include:

- af11 - Designates use of Assured Forwarding 11 PHB
- af12 - Designates use of Assured Forwarding 12 PHB
- af13 - Designates use of Assured Forwarding 13 PHB
- af21 - Designates use of Assured Forwarding 21 PHB
- af22 - Designates use of Assured Forwarding 22 PHB
- af23 - Designates use of Assured Forwarding 23 PHB
- af31 - Designates use of Assured Forwarding 31 PHB
- af32 - Designates use of Assured Forwarding 32 PHB
- af33 - Designates use of Assured Forwarding 33 PHB
- af41 - Designates use of Assured Forwarding 41 PHB
- af42 - Designates use of Assured Forwarding 42 PHB
- af43 - Designates use of Assured Forwarding 43 PHB
- be - Designates use of Best Effort forwarding PHB
- ef - Designates use of Expedited Forwarding PHB

Forwarding defaults for both uplink and downlink are:

- conversational - ef;
- streaming - af11;
- interactive 1 - ef;
- interactive 2 - af21;
- interactive 3 - af21;
- background - be

---

**source-violation**

Configures settings related to IP source-violation detection with one of the following criteria:

- **deactivate** - deactivate the PDP context with one of the following conditions:
  - all-pdp - deactivates all PDP context of the MS/UE. Default is to deactivate errant PDP contexts.
  - exclude-from-accounting - excludes packets having an invalid source IP address from the statistics used in the accounting records.
- **linked-pdp** - deactivate all associated pdp contexts (primary and secondary). Default is to deactivate errant pdp context.

- **tolerance-limit** - Configures maximum number of allowed IP source violations before the session is deactivated.

- **discard** - discard errant packets, can include the following option:
  - **exclude-from-accounting** - excludes packets having an invalid source IP address from the statistics used in the accounting records.

- **ignore** - ignore checking of packets for MS/UE IP source violation.

---

### Usage

This command configures a range of IP functions to be associated with the APN profile; such as:

- SGSN/S-GW action in response to detected IP source violations,
- DSCP marking for downlink and uplink configuration per traffic class,
- QoS class diffserv code.

### Example

The following command configures the APN profile to instruct the SGSN or S-GW not to check incoming packets for IP source violation information:

```
    ip source-violation ignore
```
isr-sequential-paging

Enables or disables the Intelligent Paging for ISR feature.

Product
S-GW
SAEGW

Privilege
Administrator

Mode
Exec > Global Configuration > APN Profile Configuration
configure > apn-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(apn-profile-profile_name)#

Syntax

[ remove ] isr-sequential-paging

remove
Disables Intelligent Paging for ISR.

Usage
This command initiates the Intelligent Paging for ISR feature for the specified APN Profile, where paging occurs first towards the last known RAT, then towards the other RAT. The Intelligent Paging for ISR feature is license dependant. Contact your Cisco account representative for more information.
ntsr

This command configures QCI and ARP in the apn-profile for Network Triggered Service Restoration (NTSR).

**Product**
S-GW

**Privilege**
Administrator, Security Administrator

**Mode**
Exec > Global Configuration > APN Profile Configuration

```
configure > apn-profile profile_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(apn-profile-profile_name)#
```

**Syntax**

```
ntsr { all | qci number arp-priority-watermark number }
```

```no ntsr all
no ntsr qci number arp-priority-watermark number
```

- **no**
  - Removes the specified configuration parameters.

- **ntsr**
  - Enables the network triggered service restoration configuration.

- **all**
  - Specifies that the NTSR configuration is enabled for all bearers with any qci or arp for MME restoration.

- **qci**
  - Specifies the Quality of Class Identifier for this NTSR configuration. Must be an integer from 1 to 255.

- **arp-priority-watermark**
  - Specifies the ARP’s prority level watermark value. Must be an integer from 1 to 15.

**Usage**

This command configures qci and arp in the apn-profile for NTSR. The S-GW will decide to retain or release the bearer based on the configured qci/arp, after path failure is detected on ingress side of S-GW. The S-GW can configure a maximum of 2 qci and arp-priority-watermark per apn-profile. The apn-profile can also be configured to retain all bearers from that PDN.

**Example**

This example configures the apn-profile to retain all bearers from the PDN.
ntsr all
overcharge-protection

Enables overcharge protection for APNs controlled by this APN profile. Each overcharging protection option is a standalone configuration and it does not override the previous option set, if any.

**Product**

S-GW
P-GW

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > APN Profile Configuration

configure > apn-profile profile_name

Entering the above command sequence results in the following prompt:

```
[local]host_name(apn-profile-profile_name)#
```

**Syntax**

```
overcharge-protection { abnormal-s1-release | ddn-failure | drop-limit drop_limit_value { packets | bytes } }

[ remove ] overcharge-protection { abnormal-s1-release | ddn-failure | drop-limit }
```

**remove**

Removes the specified configuration.

**abnormal-s1-release**

(for future use) If overcharging protection is enabled for abnormal-s1-release, S-GW would send MBR to pause charging at P-GW if Abnormal Release of Radio Link signal occurs from MME.

**Important:** Though the command is available in this release, this scenario is not possible.

**ddn-failure**

If overcharging protection is enabled for ddn-failure message, MBR would be sent to P-GW to pause charging upon receiving DDN failure from MME/S4-SGSN.

**drop-limit drop_limit_value { packets | bytes }**

Send MBR to pause charging at P-GW if specified number of packets/bytes is dropped for a PDN connection. *drop_limit_value* is an integer from 1 through 99999.

- **packets:** Configures drop-limit in packets.
- **bytes:** Configures drop-limit in bytes.
Usage

Use this command to specify P-GW to pause charging on abnormal-s1-release, DDN failure notification, or if the number of packets or bytes dropped exceeds the configured limit.

Example

Use the following command to signal P-GW to pause charging when the number of packets dropped exceeds 1000:

```
overcharge-protection drop-limit 1000 packets
```
pdp-data-inactivity

Configures the APN profile regarding PDP data inactivity. This command is specific to the SGSN.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > APN Profile Configuration

configure > apn-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(apn-profile-profile_name)#

Syntax

pdp-data-inactivity { action { deactivate [ all-pdp | linked-pdp ] | detach-when { all-pdp-inactive | any-pdp-inactive } } | timeout minutes minutes }

default pdp-data-inactivity { action | timeout }

no pdp-data-inactivity timeout

default

Resets the APN Profile configuration to the default values for PDP data-inactivity.

no

Disables the timeout feature of the PDP data-inactivity configuration for this APN profile.

action

Defines the action to be taken if PDP data-inactivity occurs:

• deactivate - defines which PDP context should be deactivated:
  • all-pdp - deactivates all PDP contexts.
  • linked-pdp - deactivates only linked PDP contexts.

• detach-when - defines the condition that warrants a detach:
  • all-pdp-inactive - detach when all PDP contexts are inactive.
  • any-pdp-inactive - detach when any PDP context is inactive.

timeout minutes minutes

Specifies the inactivity timeout in minutes. minutes: is an integer from 1 through 1440. Note that even though the timeout is set for minutes, the configuration displays in seconds.
**pdp-data-inactivity**

**Usage**

Use this command to define how the SGSN will handle a situation where the PDP is not fully active. Repeat the command, as needed, to configure more than one keyword-controlled function.

**Example**

Use the following command to have the SGSN deactivate all PDP contexts associated with the APN when it detects the PDP is inactive:

```
pdp-data-inactivity action deactivate all-pdp
```

Use the following command to have the SGSN wait 2 minutes after detecting PDP data inactivity:

```
pdp-data-inactivity timeout minutes 2
```
pdp-type-ipv4v6-override

Configure the PDP type to use, per APN, if dual PDP type addressing is not supported by the network and the MS/UE requests the IPv4v6 PDP type.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > APN Profile Configuration
configure > apn-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(apn-profile-profile_name)#

Syntax

pdp-type-ipv4v6-override { ipv4 | ipv6 }

remove pdp-type-ipv4v6-override

removes the override configuration and reverts to the default behavior so the SGSN ignores the IPv4v6 request and sends IPv4 to the GGSN.

ipv4

Configures IPv4 as the PDP type to send towards the GGSN when overriding the dual PDP type addressing requested by the MS/UE.

ipv6

Configures IPv6 as the PDP type to send towards the GGSN when overriding the dual PDP type addressing requested by the MS/UE.

Usage

This command configures the SGSN to send either IPv4 or IPv6 towards the GGSN when the MS/UE requests PDP type as IPv4v6 but either the SGSN or the RNC is not configured to support dual PDP type.

Example

Use this command to configure the SGSN to always send IPv6, for the PDP type, to the GGSN when overriding a dual PDP type address request from the MS/UE:

    pdp-type-ipv4v6-override ipv6
pgw-address

Configures the IPv4 or IPv6 address of the P-GW supporting the APN associated with this APN profile.

**Product**
- ePDG
- MME
- SGSN

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > APN Profile Configuration
`configure > apn-profile profile_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(apn-profile-profile_name)#
```

**Syntax**

```
pgw-address ip_address [ s5-s8-protocol pmip ] [ weight weight ]
nop gw-address ip_address
```

- `no` Disables the P-GW address configured in this APN profile.
- `ip_address` Specifies the IP address for the P-GW in IPv4 dotted-decimal or IPv6 colon-separated notation.
- `s5-s8-protocol pmip` *MME only.* Configures the S5-S8 protocol for the gateway.
- `weight weight` Specifies the weight (preference) assigned to the addressed P-GW for load balancing. `weight` is an integer from 1 through 100 where 1 is the least preferred and 100 is the most preferred. If no weight is specified, the P-GW address is assigned a default weight of 1. If a weight is assigned to an address, the weights of the P-GW(s) (that are operational) are totaled, and then a weighted round-robin selection is used to distribute new primary PDP contexts (for MME) or primary CPC requests (for SGSN) or new PDN connections (for ePDG) among the P-GW(s) according to their weights. As with all weighted round-robin algorithms, the distribution does not look at the current distribution, but simply uses the weights to distribute new requests. For example, two P-GWs assigned weights of 70 and 30 would distribute 70% of calls to one, and 30% to the other. The sum of all weights do not need to total 100.

**Usage**

Use this command to define load balancing to be applied during P-GW selection. A maximum of 16 P-GW addresses can be configured for this APN profile.
On the S4-SGSN, use this command to configure a local P-GW address for operators wishing to bypass DNS resolution of APN FQDN.

**Example**

The following command configures the P-GW IP address for this APN profile as 10.2.3.4:

```
pgw-address 10.2.3.4
```
qos apn-ambr

Configures the APN-AMBR (aggregate maximum bit rate) that will be stored in the Home Subscriber Server (HSS).

Product
MME

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > APN Profile Configuration

configure > apn-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(apn-profile-profile_name)#

Syntax

qos apn-ambr max-ul mbr-up max-dl mbr-dwn

remove qos apn-ambr

remove

Removes the APN-AMBR changes from the configuration for this APN profile.

max-ul mbr-up max-dl mbr-dwn

Defines the maximum bit rates for uplink (subscriber to network) and downlink (network to subscriber) traffic.

mbr-up is an integer from 0 through 1410065408.

mbr-dwn is an integer from 0 through 1410065408.

Usage

Use this command to define the MBR that will be enforced by the GGSN or P-GW for both uplink and downlink traffic shaping.

Example

  qos apn-ambr max-ul 24234222 max-dl 23423423
qos class

Configures local values for the traffic class (TC) parameters for the quality of service (QoS) configured for this APN profile.

Important: To enable any of the values/features configured with this command, the qos prefer-as-cap configuration (also in the APN profile configuration mode) must be set to either local or both-hlr-and-local.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > APN Profile Configuration
configure > apn-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(apn-profile-profile_name)#

Syntax

qos class { background | conversational | interactive | streaming } [ qualif_option ]

remove qos class { background | conversational | interactive | streaming } [ qualif_option ]

remove

Removes previously defined values for the specified option or for an entire class if a qualifying option is not included in the command.

background

Selects the background traffic class. This ‘best-effort’ class manages traffic that is handled as a background function, like email, where time to delivery is not a key factor. The selection of background traffic class can be refined with the addition of one of the following qualifying options:

• all-values
• arp
• mbr-down
• mbr-map-down
• mbr-map-up
• mbr-up
• residual-bit-error-rate
• sdu
All qualifying options are explained below.

**conversational**
Selects the ‘real-time’ conversational traffic class of service, which has the most stringent time requirements of the four classes and is typically reserved for voice traffic. The section of the conversational traffic class can be refined with the addition of one of the following qualifying options:

- all-values
- arp
- gbr-down
- gbr-up
- mbr-down
- mbr-map-down
- mbr-map-up
- mbr-up
- min-transfer-delay
- residual-bit-error-rate
- sdu

All qualifying options are explained below.

**interactive**
Selects interactive traffic class of service. This class is characterized by a request/response pattern (someone sends data and then waits for a response) which requires the preservation of the data but delivers on a ‘best-effort’ model. The section of the interactive traffic class can be refined with the addition of one of the following qualifying options:

- all-values
- arp
- mbr-down
- mbr-map-down
- mbr-map-up
- mbr-up
- residual-bit-error-rate
- sdu
- thp

All qualifying options are explained below.
streaming

Selects the streaming traffic class of service, which handles one-way, real-time data transmission - such as streaming video or audio. The section of the interactive traffic class can be refined with the addition of one of the following qualifying options:

- `all-values`
- `arp`
- `gbr-down`
- `gbr-up`
- `mbr-down`
- `mbr-map-down`
- `mbr-map-up`
- `mbr-up`
- `min-transfer-delay`
- `residual-bit-error-rate`
- `sdu`

All qualifying options are explained below.

qualif_option

Qualifying options are the QoS parameters and they include:

- `all-values` - This option will change the configuration to predefined values for all the relevant QoS parameters for the class. This keyword is not used if other options are to be defined. The predefined values are:

  1. **Predefined QoS Parameters**

<pre><code>  | QoS Parameter           | Predefined Value |
  |-------------------------|------------------|
  | Traffic Class           | Background       |
  | SDU delivery order      | No               |
  | Delivery of Erroneous SDUs | No           |
  | Max Bit Rate Uplink     | 64 kbps          |
  | Max Bit Rate Downlink   | 64 kbps          |
  | Allocation/Retention Priority | 3              |
  | SDU Max Size            | 1500 octets      |
  | SDU Error Ratio         | 3 \(1 \times 10^{-3}\) |
  | Residual Bit Error Rate | 4 \(4 \times 10^{-3}\) |
  | Traffic Class           | Conversational   |
</code></pre>
<table>
<thead>
<tr>
<th>QoS Parameter</th>
<th>Predefined Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SDU delivery order</td>
<td>No</td>
</tr>
<tr>
<td>Delivery of Erroneous SDUs</td>
<td>No</td>
</tr>
<tr>
<td>Max Bit Rate Uplink</td>
<td>16 kbps</td>
</tr>
<tr>
<td>Max Bit Rate Downlink</td>
<td>16 kbps</td>
</tr>
<tr>
<td>Allocation/Retention Priority</td>
<td>3</td>
</tr>
<tr>
<td>Guaranteed Bit Rate Uplink</td>
<td>16 kbps</td>
</tr>
<tr>
<td>Guaranteed Bit Rate downlink</td>
<td>16 kbps</td>
</tr>
<tr>
<td>SDU Max Size</td>
<td>1500 octets</td>
</tr>
<tr>
<td>Minimum Transfer Delay</td>
<td>100 milliseconds</td>
</tr>
<tr>
<td>SDU Error Ratio</td>
<td>1 ((1 \times 10^{-2}))</td>
</tr>
<tr>
<td>Residual Bit Error Rate</td>
<td>1 ((5 \times 10^{-2}))</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Traffic Class</th>
<th>Interactive</th>
</tr>
</thead>
<tbody>
<tr>
<td>SDU delivery order</td>
<td>No</td>
</tr>
<tr>
<td>Delivery of Erroneous SDUs</td>
<td>No</td>
</tr>
<tr>
<td>Max Bit Rate Uplink</td>
<td>64 kbps</td>
</tr>
<tr>
<td>Max Bit Rate Downlink</td>
<td>64 kbps</td>
</tr>
<tr>
<td>Traffic Handling Priority</td>
<td>3</td>
</tr>
<tr>
<td>SDU Max Size</td>
<td>1500 octets</td>
</tr>
<tr>
<td>SDU Error Ratio</td>
<td>3 ((1 \times 10^{-3}))</td>
</tr>
<tr>
<td>Residual Bit Error Rate</td>
<td>4 ((4 \times 10^{-3}))</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Traffic Class</th>
<th>Streaming</th>
</tr>
</thead>
<tbody>
<tr>
<td>SDU delivery order</td>
<td>No</td>
</tr>
<tr>
<td>Delivery of Erroneous SDUs</td>
<td>No</td>
</tr>
<tr>
<td>Max Bit Rate Uplink</td>
<td>16 kbps</td>
</tr>
<tr>
<td>Max Bit Rate Downlink</td>
<td>16 kbps</td>
</tr>
<tr>
<td>Allocation/Retention Priority</td>
<td>3</td>
</tr>
<tr>
<td>Guaranteed Bit Rate Uplink</td>
<td>16 kbps</td>
</tr>
<tr>
<td>Guaranteed Bit Rate downlink</td>
<td>16 kbps</td>
</tr>
<tr>
<td>SDU Max Size</td>
<td>1500 octets</td>
</tr>
<tr>
<td>Minimum Transfer Delay</td>
<td>300 milliseconds</td>
</tr>
</tbody>
</table>
### QoS Parameter Predefined Value

<table>
<thead>
<tr>
<th>QoS Parameter</th>
<th>Predefined Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SDU Error Ratio</td>
<td>7 (1 \times 10^{-3})</td>
</tr>
<tr>
<td>Residual Bit Error Rate</td>
<td>1 (5 \times 10^{-2})</td>
</tr>
</tbody>
</table>

- **arp** - Sets the allocation/retention priority. Enter an integer from 1 to 3.
- **gbr-down** - Guaranteed Kbps rate for the downlink direction. Enter an integer from the range 1 to 256000.
- **gbr-up** - Guaranteed Kbps rate for the uplink direction. Enter an integer from 1 to 256000.
- **mbr-down** - Maximum Kbps rate for the downlink direction. Enter an integer from the range 1 to 256000.
- **mbr-map-down from**\(from\) **to**\(to\) - Map received HLR MBR \(\text{from value}\) to a locally configured downlink MBR value \(\text{to value}\):
  - **from**\(kbps\) - Enter an integer from 1 to 25600.
  - **to**\(kbps\) - Enter an integer from 1 to 25600.
- **mbr-map-up from**\(from\) **to**\(to\) - Map received HLR MBR \(\text{from value}\) to a locally configured uplink MBR value \(\text{to value}\):
  - **from**\(kbps\) - Enter an integer from 1 to 25600.
  - **to**\(kbps\) - Enter an integer from 1 to 25600.
- **mbr-up** - Maximum Kbps rate for the uplink direction. Enter an integer from 1 to 256000.
- **min-transfer-delay** - Minimum transfer delay in milliseconds. Enter an integer from 80 to 4000.
- **residual-bit-error-rate** -
  - Background TC residual-bit-error-rate range is from \(4 \times 10^{-4}\) to \(6 \times 10^{-8}\). Enter one of the following integers, where:
  - **4**: represents \(4 \times 10^{-3}\)
  - **7**: represents \(10^{-5}\)
  - **9**: represents \(6 \times 10^{-8}\)
  - Conversational TC residual-bit-error-rate range is from \(5 \times 10^{-2}\) to \(10^{-6}\). Enter one of the following integers, where:
  - **1**: represents \(5 \times 10^{-2}\)
  - **2**: represents \(10^{-2}\)
  - **3**: represents \(5 \times 10^{-3}\)
  - **5**: represents \(10^{-3}\)
  - **6**: represents \(10^{-4}\)
  - **7**: represents \(10^{-5}\)
  - **8**: represents \(10^{-6}\)
  - Interactive TC residual-bit-error-rate range is from \(4 \times 10^{-4}\) to \(6 \times 10^{-8}\). Enter one of the following integers, where:
**qos class**

- 4: represents $4 \times 10^{-3}$
- 7: represents $10^{-5}$
- 9: represents $6 \times 10^{-8}$

- Streaming TC residual-bit-error-rate range is from $5 \times 10^{-2}$ to $10^{-6}$. Enter one of the following integers, where:
  - 1: represents $5 \times 10^{-2}$
  - 2: represents $10^{-2}$
  - 3: represents $5 \times 10^{-3}$
  - 5: represents $10^{-3}$
  - 6: represents $10^{-4}$
  - 7: represents $10^{-5}$
  - 8: represents $10^{-6}$

- **sdu** - Signalling data unit keyword, must include one of the following options:
  - **delivery-order** - Enter one of the two following options:
    - no - Without delivery order
    - yes - With delivery order
  - **erroneous** - Enter one of the two following options:
    - no - Erroneous SDUs will not be delivered
    - no-detect - Erroneous SDUs are not detected (‘-’)
    - yes - Erroneous SDUs will be delivered
  - **error-ratio** - The SDU error-ratio range is from $10^{-3}$ to $10^{-6}$. Enter an integer from 1 to 6, where:
    - 3: Represents $10^{-3}$
    - 4: Represents $10^{-4}$
    - 6: Represents $10^{-6}$
  - **max-size** - Defines the maximum number of octets (size) of the SDU. Enter an integer from 10 to 1502.

- **thp** - Sets the traffic handling priority. Enter an integer from 1 to 3.

**Usage**

This command defines the qualifying options (parameters) for each QoS traffic class defined for this APN profile.

**Important:** Typically this command is only used to define QoS parameters when the APN record does not exist in the subscription record.
Repeat the command as often as needed with different options to define all required QoS criteria. For example, to configure the maximum bit rate (MBR) for the downlink and uplink directions for a traffic class, this command must be used twice, specifying **mbr-down** once and **mbr-up** once.

Advantage for local mapping of MBR: some HLRs cannot be configured with high MBR values. Using the **mbr-map-up** and the **mbr-map-down** parameters allows the SGSN to be configured to treat a specific HLR value as meaning the desired high MBR value. In a case where the HLR does not support HSPA+ bit rates, but the handsets and network do, this feature allows the operator to overcome limitations on the HLR and provide HSPA+ bit rates by overwriting the provisioned HLR-QoS MBR values with SGSN-configured values. When MBR mapping is configured, if QoS is preferred as the HLR value, then the subscription QoS MBR received from the HLR is compared with the "from" value in the table. If it matches, then it is converted to the value specified by the "to" value in the table. QoS negotiation happens based on the converted value.

Advantage for QoS capping with THP and ARP: Controlling THP and ARP via Operator Policy: This functionality can differentiate home vs. roaming subscribers, and prevent visiting subscribers from receiving a high-tiered service. For example, a service provider could offer service differentiation using Ultra/Super/Standard service levels based upon QoS; this could justify charging a corporate customer more to use the Internet APN than would be charged to a consumer. This could be accomplished by controlling the traffic handling priority (THP) over the air interface, i.e. THP 1 = Ultra, THP 2 = Super and THP 3 = Standard.

**Example**

Use the following command to configure the entire conversational traffic class with predefined QoS options:

```
qos class conversational all-values
```

Now change the background class ARP from 3 to 2:

```
qos class background arp 2
```

Invalidate the THP parameter, by removing all value from the parameter, for the interactive class:

```
remove qos class interactive thp
```
qos dedicated-bearer

Configures the quality of service maximum bit rate (MBR) parameters for the dedicated bearer. This command is specific to the MME.

**Product**
MME

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > APN Profile Configuration

```
configure > apn-profile profile_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(apn-profile-profile_name)#
```

**Syntax**

```
qos dedicated-bearer mbr max-ul mbr-up max-dl mbr-dwn
```

```
remove qos dedicated-bearer
```

```
remove

Removes the dedicated bearer maximum bit rate (MBR) changes from the configuration for this APN profile.
```

```
max-ul mbr-up max-dl mbr-dl

Defines the maximum bit rates for uplink and downlink traffic.

mbr-up is an integer from 0 through 1410065408.
mbr-dl is an integer from 0 through 1410065408.
```

**Usage**

Use this command to define the MBRs that will be enforced by the P-GW for both uplink and downlink traffic shaping.

**Example**

```
qos dedicated-bearer mbr max-ul 24234222 max-dl 23423423
```
qos default-bearer

Configures the quality of service parameters for the default bearer. This command is specific to the MME.

**Product**
MME

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > APN Profile Configuration

```
configure > apn-profile profile_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(apn-profile-profile_name)#
```

**Syntax**

```
qos default-bearer { arp arp_value [ preemption-capability { may | shall-not } ] | vulnerability { not-preemptable | preemptable } ] | qci qci }
remove qos default-bearer { arp | qci }
```

**remove**

Removes the default bearer QoS configuration from this APN profile.

**arp arp_value**

Defines the address retention priority value. *arp_value* is an integer from 1 through 15.

**preemption-capability { may | shall-not }**

Specifies the preemption capability flag. Options are:

- **may**: Bearer may be preempted
- **shall-not**: Bearer shall not be preempted

**vulnerability { not-preemptable | preemptable }**

Specifies the vulnerability flag. Options are:

- **not-preemptable**: Bearer cannot be preempted.
- **preemptable**: Bearer can be preempted.

**qci qci**

Specifies the QoS Class Identifier for the default bearer profile. *qci* is an integer from 0 through 255.

**Usage**

Use this command to set the QoS APR and QCI parameters for the default bearer configuration.
qos default-bearer arp 2 preemption-capability may
**qos pgw-upgrade**

Configures the action to be taken when the MME receives a QoS upgrade from P-GW for default bearers/Non-Guaranteed Bit Rate (Non-GBR) bearers.

**Product**
MME

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > APN Profile Configuration

```
configure > apn-profile profile_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(apn-profile-profile_name)#
```

**Syntax**

```
quos pgw-upgrade non-gbr { accept | reject | locally-cap }
```

```
[ remove ] qos pgw-upgrade non-gbr
```

**remove**
Removes the configuration, returning the system to the default setting where the MME accepts the P-GW upgraded QoS values for Non-GBR (default) bearers.

```
non-gbr { accept | reject | locally-cap }
```

For Non-GBR (default) bearers, this keyword configures the action the MME takes when it receives a P-GW upgraded QoS value.

- **accept**: The MME will accept the P-GW upgraded QoS values.
- **reject**: The MME will reject the P-GW upgraded QoS values.
- **locally-cap**: The MME compares QCI, ARP and ARP-PVI provided by P-GW to the locally configured values of those parameters. If the values match, then accepts towards the P-GW and use locally configured values towards the UE/RAN for APN-AMBR and ARP-PCI. If the values do not match, the MME rejects the P-GW upgraded QoS values.

**Usage**

Use this command to provide configurability at the APN Profile level for the MME to accept, reject, or locally-cap P-GW upgraded QoS values for default (non-GBR) bearers. This S11 Control is applied whenever QoS parameters are received on S11 interface. The relevant procedures for default bearers are Create Session Response (sent by P-GW during Attach, UE requested PDN connectivity) and Update Bearer Procedures (initiated by P-GW resulting from trigger QoS change or other in PCEF/PCRF, or from Modify Bearer Command or Bearer Resource Command sent by MME). **Note**: This configuration is supported only for Default bearers (i.e Non-GBR bearers) in a roaming scenario.

The MME will set the sum of the APN-AMBR of all active APNs up to the value of the subscribed UE-AMBR, subject to the UE-AMBR restriction.
In the case of an Attach Reject or PDN Connectivity Reject, the ESM failure cause “Operator determined barring” is used and the corresponding MME schema bulk statistic is incremented.
In the case of Update Bearer Request Reject, the EGTP cause “Request rejected” is used and the corresponding EGTP bulk statistic is incremented.
A session disconnect reason mme-qos-pgw-upgrade-reject(589) is incremented when QoS upgrade by P-GW is rejected by the MME during initial attach. The corresponding session disconnect reason statistics are incremented.
Refer to the dedicated-bearers command to configure QoS controls for dedicated bearers (GBR and Non-GBR).

Example

The following command configures the MME to reject the QOS upgrade from P-GW for non-GBR bearers:

```
qos pgw-upgrade non-gbr reject
```
qos prefer-as-cap

Specifies operational preferences for QoS parameters, specifically QoS bit rates. This command is specific to the SGSN in releases prior to 14.0.

Product
MME
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > APN Profile Configuration

configure > apn-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(apn-profile-profile_name)#

Syntax

qos prefer-as-cap { both-hlr-and-local | both-hss-and-local { local-when-subscription-not-available | minimum | subscription-exceed-reject } | hlr-subscription | local }

remove qos prefer-as-cap

> **Important:** Command and keyword names have changed. prefer has become prefer-as-cap and hlr has become hlr-subscription. These changes will not impact configuration generated with earlier releases as the keywords are aliases for the previous names.

remove

Removes previous configuration changes and resets the default.

both-hlr-and-local

Instructs the SGSN to use, as the capping value during session establishment, the lower of either the locally configured QoS bit rate or the Home Location Register (HLR) subscription.

both-hss-and-local { local-when-subscription-not-available | minimum | subscription-exceed-reject }

For the MME only, specifies the QoS cap value to use.

• **local-when-subscription-not-available:** Use the locally configured values if the Home Subscriber Server (HSS) does not provide any values.

• **minimum:** Use the lower of either the locally configured QoS bit rate or the HSS-provided QoS bit rate.

• **subscription-exceed-reject:** If the requested QoS bit rate exceeds the locally configured value, reject the PDN connection.
**Usage**

Use this command to instruct the SGSN or MME to take QoS configuration as the bit rate for session establishment. The MME has no default setting for this command.

**Example**

The following command specifies use of the bit rate in subscription at the HLR:

```
qos prefer-as-cap hlr-subscription
```

The following command instructs the SGSN to cap the bit rate with the lower rate of the two configurations, HLR or local:

```
qos prefer-as-cap both-hlr-and-local
```
qos rate-limit direction

Configures the actions governing the subscriber traffic flow, if the flow violates or exceeds the configured or negotiated peak or committed data-rates.

This command can be entered multiple times to specify different combinations of traffic direction and class. The SGSN only performs traffic policing if qos rate-limit direction is configured.

Additional information on the QoS traffic policing functionality is located in the System Administration Guide.

Product

SGSN
S-GW
SAEGW

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > APN Profile Configuration
configure > apn-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(apn-profile-profile_name)#

Syntax

qos rate-limit direction { downlink | uplink } [ burst-size { auto-readjust [ duration seconds ] | bytes } ] [ class { background | conversational | interactive traffic_priority | streaming } ] [ exceed-action { drop | lower-ip-precedence | transmit } ] [ gbr-qci [ committed-auto-readjust duration seconds ] ] [ non-gbr-qci [ committed-auto-readjust duration seconds ] ] [ violate-action { drop | lower-ip-precedence | transmit } ]

remove qos rate-limit direction { downlink | uplink } [ class { background | conversational | interactive traffic_priority | streaming } ]

remove

Removes the qos rate-limit direction entries from the configuration.

downlink | uplink

Apply the limits and actions configured with the other keywords to the selected link:
downlink - This is the direction from the GGSN or P-GW to the MS.
uplink - This is the direction from the MS to the GGSN or the P-GW.

burst-size { auto-readjust [ duration seconds ] | bytes }

Default: See the table of class default values in the Usage section below.
This keyword specifies the peak burst size allowed. System measurements for this value exclude the GTP and outer packet headers. Supported options include:

* auto-readjust: This keyword enables dynamic burst-size calculation using negotiated peak data-rate and negotiated committed data-rate.
**duration seconds**: Must be an integer from 1 to 30; default is 1. This keyword sets the number of seconds that the dynamic burst-size calculation will last. This allows the traffic to be throttled at the negotiated rates.

**bytes**: Must be an integer from 1 to 6000000. This value specifies the static burst size for traffic policing. This option is present for backward compatibility.

---

**Important**: Use of dynamic burst size (**auto-readjust**) for traffic policing is recommended, rather than the static burst size.

```plaintext
class { background | conversational | interactive traffic_priority | streaming }
```

The `class` keyword configures the specified traffic policing actions per traffic class, or per traffic priority in the case of interactive traffic class. The following classes are supported:

- **background**: Specifies the traffic action for traffic patterns in which the data transfer is not time-critical (for example, email exchanges).
- **conversational**: Specifies the traffic policing action for traffic patterns in which there is a constant flow of packets in each direction, upstream and downstream.
- **interactive traffic_priority**: Specifies the traffic policing action for traffic patterns in which there is an intermittent flow of packets in each direction, upstream and downstream.
  - `traffic_priority` is the 3GPP traffic handling priority and can be an integer 1, 2 or 3.
- **streaming**: Specifies the traffic policing action for traffic patterns in which there is a constant flow of data in one direction, either upstream or downstream.

---

**Important**: This is an SGSN-specific feature. If this keyword is omitted, the same values are used for all classes.

```plaintext
exceed-action { drop | lower-ip-precedence | transmit }
```

Default: See the table of class default values in the Usage section below.

The action to take on the packets that exceed the committed-data-rate but do not violate the peak-data-rate.

The following actions are supported:

- **drop**: Drop the packet
- **lower-ip-precedence**: Transmit the packet after lowering the ip-precedence
- **transmit**: Transmit the packet

```plaintext
gbr-qci [ committed-auto-readjust duration seconds ]
```

Applies the traffic policing policy to guaranteed bitrate bearers.

- `committed-auto-readjust duration seconds`: Must be an integer from 1 to 30. This keyword sets the number of seconds that the committed burst-size calculation will last. This allows the traffic to be throttled to the negotiated rates.

---

**Important**: This is an S-GW-specific feature.

```plaintext
non-gbr-qci [ committed-auto-readjust duration seconds ]
```

Applies the traffic policing policy to non-guaranteed bitrate bearers.
**committed-auto-readjust duration seconds**: Must be an integer from 1 to 30. This keyword sets the number of seconds that the committed burst-size calculation will last. This allows the traffic to be throttled to the negotiated rates.

**Important**: This is an S-GW-specific feature.

\[\text{violate-action} \{ \text{drop} \mid \text{lower-ip-precedence} \mid \text{transmit} \}\]

Default: See the table of class default values in the Usage section below.

The action to take on the packets that exceed both the committed-data-rate and the peak-data-rate. The following actions are supported:

- **drop**: Drops the packet
- **lower-ip-precedence**: Transmits the packet after lowering the IP precedence
- **transmit**: Transmits the packet

This symbol indicates that the keywords can be entered multiple times within a single command.

### Usage

This command configures the APN’s quality of service (QoS) traffic policing. Configured actions prevent subscriber flow exceeding or violating configured peak or negotiated peak or committed data rate limits.

**Important**: If either **exceed action** or **violate action** is set to **lower-ip-precedence**, this command may override the configuration of the **ip qos-dscp** command in the APN profile.

<table>
<thead>
<tr>
<th>Class: Background</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Downlink Traffic: Disabled</td>
<td></td>
</tr>
<tr>
<td>Peak Data Rate (in bps): 16000000</td>
<td></td>
</tr>
<tr>
<td>Committed Data Rate (in bps): n/a</td>
<td></td>
</tr>
<tr>
<td>Burst Size (in bytes): 65535</td>
<td></td>
</tr>
<tr>
<td>Exceed Action: n/a</td>
<td></td>
</tr>
<tr>
<td>Violate Action: drop</td>
<td></td>
</tr>
<tr>
<td>Uplink Traffic: Disabled</td>
<td></td>
</tr>
<tr>
<td>Peak Data Rate (in bps): 8640000</td>
<td></td>
</tr>
<tr>
<td>Committed Data Rate (in bps): n/a</td>
<td></td>
</tr>
<tr>
<td>Burst Size (in bytes): 65535</td>
<td></td>
</tr>
<tr>
<td>Exceed Action: n/a</td>
<td></td>
</tr>
<tr>
<td>Violate Action: drop</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Class: Conversational</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Downlink Traffic: Disabled</td>
<td></td>
</tr>
<tr>
<td>Peak Data Rate (in bps): 16000000</td>
<td></td>
</tr>
<tr>
<td>Committed Data Rate (in bps): 16000000</td>
<td></td>
</tr>
<tr>
<td>Burst Size (in bytes): 65535</td>
<td></td>
</tr>
<tr>
<td>Exceed Action: lower-ip-precedence</td>
<td></td>
</tr>
<tr>
<td>Violate Action: drop</td>
<td></td>
</tr>
<tr>
<td>Uplink Traffic: Disabled</td>
<td></td>
</tr>
<tr>
<td>Peak Data Rate (in bps): 8640000</td>
<td></td>
</tr>
<tr>
<td>Committed Data Rate (in bps): 8640000</td>
<td></td>
</tr>
<tr>
<td>Burst Size (in bytes): 65535</td>
<td></td>
</tr>
<tr>
<td>Exceed Action: lower-ip-precedence</td>
<td></td>
</tr>
<tr>
<td>Violate Action: drop</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Class: Interactive, Traffic Handling Priority: 1</th>
</tr>
</thead>
</table>
## APN Profile Configuration Mode

### qos rate-limit direction

<table>
<thead>
<tr>
<th>Class: Interactive, Traffic Handling Priority: 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Downlink Traffic: Disabled</td>
</tr>
<tr>
<td>Peak Data Rate (in bps): 16000000</td>
</tr>
<tr>
<td>Committed Data Rate (in bps): n/a</td>
</tr>
<tr>
<td>Burst Size (in bytes): 65535</td>
</tr>
<tr>
<td>Exceed Action: n/a</td>
</tr>
<tr>
<td>Violate Action: drop</td>
</tr>
<tr>
<td>Uplink Traffic: Disabled</td>
</tr>
<tr>
<td>Peak Data Rate (in bps): 8640000</td>
</tr>
<tr>
<td>Committed Data Rate (in bps): n/a</td>
</tr>
<tr>
<td>Burst Size (in bytes): 65535</td>
</tr>
<tr>
<td>Exceed Action: n/a</td>
</tr>
<tr>
<td>Violate Action: drop</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Class: Interactive, Traffic Handling Priority: 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Downlink Traffic: Disabled</td>
</tr>
<tr>
<td>Peak Data Rate (in bps): 16000000</td>
</tr>
<tr>
<td>Committed Data Rate (in bps): n/a</td>
</tr>
<tr>
<td>Burst Size (in bytes): 65535</td>
</tr>
<tr>
<td>Exceed Action: n/a</td>
</tr>
<tr>
<td>Violate Action: drop</td>
</tr>
<tr>
<td>Uplink Traffic: Disabled</td>
</tr>
<tr>
<td>Peak Data Rate (in bps): 8640000</td>
</tr>
<tr>
<td>Committed Data Rate (in bps): n/a</td>
</tr>
<tr>
<td>Burst Size (in bytes): 65535</td>
</tr>
<tr>
<td>Exceed Action: n/a</td>
</tr>
<tr>
<td>Violate Action: drop</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Class: Streaming</th>
</tr>
</thead>
<tbody>
<tr>
<td>Downlink Traffic: Disabled</td>
</tr>
<tr>
<td>Peak Data Rate (in bps): 16000000</td>
</tr>
<tr>
<td>Committed Data Rate (in bps): n/a</td>
</tr>
<tr>
<td>Burst Size (in bytes): 65535</td>
</tr>
<tr>
<td>Exceed Action: n/a</td>
</tr>
<tr>
<td>Violate Action: drop</td>
</tr>
<tr>
<td>Uplink Traffic: Disabled</td>
</tr>
<tr>
<td>Peak Data Rate (in bps): 8640000</td>
</tr>
<tr>
<td>Committed Data Rate (in bps): n/a</td>
</tr>
<tr>
<td>Burst Size (in bytes): 65535</td>
</tr>
<tr>
<td>Exceed Action: n/a</td>
</tr>
<tr>
<td>Violate Action: drop</td>
</tr>
</tbody>
</table>

### Example

The following command lowers the IP precedence when the committed-data-rate and the peak-data-rate are violated in uplink direction:

```plaintext
qos rate-limit direction uplink violate-action lower-ip-precedence
```

The following command drops the excess user packets when the subscriber traffic violates both the configured peak and the committed data-rate in the uplink direction. Once either the peak or the committed data-rate for that subscriber goes below the configured/negotiated limit, it transmits them.

```plaintext
qos rate-limit direction uplink exceed-action drop
```
ranap allocation-retention-priority-ie

Configures the allocation/retention priority (ARP) IE for this APN profile. This command is specific to the SGSN.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > APN Profile Configuration
configure > apn-profile profile_name

Entering the above command sequence results in the following prompt:

```
[local]host_name(apn-profile-profile_name)#
```

**Syntax**

```
ranap allocation-retention-priority-ie subscription-priority priority class { { background | conversational | interactive | streaming } { not-pre-emptable | priority | queuing-not-allowed | shall-not-trigger-pre-emptable } + }
```

Important: All parameters not specifically configured will be included in the configuration with default values.

```
[ default | remove | no ] ranap allocation-retention-priority-ie [ subscription-priority priority class { background | conversational | interactive | streaming } ]
```

- **default**
  Resets the configuration to the default values.

- **no**
  Disables the specified configuration

- **remove**
  Removes the specified configuration.

- **subscription-priority priority**
  This keyword sets the subscription priority. The lowest number has the highest priority. *priority* must be an integer from 1 to 3.

- **class**
  Configure allocation/retention priority (ARP) for specific QoS traffic classes. Include one or more of the following class options:
  - **background**: background class of service
  - **conversational**: conversational class of service
  - **interactive**: interactive class of service
- **streaming**: streaming class of service

Default values will be included in the configuration for any class configuration not specified.

### qualifying options

For each of the class options, the configuration must include one or more of the following qualifying options:

- **not-pre-emptable**
- **priority**: smallest number is the highest priority. Value must be an integer from 1 to 15
- **queuing-not-allowed**
- **shall-not-trigger-pre-emptable**

When entering more than one option, we recommend that you do it in the order in which they are listed.

+ This symbol indicates that the keywords can be entered multiple times within a single command.

### Usage

Use this command to configure values for the allocation/retention priority (ARP) IE in the radio access bearer (RAB) assignment request message for RANAP that occurs during RAB setup.

This command can be used multiple times to define multiple priorities, with different combinations of **subscription-priority** and **class**.

If the HLR returns a matching value for the subscribed ARP for the desired traffic class, the SGSN includes the configured qualifying options for the ARP IE in the RANAP message.

### Example

The following series of commands define the highest priority for conversational traffic class with priority level 1-10 (Subscribed priority 0-3), PCI of shall-not-trigger-pre-emption, PVI of not-pre-emptable with queuing-not-allowed:

```
ranap allocation-retention-priority-ie subscription-priority 0 priority class conversational not-pre-emptable priority 1 shall-not-trigger-pre-emptable

ranap allocation-retention-priority-ie subscription-priority 1 priority class conversational not-pre-emptable priority 4 shall-not-trigger-pre-emptable

ranap allocation-retention-priority-ie subscription-priority 2 priority class conversational not-pre-emptable priority 7 shall-not-trigger-pre-emptable

ranap allocation-retention-priority-ie subscription-priority 3 priority class conversational not-pre-emptable priority 10 shall-not-trigger-pre-emptable
```
restrict access-type

Configures the activation restrictions of PDP context on the basis of the access type and QoS class. This command is specific to the SGSN.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > APN Profile Configuration
configure > apn-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(apn-profile-profile_name)#

Syntax

restrict access-type { { gprs | umts } [ qos-class { background | conversational | interactive | streaming } ] }

no restrict access-type { gprs | umts } [ qos-class ]

default restrict access-type { gprs | umts }

no
Remove the restriction rules for PDP context activation configured in this APN profile.

default
Resets the restriction rules for PDP context activation to the default values to allow all access types and QoS class.

gprs
Configures the APN profile to restrict the PDP context activation from General Packet Radio Service (2.5G) network access.

umts
Configures the APN profile to restrict the PDP context activation from Universal Mobile Telecommunications Systems (3G) network access.

qos-class
Configures the APN profile to restrict the PDP context activation for to a specific QoS traffic class. It is optional and can be configured after selecting the network access type. Possible traffic classes options are:

•background: Specifies the QoS class as background service session
•conversational: Specifies the QoS class as conversational service session
•interactive: Specifies the QoS class as interactive service session
**Streaming**: Specifies the QoS class as streaming service session

**Usage**

Use this command to configure the restriction rules in an APN profile for activation of PDP context on the basis of the access type. It also provides the facility to restrict type of traffic QoS class.

**Example**

The following command configures the APN profile to restrict all traffic from a GPRS network service having a QoS class of interactive:

```
restrict access-type grps qos-class interactive
```
Chapter 25
APN Remap Table Configuration Mode

APN Remap Table Configuration mode provides the commands to configure parameters for multiple features related to Access Point Name (APN) handling, such as: Default APN, APN Remap, and Wildcard APN. APN remap table is a key element of the Operator Policy feature and a table is not usable (valid) until it has been associated with an operator policy (see the Operator Policy Configuration Mode Commands) or an IMEI profile (see the IMEI Profile Configuration Mode Commands).

A maximum of 1,000 APN remap tables are supported, and each APN remap table supports a maximum of 100 APN remap entries. Multiple tables can be defined and stored but an operator policy and/or IMEI profile each only support association with a single (one) table per policy/profile configuration. The APN remap table associated with an IMEI profile will be used in IMEI override scenarios.

Mode

Exec > Global Configuration > APN Remap Table Configuration

configure > apn-remap-table table_name

Entering the above command sequence results in the following prompt:

[local]host_name(apn-remap-table_name)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
**apn-remap**

Creates an entry in the APN remap table and provides the ability to override the APN requested by the UE.

**Product**
- MME
- SGSN

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration > APN Remap Table Configuration
- configure > apn-remap-table table_name

Entering the above command sequence results in the following prompt:

```
[local]host_name(apn-remap-table_name)#
```

**Syntax**

```
apn-remap { network-identifier apn_net_id { new-ni new_apn_net_id | operator-identifier apn_op_id new-ni new_apn_net_id { new-oi new_apn_op_id | value-for-oi-mcc mcc | value-for-oi-mnc mnc } | value-for-ni-wc new_apn_net_id } | operator-identifier apn_op_id { new-oi new_apn_op_id | value-for-oi-mcc mcc | value-for-oi-mnc mnc } }
```

```
no apn-remap { network-identifier apn_net_id | operator-identifier apn_op_id }
```

**no**

Deletes the specified APN remap entry from the APN remap table.

**network-identifier apn_net_id**

Identifies the "old" APN network identifier that is being mapped for replacement.  
*apn_net_id* is a string of 1 to 62 characters, including digits, letters, dots (.) and dashes (-). Additionally, one wildcard character ( * ) can be included anywhere within the string.

**new-ni new_apn_net_id**

Identifies the new (target) network identifier to use when no wildcard character is included in the “old” APN network identifier.  
*new_apn_net_id* is a string of 1 to 62 characters, including digits, letters, dots (.) and dashes (-).

**value-for-ni-wc new_apn_net_id**

Identifies the information to replace the wildcard in the new APN network identifier when a wildcard character is included in the “old” APN network identifier.  
*new_apn_net_id* is an alphanumeric string of characters, including dots (.) and dashes (-). This string replaces the wildcard (*) specified in the *apn_net_id*. The two strings together must not exceed 62 characters.

**operator-identifier apn_op_id**

Identifies the “old” APN operator identifier that is being mapped for replacement.
**apn_op_id** is a string of 1 to 18 characters including digits, letters, and dots (.). The entry must be in the following format, where # represents a digit: MNC###.MCC###.GPRS.

Optionally, either one or two wildcard characters ( * ) can be entered. Wildcard characters can be used in place of one # or three # -- for example MNC12*.MCC*.GPRS.

**new-oi new_apn_op_id**

Identifies the new (target) operator identifier to use when no wildcard character is included in the “old” APN operator identifier.

**new_apn_op_id** is a string of 1 to 18 characters including digits, letters, and dots (.). The entry must be in the following format, where # represents a digit: MNC###.MCC###.GPRS.

**value-for-oi-mcc mcc**

Identifies the information to replace the wildcard in the new APN operator identifier when a wildcard character is included in the MCC portion of the “old” APN operator identifier; for example MNC###.MCC*.GPRS.

**value-for-oi-mnc mnc**

Identifies the information to replace the wildcard in the new APN operator identifier when a wildcard character is included in the MNC portion of the “old” APN operator identifier; for example MNC*.MCC###.GPRS.

**Usage**

**Important:** Entries in the APN remap table are only valid if the table is associated with an operator policy. The same table can then be associated with an IMEI profile as IMEI-specific remap entries are not supported.

This command defines mapping entries in the APN remap table which supports a range of APN overrides. Mapping can be done one-to-one:

- a "new" APN network identifier (NI) can be mapped to override an “old” APN network identifier (NI) or an “old” APN operator identifier (OI)
- a "new" APN operator identifier (OI) can be mapped to override an “old” APN network identifier (NI) or an “old” APN operator identifier (OI)

Mapping can also be done with wildcards in the "old" APN entry mapped to wildcard replacements to dynamically create “new” APN network/operator identifiers.

**Related Commands:** APN override can also be based on charging characteristics. This type of override mapping is defined with the **cc** command, also part of this configuration mode.

**Example**

A one-to-one APN NI remap entry is illustrated by:

```
    apn-remap network-identifier 123abc.com new-ni 333CBC.com
```

Create an entry with a wildcard so that part of an incoming APN NI will be replaced - for example, incoming xyzabc$pqr.com becomes xyzinternet2$pqr.com.

```
    apn-remap network-identifier xyz*pqr.com value-for-ni-wc internet2
```

Replace any incoming APN NI with a new APN NI.
apn-remap network-identifier * value-for-ni-wc newnet.com

A one-to-one APN OI remap entry is illustrated by:

apn-remap operator-identifier MNC423.MCC222.GPRS new-oi
MNC123.MCC456.GPRS

Replace any incoming APN OI with a new APN OI MNC123.MCC456.GPRS:

apn-remap operator-identifier MNC*.MCC*.GPRS value-for-oi-mnc 123 value-for-oi-mcc 456
apn-selection-default

Enables and configures or disables the Default APN feature for use when the normal APN selection process fails.

Product
MME
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > APN Remap Table Configuration
configure > apn-remap-table table_name

Entering the above command sequence results in the following prompt:

[local]host_name(apn-remap-table_name)#

Syntax


no apn-selection-default { first-in-subscription | lowest-context-id | network-identifier apn_net_id }

no
Delete the configuration statement and disable the default APN feature.

first-in-subscription

Specifies that the first APN in the subscription record matching the requested PDN type is used as the default APN. This applies when normal APN selection fails and if the UE APN is absent and the defined default APN is not a match.
For the SGSN, “first-in-subscription” means the first record from the list of records sent from the HLR (in the same order) with PDP type matching the requested PDP type. With this configuration, if the first record is a wildcard APN it is expected that the wildcard APN be configured. If not, the activation will be rejected.
For the MME, “first-in-subscription” means the first record from the list of records (apn-list) sent from the HSS with PDP type matching the UE-requested PDP type. The apn-list is sorted according to apn-name.

lowest-context-id

Specifies that the subscription APN with the lowest context-ID in the subscription record matching the PDN type is used as the default APN when normal APN selection fails.
With this configuration, if the record with the lowest context-ID is a wildcard APN, then it is expected that the wildcard APN has already been configured. If not, the activation will be rejected.
If both apn-selection-default lowest-context-id and apn-selection-default first-in-subscription options are configured, whichever command was executed (configured) first will be the behavior used.
Starting with Release 14.0, MME also supports use of this keyword.
**network-identifier apn_net_id**

Specifies the network identifier will be used as the default APN name as a string of 1 to 62 characters, including digits, letters, dots (.) and dashes (-).

Any of the following optional keywords can be used with `network-identifier` as qualifications.

**fallback-apn network-identifier apn_net_id**

SGSN only.

Specifies a dummy APN to be used when the default APN is not present in the subscription so that the activation does not fail. With this keyword configured, the context is activated with a dummy APN and the GGSN displays a static page for this APN, instructing the subscriber to subscribe for appropriate services.  

`apn_net_id` is a string of 1 to 62 characters, including letters, digits, dots (.) and dashes (-).

**fallback-to-first-in-subscription**

Uses the APN from the first subscription record when the configured default APN is not available.

**prefer-single-subscription**

Uses the APN from the subscription record if it is the only record available and normal APN selection fails.

**reject-blank-apn**

Disables use of the default APN if a blank APN is received.

**require-dns-fail-wildcard**

Enables the default APN to be used if the DNS query fails with the requested APN.  
Starting with Release 18.2, this keyword is also supported by the MME.

**require-subscription-apn network-identifier apn_net_id**

If defined, this APN name must also be included in the subscription data for the default APN feature to function.

`apn_net_id` is a string of 1 to 62 characters, including letters, digits, dots (.) and dashes (-).

**Usage**

The default APN feature will be used in error situations when the MME or the SGSN cannot select a valid APN via the normal APN selection process. Within an operator policy, an APN remap table with a default APN can be configured for the MME/SGSN to:

- override a requested APN when the HSS/HLR does not have the requested APN in the subscription profile.
- provide a viable APN if APN selection fails because there was no "requested APN" and wildcard subscription was not an option.

The default APN feature can also be used in the event of a DNS query failure with the selected APN, if:

- the `wildcard-apn` command is configured, (requirement only for SGSN)
- a wildcard subscription is present,
- the `require-dns-fail-wildcard` keyword is included with the `apn-selection-default` command then the configured default APN will be used when the DNS query is retried.

In all of the instances outlined above, the MME/SGSN can provide the default APN as an alternate behavior to ensure that PDP context activation is successful.
Example

The following command enables the default APN feature for APN *HomeNet1*:

```
apn-selection-default network-identifier HomeNet1
```

The following command enables use of a default APN selected on the basis of lowest context-ID if the APN is not contained within the subscription:

```
apn-selection-default lowest-context-id
```

The following command enables use of a default APN if the DNS query fails:

```
apn-selection-default network-identifier HomeNet1 require-dns-fail-wildcard
```
**blank-apn**

Enables the Blank APN feature and defines the APN that will be used when no APN is requested. This command is specific to SGSN.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > APN Remap Table Configuration

```
configure > apn-remap-table table_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(apn-remap-table_name)#
```

**Syntax**

```
blank-apn network-identifier apn_net_id

no blank-apn
```

- **no**

  Removes the APN NI from the APN remap table configuration and disables the Default APN feature.

- **network-identifier apn_net_id**

  Identifies the APN network identifier (NI) that will be used when no APN is requested.
  
  `apn_net_id` is a string of 1 to 62 characters, including letters, digits, dots (.) and dashes (-).

**Usage**

Use this command to enable the Blank APN feature.

**Example**

The following command creates an entry that supplies the `starnet.com` as the APN network identifier whenever a request does not include an APN:

```
blank-apn network-identifier starnet.com
```
**CC**

This command maps an APN override based on charging characteristics.

**Product**

MME  
SGSN

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > APN Remap Table Configuration  
`configure > apn-remap-table table_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(apn-remap-table_name)#
```

**Syntax**

```
cc behavior bit_value profile index_bit apn-remap network-identifier apn_net_id new-ni new_apn_net_id

no cc behavior bit_value profile index_bit apn-remap network-identifier apn_net_id
```

**no**

Disables the configured cc-based remapping behavior.

**behavior bit_value**

Specifies the value for the charging characteristic behavior bit.  
`bit_value` is a hex value from 0x0 to 0xFFF.

**profile index_bit**

Specifies the index for the charging characteristic profile.  
`index_bit` is an integer from 1 through 15.  
Some of the index values are predefined according to 3GPP standards:  
- 1 for hot billing  
- 2 for flat billing  
- 4 for prepaid billing  
- 8 for normal billing

**apn-remap network-identifier apn_net_id**

Identifies the “old” APN network identifier that is being mapped for replacement.  
`apn_net_id` is a string of 1 to 62 characters, including letters, digits, dots (.) and dashes (-).

**new-ni new_apn_net_id**

Identifies the “new” APN network identifier that is being mapped to.  
`new_apn_net_id` is a string of 1 to 62 characters, including letters, digits, dots (.) and dashes (-).
Usage

Use this command to enable APN remapping only when the charging characteristic value in the subscription record associated with the requested APN matches the value configured for the new-ni. The new APN NI must be part of the subscription data so that the charging characteristic associated with the new APN NI will be used for activating the context. If there is not one associated, then the general charging characteristic will be used.

Example

The following command associates a new APN NI locals1 with a set of charging characteristics:

```
cc behavior 0xF profile 4 apn-remap network-identifier homer1 new-ni locals1
```
description

Defines a string that describes this APN remap table.

Product
MME
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > APN Remap Table Configuration
configure > apn-remap-table table_name

Entering the above command sequence results in the following prompt:

[local]host_name(apn-remap-table_name)#

Syntax

description description

no description

no

Removes the description configuration from this APN Remap Table configuration.

description

Specifies descriptive text to be associated with the APN remap table as an alphanumeric string of 1 through 100 characters. The string may include spaces, punctuation, and case-sensitive letters if the string is enclosed in double quotation marks (").

Usage

Define information that identifies this particularly APN remap table.

Example

description “APN_remap1 replaces all MNCl## Ids.”
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
end

**Usage**
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Use this command to return to the parent configuration mode.
**wildcard-apn**

Enables or disables the Wildcard APN feature and define the default APN to be used whenever a wildcard APN is included in the subscriber record.

**Product**
- MME
- SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > APN Remap Table Configuration

```
configure > apn-remap-table table_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(apn-remap-table_name)#
```

**Syntax**

```
wildcard-apn pdp-type { dual-ipv4v6 | ipv4 | ipv6 | ppp } network-identifier apn_net_id
```

```
no wildcard-apn pdp-type { dual-ipv4v6 | ipv4 | ipv6 | ppp }
```

```
no
```

Disables the wildcard-apn definition from the configuration.

```
pdp-type { dual-ipv4v6 | ipv4 | ipv6 | ppp }
```

Specifies the PDP type.
- *dual-ipv4v6* - for a dual PDP context association with one IPv4 address and one IPv6 address/prefix (SGSN only)
- *ipv4* - for an IPv4 context
- *ipv6* - for an IPv6 context
- *ppp* - for a PPP context

```
network-identifier apn_net_id
```

Identifies one of the APN network identifiers specified via the `apn` command in the Operator Policy configuration mode.

*apn_net_id* is a string of 1 to 62 characters, including letters, digits, dots (.) and dashes (-).

**Usage**

This command is used to define a wildcard APN with the type of PDP context and the APN’s network identifier (NI). This wildcard APN would be used when an APN is not identified. The command should be repeated per PDP type, as needed, to enable wildcard APN for two or more of the PDP types.

The wildcard APN configured with the dual PDP IPv4v6 context will be used in the following scenarios:
• the UE requested a PDP type of IPv4v6
• the UE did not request any specific APN
• the subscription includes wildcard APN with PDP type as IPv4v6.

**Important:** Wildcard APN feature configuration is only valid if the APN remap table is associated with at least one operator policy. The same table can then be associated with an IMEI profile as IMEI-specific Wildcard APN is not supported.

**Example**

Use this command to enable an APN wildcard for PDP type IPv4 and NI *homer1*:

```
wildcard-apn pdp-type ipv4 network-identifier homer1
```
Chapter 26
ATM Port Configuration Mode Commands

The Asynchronous Transfer Mode (ATM) port configuration mode provides the commands to create, configure, bind, and manage the ATM ports on line cards that support ATM, such as the ATM/POS OC-3 single-mode and multi-mode optical line cards.

**Important:** Before using these commands, card framing should be configured for either SDH or SONET with the framing command described in the Card Configuration Mode chapter.

Mode

Exec > Global Configuration > ATM Port Configuration

```
configure > port atm slot_number/port_number
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-port-slot_number/port_number)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
clock-source

This command sets the source of the port’s transmit clock.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > ATM Port Configuration

configure > port atm slot_number/port_number

Entering the above command sequence results in the following prompt:

[local]host_name(config-port-slot_number/port_number)#

Syntax

clock-source { internal-timing | loop-timing }

default clock-source

default
Using this command combination sets the port clock source to internal timing.

internal-timing
Sets the port clock to derive timing from the recovered receive clock.

loop-timing
Sets the port clock to transmit in sync with the system timing.

Usage
Use this command for either SONETports on the SGSN.

⚠️ Important: This command is only available for releases 8.1 or higher.

Example

The following command resets the transmit clock source to internal timing.

default clock-source
description

Defines descriptive text that provides useful information about the port.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > ATM Port Configuration

configure > port atm slot_number/port_number

Entering the above command sequence results in the following prompt:

[local]host_name(config-port-slot_number/port_number)#

Syntax

description text

no description

no

Erases the port’s defined description from the configuration file.

text

text must be a string of 1 to 79 alphanumeric characters with no spaces or a string within double quotes that includes printable characters. The description is case-sensitive.

Usage

Set the description to provide helpful information, for example the port’s primary function, services, end users. Define any information, the only limit is the number of characters.

Example

The following example sets a port description that will read in the configuration file:

    description samplePortDescriptiveText

The following example sets a port description that will be easy to read because it retains the spaces between words:

    description "This is a sample description"
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Use this command to return to the parent configuration mode.
line-timing

This command enables the SPIO to recover transmit timing source via the line attached to the selected port. By default, line-timing is not enabled.

⚠️ **Important:** To employ line-timing recovery, the SPIO card(s) must be equipped with the optional Stratum 3 clock module.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > ATM Port Configuration

```
configure > port atm slot_number/port_number
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-port-slot_number/port_number)#
```

**Syntax**

```
[ no ] line-timing
```

<table>
<thead>
<tr>
<th>no</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disables line-timing as the source for the transmit clock.</td>
</tr>
</tbody>
</table>

**Usage**

The port must be enabled (no shutdown) to enable recovery of timing source via the line. As well, the card’s slot number must be entered in the recover line# command in the BITS port configuration mode.

⚠️ **Important:** If the SPIO is connected to an external Building Integrated Timing Supply (BITS) source, BITS timing always takes precedence over line-timing.

**Example**

Disable configured line-timing as the clock source for this port.

```
no line-timing
```
loopback

Enables/disables loopback and configures the type of loopback mode used for diagnostic testing.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > ATM Port Configuration

```
configure > port atm slot_number/port_number
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-port-slot_number/port_number)#
```

**Syntax**

```
loopback { dsl-el-diag | dsl-el-line | none | sonet-sdh-diag | sonet-sdh-line }
```

- **dsl-el-diag**
  Enables a system generated diagnostic lookback signal at the DS1/E1 layer.

- **dsl-el-line**
  Loops back a network diagnostic signal at the DS1/E1 layer.

- **none**
  Stops diagnostic loopback signalling.

- **sonet-sdh-diag**
  Enables a system generated diagnostic lookback signal at the SONET/SDH layer.

- **sonet-sdh-line**
  Loops back a network diagnostic signal at the SONET/SDH layer.

**Usage**
Setup diagnostic loopback signals for troubleshooting purposes.

**Example**
Use the following command to setup loopback diagnosis:

```
loopback dsl-el-diag
```

Use the following command to disable loopback:

```
loopback none
```
preferred slot

This command identifies which card in a chassis assumes revertive (redundancy auto-recovery) functionality when the slot/port being configured go down.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > ATM Port Configuration

`configure > port atm slot_number/port_number`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-port-slot_number/port_number)#
```

**Syntax**

```
preferred slot slot#

[ default | no ] preferred slot
```

- **default**
  Default: non-revertive operation.
  Sets the port for non-revertive operation for port redundancy auto-recovery; requiring an administrative user to manually issue a port switch command to return service to the original port.

- **no**
  Disables revertive, or auto-recovery, operation for the port.

- **slot#**
  Identifies the physical slot in the chassis where the preferred line card is installed.

**Usage**

This command enables or disables revertive port redundancy. So after a port failover, when the original port is restored to service (i.e. link up) the system will return service to that port automatically.

This command must be issued on a per port basis, allowing you to configure specific ports to be used on individual LCs or SPIO cards. For example, ports 1 through 4 could be configured as “preferred” on the LC in slot 17 while ports 5 through 8 are “preferred” on the LC in slot 33. In this scenario, both LCs would be in an Active operational state while still providing LC and port redundancy for the other.

Disabled, which is the default setting, causes non-revertive operation; requiring an administrative user to manually issue a port switch command to return service to the original port.

**Example**

The following commands sets revertive port redundancy for ports on the card in slot 17:

```
pREFERRED slot 17
```
**pvc**

This command creates a Permanent Virtual Connection (PVC), including the definition of the associated Virtual Path Identifiers (VPI) and Virtual Connection Identifiers (VCI) for the PVC. By defining a PVC, this command enters into PVC configuration mode. The ATM port supports a maximum of 256 PVC definitions.

**Product**

HNB-GW
SGSN

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > ATM Port Configuration

`configure > port atm slot_number/port_number`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-port-slot_number/port_number)#
```

**Syntax**

```
[ no ] pvc vpi vpi# vci vci# [ type { aal2 [ -cps-payload-size cps_payload_value | aal5 ] } ] [ -noconfirm ]
```

- **no**
  Deletes the PVC’s entry from the configuration.

- **vpi vpi#**
  VPI identifies a unique path to a destination point in the ATM portion of the network. The VPI and the VCI combine to create the PVC between the MS and the destination point. `vpi#` must be an integer, 0 to 255.

- **vci vci#**
  VCI identifies a unique virtual circuit within the associated VPI. `vci#` must be an integer, 0 to 65535.

- **type**
  This keyword is used to define the type of PVC as AAL2 or AAL5 for HNB-GW service configuration within the associated VPI and VCI.

- **aal2**
  This keyword is used to define the type of PVC as AAL2 for HNB-GW service configuration within the associated VPI and VCI.

- **aal5**
  This keyword is used to define the type of PVC as AAL5 for HNB-GW service configuration within the associated VPI and VCI.
**Usage**

Creates a virtual circuit between two specific points that the carrier will use repeatedly. This command is used to define the type of PVC as AAL2 or AAL5 for HNB-GW service configuration. It also configures the CPS payload which is carried out by the AAL2 protocol over ATM. During the call, the payload size is negotiated between HNB-GW and MSC. Default size for payload is 64 but values may range from 1 to 64 Bytes. This command makes the operator to choose the size dynamically.

This command configures the type of PVC to ATM Adaptation Layer2 (AAL2) or ATM Adaptation Layer5 (AAL5) for ATM traffic between HNB-GW and MSC. It also enables the operator to configure the Common Part Sublayer (CPS) payload for AAL2 protocol over ATM for HNB-GW session between MSC and HNB-GW.

**Example**

Define a PVC with VPI 2 and VCI 353.

```
pvc vpi 2 vci 353
```

Following command configures the PVC type as AAL2 with VPI as 2 and VCI as 353. It also configures the CPS payload to 45 bytes over the ATM during the call.

```
pvc vpi 2 vci 353 type aal2 cps-payload-size 45
```
shutdown

Terminates all processes supporting the port or blocks the shutting down of the port. Conversely, this command with the no keyword enables the port.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > ATM Port Configuration

configure > port atm slot_number/port_number

Entering the above command sequence results in the following prompt:

[local]host_name(config-port-slot_number/port_number)#

Syntax

[ no ] shutdown

no

Enables the port’s administrative state. When this command is omitted from the configuration, the card is shutdown (removed from service).

Usage
Shut down a port prior to re-cabling and/or other maintenance activities. This is the default state of each port upon installation and initial configuration.
This command with the no keyword is required to bring a port into active service.

Example
The following command enables the port for service:

no shutdown

The following command disables the port and takes it out of service:

shutdown
snmp trap link-status

Enables/disables the generation and sending of an SNMP (notification) trap when the port experiences a change of state (up or down).

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > ATM Port Configuration

```
configure > port atm slot_number/port_number
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-port-slot_number/port_number)#
```

**Syntax**

```
[ no ] snmp trap link-status
```

- **no**
  Disables the sending of traps for link-status changes.

**Usage**

Enable the sending of link-status change traps for this port if there is a monitoring facility that can use the information or if there are troubleshooting activities in progress.

**Example**

Use the following command to send SNMP link-status traps for this port:

```
snmp trap link-status
```

Use the following command to disable the sending SNMP link-status traps for this port:

```
no snmp trap link-status
```
**threshold high-activity**

Configures the port’s high and low activity thresholds.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > ATM Port Configuration

```bash
configure > port atm slot_number/port_number
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-port-slot_number/port_number)#
```

**Syntax**

```bash
threshold high-activity high_thresh   [ clear low_thresh ]
```

**default threshold high-activity**

- **default**
  Restores both port high-activity thresholds to the system default of 50 percent.

- **high_thresh**
  Default: 50
  Sets the threshold for the highest percentage of port activity that must be met or exceeded, within the polling interval, to generate an alert or alarm.
  `high_thresh_\%` can be configured to any integer value between 0 and 100.

- **clear low_thresh**
  Default: 50
  Sets the threshold for the lowest percentage level of port activity that must be met to generate and send a clear alarm. If port activity does not drop to or below this threshold then the alarm is maintained.
  `low_thresh_\%` can be configured to any integer value between 0 and 100.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**

High port activity thresholds generate alerts or alarms based on the utilization percentage of each configured port during the specified polling interval. This threshold is configured on a per-port basis. Alerts or alarms are triggered for high port activity based on the following rules:

- **Enter condition:** Actual percent utilization of a port > High Threshold
- **Clear condition:** Actual percent utilization of a port < Low Threshold
If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval. Refer to the `threshold poll` command in the *Global Configuration Mode Commands* chapter of this reference to configure the polling interval and the `threshold monitoring` command in this chapter to enable thresholding for this value.

**Example**

The following command configures a high port utilization threshold of 70 percent and a low threshold of 50 percent for a system using the Alarm thresholding model:

```
threshold high-activity 70 clear 50
```
threshold monitoring

Enables thresholding for port-level values.

Product
HNB-GW
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > ATM Port Configuration

configure > port atm slot_number/port_number

Entering the above command sequence results in the following prompt:

[local]host_name(config-port-slot_number/port_number)#

Syntax

[ default | no ] threshold monitoring

default
Restores the system default to disable threshold monitoring for port-level values.

no
Disables threshold monitoring for port-level values. This is the default setting.

Usage

Thresholding on the system is used to monitor the system for conditions that could potentially cause errors or outage. Typically, these conditions are temporary (i.e. high-activity) and are quickly resolved. However, continuous or large numbers of these error conditions within a specific time interval may be indicative of larger, more severe issues. The purpose of thresholding is to help identify potentially severe conditions so that immediate action can be taken to minimize and/or avoid system downtime.

Thresholding reports conditions using one of the following mechanisms:

• **SNMP traps**: SNMP traps have been created that indicate the condition (high threshold crossing and/or clear) of each of the monitored values. Complete descriptions and other information pertaining to these traps is located in the starentMIB(8164).starentTraps(2) section of the SNMP MIB Reference.

The generation of specific traps can be enabled or disabled on the system allowing you to view only those traps that are most important to you.

• **Logs**: The system provides a facility called threshold for which active and event logs can be generated. As with other system facilities, logs are generated Log messages pertaining to the condition of a monitored value are generated with a severity level of WARNING.

• **Alarm System**: High threshold alarms generated within the specified polling interval are considered “outstanding” until the condition no longer exists and/or a condition clear alarm is generated.

“Outstanding” alarms are reported to through the system’s alarm subsystem and are viewable through the system’s CLI.

The following table indicates the reporting mechanisms supported by each of the above models.
Table 16. Thresholding Reporting Mechanisms by Model

<table>
<thead>
<tr>
<th>Model</th>
<th>SNMP Traps</th>
<th>Logs</th>
<th>Alarm System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Alarm</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

This command enables thresholding for port-level values. Refer to the sections covering threshold high-activity, threshold rx-utilization, and threshold tx-utilization commands in this chapter for information on configuring these values. In addition, refer to the threshold poll command in the Global Configuration Mode Commands chapter of this reference for information on configuring the polling interval over which these values are monitored.
threshold rx-utilization

Configures thresholds for receive-port utilization.

Product
HNB-GW
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > ATM Port Configuration
configure > port atm slot_number/port_number

Entering the above command sequence results in the following prompt:

[local]host_name(config-port-slot_number/port_number)#

Syntax

threshold rx-utilization high_thresh [ clear low_thresh ]

default threshold rx-utilization

default
Restores both rx-utilization thresholds to the system default of 80 percent.

high_thresh
Default: 80
The high threshold receive port utilization percentage that must be met or exceeded within the polling interval to generate an alert or alarm.
The percentage can be configured to any integer value between 0 and 100.

clear low_thresh
Allows the configuration of the low threshold.
Default: 80
The low threshold receive port utilization percentage that maintains a previously generated alarm condition. If the utilization percentage falls below the low threshold within the polling interval, a clear alarm will be generated.
The percentage can be configured to any integer value between 0 and 100.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.
Usage

Receive port utilization thresholds generate alerts or alarms based on the utilization percentage of each configured port in relation to data received during the specified polling interval. This threshold is configured on a per-port basis.

**Important:** Ports configured for half-duplex do not differentiate between data received and data transmitted. Therefore, to avoid redundant alarms, it is recommended that only the receive or transmit utilization threshold be configured.

Alerts or alarms are triggered for receive port utilization based on the following rules:

- **Enter condition:** Actual percent utilization of a port for received data > High Threshold
- **Clear condition:** Actual percent utilization of a port for received data < Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the `threshold poll` command in the Global Configuration Mode Commands chapter of this reference to configure the polling interval and the `threshold monitoring` command in this chapter to enable thresholding for this value.

Example

The following command configures a receive port high utilization threshold percent of 70 and a low threshold of 50 for an system using the Alarm thresholding model:

```
threshold rx-utilization 70 clear 50
```
**threshold tx-utilization**

Configures thresholds for transmit port utilization.

**Product**

HNB-GW
SGSN

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > ATM Port Configuration

`configure > port atm slot_number/port_number`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-port-slot_number/port_number)#
```

**Syntax**

```
threshold tx-utilization high_thresh [ clear low_thresh ]
default threshold tx-utilization
```

**default**

Restores the port tx-thresholds to their system defaults of 80 percent.

**high_thresh**

Default: 80
The high threshold transmit port utilization percentage that must be met or exceeded within the polling interval to generate an alert or alarm.
The percentage can be configured to any integer value between 0 and 100.

**clear low_thresh**

Allows the configuration of the low threshold.
Default: 80
The low threshold transmit port utilization percentage that maintains a previously generated alarm condition.
If the utilization percentage falls below the low threshold within the polling interval, a clear alarm will be generated.
The percentage can be configured to any integer value between 0 and 100.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**

Transmit port utilization thresholds generate alerts or alarms based on the utilization percentage of each configured port in relation to data transmitted during the specified polling interval. This threshold is configured on a per-port basis.
**Important:** Ports configured for half-duplex do not differentiate between data received and data transmitted. Therefore, to avoid redundant alarms, it is recommended that only the receive or transmit utilization threshold be configured.

Alerts or alarms are triggered for transmit port utilization based on the following rules:

- **Enter condition:** Actual percent utilization of a port for transmit data > High Threshold
- **Clear condition:** Actual percent utilization of a port for transmit data < Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval. Refer to the `threshold poll` command in the Global Configuration Mode Commands chapter of this reference to configure the polling interval and the `threshold monitoring` command in this chapter to enable thresholding for this value.

**Example**

The following command configures a transmit port high utilization threshold percent of 70 and a low threshold of 50 for a system using the Alarm thresholding model:

```
threshold tx-utilization 70 clear 50
```
**toh-sdsf**

Enable/disable line SDSF BER thresholds and configure the line transport overhead (TOH) signal degrade and signal failure (SDSF) bit error rate (BER) threshold.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > ATM Port Configuration

```
configure > port atm slot_number/port_number
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-port-slot_number/port_number)#
```

**Syntax**

```
toh-sdsf toh_value

default toh-sdsf
```

**default toh-sdsf**

Resets the default which disables this threshold.

**toh_value**

To facilitate configuration the SD and SF rates have been combined into a single setting.

- 0: Disabled
- 1 - 1.E-04
- 2 - 1.E-05
- 3 - 1.E-06
- 4 - 1.E-07
- 5 - 1.E-08
- 6 - 1.E-09
- 7 - 1.E-10
- 8 - 1.E-11

**Usage**

This command is typically configured in combination with configuring APS/MSP redundancy for the line card - see the `aps` and the `redundancy` commands documented in the Card Configuration Mode Commands chapter.

This command can be used to configure the line threshold whether the port is active or standby and sets a standard option for the paired values of the line’s signal degrade and signal failure (SDSF) BER.
The SD is kept at a value of 100 erroredBits/sec less than the corresponding value of the SF. So if the SD threshold is configured at 1 error in every 100000 bits/sec, then the SF threshold automatically becomes 1 error in every 1000 bits/sec.

The port will go operationally down as soon as the SD threshold is crossed.

Example

Set the SD and SF rates to 1.E-04:

```
toh-sdsf 1
```
Chapter 27
BFD Configuration Mode Commands

The BFD Configuration Mode manages the protocol settings for Bidirectional Forwarding Detection (BFD).

BFD provides a low-overhead, short duration method of detecting failures in the forwarding path between two BGP or OSPF adjacent routers, including the interfaces, data links, and forwarding plane. BFD must be enabled on both routers. The ASR 5000 and ASR 5500 supports BFD on Layer 3 clients only in asynchronous mode with optional Echo functionality.

Mode

Exec > Global Configuration > Context Configuration > BFD Configuration
configure > context context_name > bfd-protocol

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-bfd)#

⚠️ **Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
**bfd multihop-peer**

Configures parameters for any multihop-BFD sessions with the same destination address. If these parameters are not configured via this command, MH-BFD sessions with the same destination address will be in the Admin-down state.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > BFD Configuration

```
configure > context context_name > bfd-protocol
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-bfd)#
```

**Syntax**

```
bfd multihop-peer dst-ip-address { authentication { md5 | meticulous-md5 | meticulous-sha1 plain-text | sha1 } { encrypted password-string | password password-string } | interval tx_interval min_rx rx_interval multiplier value } 
```

```
no bfd multihop-peer dst-ip-address authentication
```

**dst-ip-address**

Specifies the destination address of the BFD enabled peer in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation. This destination address must have been previously configured via the `ip route static bfd` or `ipv6 route static bfd` commands in the Context Configuration mode.

**authentication { md5 | meticulous-md5 | meticulous-sha1 plain-text | sha1**

Specifies the method for authenticating all multihop BFD sessions to the specified peer. By default, authentication for Multihop-BFD sessions to a destination address is disabled. The authentication type options include:

- **md5** – Message Digest 5
- **meticulous-md5** – MD5 using a secret key and sequence numbers updated for every packet
- **meticulous-sha1** – SHA1 with sequence numbers updated for every packet
- **plain-text** – plain text (unencrypted)
- **sha1** – Secured Hash Algorithm 1

**encrypted password-string | password password-string**

Specifies the password for authentication of BFD sessions. The password must be the same between the peer neighbors for the BFD sessions to work. If the authentication password is configured incorrectly between
peers, the BFD sessions to the destination address will not come UP. If the password is configured for BFD sessions that are already UP, BFD neighbors will be reset.

**encrypted password-string:** Specifies the use of an encrypted password for authentication of BFD sessions as an alphanumeric string of up to 523 characters.

**password password-string:** Specifies the use of a plain text password for authentication of BFD sessions as an alphanumeric string of 1 through 19 characters.

---

**Important:** The destination address and its transmit/receive intervals must be configured before the password is applied to any MH-BFD sessions at a destination address.

```
interval tx_interval min_rx rx_interval multiplier value
```

- **interval tx_interval:** Specifies the transmit interval (in milliseconds) between BFD packets as an integer from 50 through 999. Default: 50
- **min_rx rx_interval:** Specifies the receive interval (in milliseconds) between BFD packets as an integer from 50 through 999. Default: 50
- **multiplier value:** Specifies the multiplier value used to compute holddown as an integer from 3 through 50. Default: 3

---

**Usage**

Use this command to configure basic operating parameters between BFD enabled peers.

**Example**

```
bfd multihop-peer 10.2.3.4 authentication md5 encrypted 5-klm7783bfd
multihop-peer 10.2.3.4 interval 100 min_rx 100 multiplier 5
```
**bfd nbr-group-name**

Configures BFD neighbor groups.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > BFD Configuration

```
configure > context context_name > bfd-protocol
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-bfd)#
```

**Syntax**

```
[no] bfd nbr-group-name neighbor-group { active-if-name if-name | passive-if-name if-name }
  gw-ip-address
```

```
no bfd nbr-group-name neighbor-group
```

```
no
```

Removes all the parameters for the BFD neighbor group.

```
neighbor-group
```

Specifies an identifier for a BFD neighbor group as an alphanumeric string of 1 through 19 characters.

```
active-if-name if-name | passive-if-name if-name
```

Specifies the logical/physical interface associated with this BFD group. 
**active-if-name if-name**: Specifies an active interface that notifies all passive interfaces in this group. There should be only one active interface in a group. *if-name* is a logical or physical interface specified as an alphanumeric string of 1 through 79 characters.

**passive-if-name if-name**: Specifies a passive interface that receives BFD notifications from the active interface in this group. *if-name* is a logical or physical interface specified as an alphanumeric string of 1 through 79 characters.

```
gw-ip-address
```

Specifies the gateway address of the BFD neighbor in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation (optional CIDR notation).

**Usage**

Allow scaling of BFD sessions when a large number of logical interfaces are configured on a physical interface. A failure on the physical interface or a logical interface can be propagated to all passive interfaces in this group.

**Example**

...
bfd nbr-group-name bgp group132 active-if-name bgp if02
echo

Enables or disables BFD echo mode functionality. The Echo function tests the forwarding path on the remote system. Echo is only used for single hop BFD sessions.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > BFD Configuration

`configure > context context_name > bfd-protocol`

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-bfd)#`

**Syntax**

```
[ no ] echo
```

---

- **no echo**
  
  Disables BFD echo functionality.

**Usage**

Use this function to send a stream of Echo packets that the other endpoint then sends back via its forwarding plane. Echo tests the forwarding path on the remote system.
**end**

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**

Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Use this command to return to the parent configuration mode.
slow-timers

Specifies the asynchronous mode control packet interval when Echo mode is enabled. In BFD asynchronous mode, BFD-enabled peers periodically send BFD Control packets to one another. If a number of those packets in a row are not received within the specified interval by the other peer, the session is declared to be down.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > BFD Configuration

`configure > context context_name > bfd-protocol`

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-bfd)#`

**Syntax**

```
slow-timers timer-value

no slow-timers
```

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
</tr>
<tr>
<td>Disables previously specified BFD slow timers.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>timer-value</td>
</tr>
<tr>
<td>Specifies the BFD control packet interval (in milliseconds) for Echo mode as an integer from 1000 through 300000. Default: 2000</td>
</tr>
</tbody>
</table>

**Usage**
Use this command to configure the interval between BFD control packets sent between peers in Echo mode.

**Example**
```
slow-timers 10000
```
Chapter 28
BGP Address-Family (IPv4/IPv6) Configuration Mode Commands

The Border Gateway Protocol (BGP) Address-Family (IPv4/IPv6) Configuration Mode is used to configure the IPv4 and IPv6 address family information.

Mode

Exec > Global Configuration > Context Configuration > BGP Configuration > BGP Address-Family Configuration

configure > context context_name > router bgp as_number > address-family

address_family_type

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-bgp-af-v6)#

⚠️ **Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

```exit```

**Usage**

Use this command to return to the parent configuration mode.
maximum-paths

Controls the maximum number of parallel external BGP (eBGP) or internal BGP (iBGP) routes that can be installed in a routing table.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > BGP Configuration > BGP Address-Family Configuration

```
configure > context context_name > router bgp as_number > address-family
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-bgp-af-v6)#
```

**Syntax**

```
[ no ] maximum-paths { ebgp num_paths | ibgp num_paths }
```

- **no**
  Disables the above command.

- **maximum-paths ebgp num_paths**
  Specifies the maximum number of parallel External Border Gateway Protocol routes as an integer from 1 through 10.

- **maximum-paths ibgp num_paths**
  Specifies the maximum number of parallel Internal Border Gateway Protocol routes as an integer from 1 through 10.

**Important:** If configured under the router-bgp-mode, multipath is enabled only for the prefixes learnt in the default-vrf. There is no support for vpnv4 prefixes even though multipath is turned on for the default-vrf. If configured under the address-family-vrf-mode, multipath is enabled only for prefixes learnt in the vrf.

**Usage**
Use this command to forward packets over multiple paths. User can control the maximum number of parallel eBGP routes that can be installed in a routing table. Enabling multipath does not affect the best path selection in BGP. If multipath is enabled, all the paths with the same weight, local-preference, as-path length, origin, and multi-exit discriminator (MED) as the best path are added to the routing table.

**Example**
The following command disables forward of packets over multiple paths:

```
no maximum-paths ebgp
```
**neighbor**

Configures the IPv4/IPv6 Address Family for BGP routers that interconnect to non-broadcast networks.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > BGP Configuration > BGP Address-Family Configuration

```
configure > context context_name > router bgp as_number > address-family address_family_type
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-bgp-af-v6)#
```

**Syntax**

```
[ no ] neighbor ip_address { activate | advertisement-interval adv_time | capability graceful-restart | default-originate [ route-map map_name ] | distribute-list dist_list { in | out } | ebgp-multihop [ max-hop number ] encrypted password encryp_password fall-over bfd multihop | filter-list filt_list { in | out } | max-prefix max_num [ threshold thresh_percent ] | warning-only ] next-hop-self | password password | remote-as AS_num | remove-private-AS | restart-time rest_time | route-map map_name { in | out } | send-community { both | extended | standard } | shutdown | srp-activated-soft-clear | timers { connect-interval connect_interval [ keepalive-interval keepalive_interval holdtime-interval holdtime_interval ] } | keepalive-interval keepalive_interval holdtime-interval holdtime_interval { connect-interval connect_interval | min-peer-holdtime-interval min_peer_hold_interval [ connect-interval connect_interval ] } } | update-source ip_address | weight value }
```

**no**

Delete the specified parameter from the router configuration.

**neighbor ip_address**

Specifies the IP address of a BGP neighbor. *ip_address* must be in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

**activate**

Enables the exchange of routes with this neighbor.

**advertisement-interval adv_time**

Specifies the minimum interval (in seconds) between sending BGP routing updates. *adv_time* must be an integer from 0 through 600. Default: 30

**capability graceful-restart**

Configures graceful re-start attributes.
### default-originate [ route-map map_name ]

Specifies the default originate routes to this neighbor

**route-map map_name**: Specifies the route-map that contains the criteria to originate default routes.

**map_name** must be the name of an existing route-map in the current context.

### distribute-list dist_list { in | out }

Filters updates to and from this neighbor based on a route access list. Default: No filtering is performed.

**dist_list** is the name or number of an existing route-access-list.

**in**: Indicates that incoming advertised routes should be filtered.

**out**: Indicates that outgoing advertised routes should be filtered.

### ebgp-multihop [ max-hop number ]

Allows eBGP neighbors that are not on directly connected networks.

**max-hop number**: Specifies the maximum number of hops allowed to reach a neighbor as an integer from 1 through 255. Default hop count: 255

### encrypted password encryp_password

Specifies the encrypted password that is used only inside configuration files. This is an alphanumeric string of 1 through 24 characters.

### fall-over bfd multihop

Supports Bidirectional Forwarding Detection (BFD) multihop for fallover.

### filter-list filt_list { in | out }

Establishes BGP filters based on an autonomous system (AS) path access list. **filt_list** is name of an existing AS path access list.

**in**: Indicates that incoming advertised routes will be filtered.

**out**: Indicates that outgoing advertised routes will be filtered.

### max-prefix max_num [ threshold thresh_percent ] [ warning-only ]

Specifies the maximum number of prefixes accepted from this peer. When the maximum is exceeded the neighbor connection is reset. **max_num** is an integer from 1 through 4294967295. Default: No maximum prefix limit.

**threshold thresh_percent**: Specifies a percentage value of when the BGP table is full. When this value is reached peer warnings are sent to the neighbor. **thresh_percent** must be an integer from 1 through 100.

**warning-only**: Specifies that only a warning message is sent when the limit is exceeded. The neighbor connection is not reset.

### next-hop-self ip_address

Disables the next hop calculation for this neighbor.

### password password

Sets a **password** expressed as an alphanumeric string of 1 through 24 characters.

### remote-as AS_num

Specify the AS number of the BGP neighbor as an integer from 1 through 4294967295.
remove-private-AS
Removes the private AS number from outbound updates. Default: Do not remove the private AS number.

restart-time rest_time
Specifies the maximum time (in seconds) required to for neighbor to restart as an integer from 1 through 3600.

route-map map_name { in | out }
Applies a route map to the neighbor. map_name must be the name of an existing route-map in the current context.
in: Indicates that the route map applies to incoming advertisements.
out: Indicates that the route map applies to outgoing advertisements.

send-community{ both | extended | standard }
Sends the community attributes to a peer router (neighbor).
both:Sends standard and extended community attributes
extended:Sends extended community attributes.
standard:Sends standard community attributes.

shutdown
Administratively shuts down this neighbor. This disables exchanging routes or configuring parameters for this neighbor.

srp-activated-soft-clear
Enables BGP updates when SRP-enabled resources are modified.

timers { [ [ connect-interval connect_interval ] | [ keepalive-interval keepalive_interval holdtime-interval holdtime_interval ] ] }
Sets BGP timers for the specified neighbor.
connect-interval connect_interval: Specifies the connect timer (in seconds) as an integer from 0 through 65535. The default is 60 seconds.
keepalive-interval keepalive_interval: Specifies the frequency (in seconds) at which the current BGP router sends keepalive messages to its neighbor. keep_time must be an integer from 0 through 65535. The default is 30 seconds.
holdtime-interval holdtime_interval: Specifies the interval (in seconds) the router waits for a keepalive message before declaring a neighbor dead. hold_time must be an integer from 0 through 65535. The default is 90 seconds.
min-peer-holdtime-interval min_peer_hold_interval: Specifies the minimum acceptable hold time (in seconds) from peer for a keepalive message before declaring a neighbor dead.
min_peer_hold_interval must be an integer from 0 through 65535. The default is 90 seconds.

update-source ip_address
Binds the specified IP address to the BGP socket that is used to communicate to the peer. ip_address is an IPv4 address in dotted-decimal notation.
In most cases you should set the update-source address to the address of the loopback interface in the current context. By doing this, the TCP connection does not go down until there is no route for the loopback address in the peering router.
weight value
Sets the default weight for routes from this neighbor as an integer from 0 through 65535. Default: 0

Usage
Use this command to set parameters for communication with a specified neighbor. The chassis supports a maximum of 64 peers per context.

Important: A remote AS number must be specified for a neighbor before other parameters can be configured.

Example
The following command specifies that the neighbor at the IP address 192.168.100.25 has an AS number of 2000:

```
neighbor 192.168.100.25 remote-as 2000
```

The following command allows BGP neighbors that are a maximum of 27 hops away:

```
neighbor 192.168.100.25 ebgp-multihop max-hop 27
```

The following command sets the minimum interval between sending routing updates to 3 minutes (180 seconds):

```
neighbor 192.168.100.25 advertisement-interval 180
```

The following command sets the default weight for all routes from the specified neighbor to 100:

```
neighbor 192.168.100.25 weight 100
```
network

Configures and specifies a network to announce via BGP.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > BGP Configuration > BGP Address-Family Configuration

configure > context context_name > router bgp as_number > address-family
address_family_type

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-bgp-af-v6)#

Syntax

[ no ] network ip_address/mask [ route-map map_name ]

no
Delete the specified network from the configuration for the BGP router.

network ip_address/mask

Specifies the IP address and netmask bits for the network to announce via BGP. ip_address is a network IP address in IPV4 dotted-decimal notation and mask is the number of subnet bits, representing a subnet mask in CIDR. These must be entered in the IPv4 dotted-decimal notation/subnet bits format.

route-map map_name

Filter routes through the specified route map before announcing the network. map_name specifies the name of the route-map to use as an alphanumeric string of 1 through 79 characters.

Usage

Use this command to specify a network to announce via BGP.

Example

The following command announces the network 192.168.0.0 with a netmask of 16 via BGP:

network 192.168.0.0/16

The following command removes the network from the BGP router configuration:

no network 192.168.0.0/16
redistribute

Redistributes routes into BGP from another protocol as BGP neighbors.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > BGP Configuration > BGP Address-Family Configuration

```
configure > context context_name > router bgp as_number > address-family address_family_type
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-bgp-af-v6)#
```

**Syntax**

```
[ no ] redistribute { connected | ospf | rip | static } [ route-map map_name ]
```

- **no**
  Remove the specified redistribution parameters from the BGP router configuration.

- **redistribute connected**
  Specifies that connected routes will be redistributed.

- **redistribute ospf**
  Specifies that Open Shortest Path First (OSPF) routes will be redistributed.

- **redistribute rip**
  Specifies that Routing Information Protocol (RIP) routes will be redistributed. (RIP is not supported at this time.)

- **redistribute static**
  Specifies that static routes will be redistributed.

- **route-map map_name**
  Filters routes through the specified route map before redistribution. `map_name` specifies the name of the route-map to use as an alphanumeric string of 1 through 79 characters.

**Usage**

Use this command to specify what routes this BGP router should redistribute into BGP.

**Example**

The following command redistributes OSPF routes after filtering them through the route map named `Map1`:
redistribute ospf route-map Map1

The following command removes the redistribution of OSPF routes from the router’s configuration:

no redistribute ospf route-map Map1
The Border Gateway Protocol (BGP) Address-Family (VPNv4/VPNv6) Configuration Mode is used to configure the VPNv4 or VPNv6 address family information.

**Mode**

Exec > Global Configuration > Context Configuration > BGP Configuration > BGP Address-Family Configuration

```
configure > context context_name > router bgp as_number > address-family
address_family_type
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-bgp-af-v4)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
Exit

Exits the current mode and returns to the parent configuration mode.

Usage
Use this command to return to the parent configuration mode.
neighbor

Configures the VPNv4 or VPNv6 address family on BGP routers that interconnects to non-broadcast networks and enables the exchange of routing information with a peer router (neighbor).

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > BGP Configuration > BGP Address-Family Configuration

configure > context context_name > router bgp as_number > address-family address_family_type

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-bgp-af-v4)#

Syntax

[ no ] neighbor ip_address { activate | send-community { both | extended | standard } }

no
Delete the specified parameter from the router configuration.

neighbor ip_address
Specifies the IP address of the peer router (neighbor) in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

activate
Enables the exchange of routing information with this neighbor.

send-community { both | extended | standard }
Sends the community attributes to a peer router (neighbor).
both: Sends standard and extended community attributes.
extended: Sends extended community attributes.
standard: Sends standard community attributes.

Usage
Use this command to enable the exchange of routing information with a peer router. The chassis supports a maximum of 64 peers per context.

Example
The following command enables the exchange of routing information with the neighbor at IP address 192.168.100.25:

neighbor 192.168.100.25 activate

Cisco ASR 5x00 Command Line Interface Reference
Chapter 30
BGP Address-Family (VRF) Configuration Mode Commands

The Border Gateway Protocol (BGP) Address-Family (VRF) Configuration Mode is used to configure the Virtual Routing and Forwarding address family information.

Mode

Exec > Global Configuration > Context Configuration > BGP Configuration > BGP Address-Family Configuration

configure > context context_name > router bgp as_number > address-family address_family_type

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-bgp-af-vpnv4)#

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Use this command to return to the parent configuration mode.
neighbor

Configures the Virtual Routing and Forwarding (VRF) address family for BGP routers that interconnect to non-broadcast networks.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > BGP Configuration > BGP Address-Family Configuration

configure > context context_name > router bgp as_number > address-family address_family_type

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-bgp-af-vpnv4)#

Syntax

[ no ] neighbor ip_address { activate | advertisement-interval adv_time | default-originate [ route-map map_name ] | distribute-list dist_list { in | out } | ebgp-multihop [ max-hop number ] | filter-list filt_list { in | out } | max-prefix max_num [ threshold thresh_percent ] [ warning-only ] | remote-as AS_num | remove-private-AS | route-map map_name { in | out } | shutdown | srp-activated-soft-clear | timers { [ connect-interval conn_time ] | [ keepalive-interval keep_time holdtime-interval hold_time ] } } | update-source ip_address | weight value }

no
Delete the specified parameter from the router configuration.

neighbor ip_address

Specifies the IP address of the peer router (neighbor) in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

activate

Enables the exchange of routes with this neighbor.

advertisement-interval adv_time

The minimum interval (in seconds) between sending BGP routing updates.

adv_time must be an integer from 0 through 600.

Default: 30

default-originate [ route-map map_name ]

Originate default routes to this neighbor

route-map map_name: Specifies the route-map that contains the criteria to originate default routes.

map_name must be the name of an existing route-map in the current context.
**distribute-list dist_list {in | out}**
Filter updates to and from this neighbor based on a route access list.
Default: No filtering is performed.
*dist_list*: The name or number of an existing route-access-list.
*in*: Indicates that incoming advertised routes should be filtered.
*out*: Indicates that outgoing advertised routes should be filtered.

**ebgp-multihop [max-hop number]**
Allow external BGP (eBGP) neighbors not on directly connected networks.
*max-hop number*: The maximum number of hops allowed to reach a neighbor. *number* must be an integer from 1 through 255.
Default hop count: 255

**filter-list filt_list { in | out }**
Establish BGP filters based on an AS path access list
*filt_list*: The name of an existing AS path access list.
*in*: Indicates that incoming advertised routes will be filtered.
*out*: Indicates that outgoing advertised routes will be filtered.

**max-prefix max_num [ threshold thresh_percent ] [ warning-only ]**
The maximum number of prefixes accepted from this peer. When the maximum is exceeded the neighbor connection is reset.
*max_num*: Specifies the maximum number of prefixes permitted. This must be an integer from 1 through 4294967295.
Default: No maximum prefix limit.
*threshold thresh_percent*: A percentage value which specifies that when the BGP table is the specified percentage full from this peer warnings are sent to the neighbor. *thresh_percent* must be an integer from 1 through 100.
*warning-only*: This keyword specifies that only a warning message is sent when the limit is exceeded. The neighbor connection is not reset

**remote-as AS_num**
Specify the AS number of the BGP neighbor.
*AS_num*: The neighbor’s autonomous system number. must be an integer from 1 through 65535.

**remove-private-AS**
Remove the private AS number from outbound updates.
Default: Do not remove the private AS number.

**route-map map_name { in | out }**
Apply a route map to the neighbor.
*map_name*: Specifies the route-map apply. *map_name* must be the name of an existing route-map in the current context.
*in*: Indicates that the route map applies to incoming advertisements.
*out*: Indicates that the route map applies to outgoing advertisements.
shutdown
Administratively shut down this neighbor. This disables exchanging routes or configuring parameters for this neighbor.

srp-activated-soft-clear
Enables BGP updates when SRP-enabled resources are modified.

timers {
connect-interval conn_time } | \[ keepalive-interval keep_time
holdtime-interval hold_time ]
BGP timers for the specified neighbor.
connect-interval conn_time: Specifies the connect timer in seconds. conn_time must be an integer from 0 through 65535. The default is 60 seconds.
keepalive-interval keep_time: The frequency (in seconds) at which the current BGP router sends keepalive messages to its neighbor. keep_time must be an integer from 0 through 65535. The default is 30 seconds.
Holdtime-interval hold_time: The interval (in seconds) the router waits for a keepalive message before declaring a neighbor dead. hold_time must be an integer from 0 through 65535. The default is 90 seconds.

update-source ip_address
use this keyword to bind the specified IP address to the BGP socket that is used to communicate to the peer. ip_address is an IPv4 address in dotted-decimal notation.
In most cases you should set the update-source address to the address of the loopback interface in the current context. By doing this, the TCP connection does not go down until there is no route for the loopback address in the peering router.

weight value
This command sets the default weight for routes from this neighbor.
value: This must be an integer from 0 through 65535.
Default: 0

Usage
Use this command to set parameters for communication with a specified neighbor. The chassis supports a maximum of 64 peers per context.

Important: A remote AS number must be specified for a neighbor before other parameters can be configured.

Example
The following command specifies that the neighbor at the IP address 192.168.100.25 has an AS number of 2000:

neighbor 192.168.100.25 remote-as 2000

The following command allows BGP neighbors that are a maximum of 27 hops away:

neighbor 192.168.100.25 ebgp-multihop max-hop 27

The following command sets the minimum interval between sending routing updates to 3 minutes (180 seconds):

neighbor 192.168.100.25 timers 3 3 3

Cisco ASR 5x00 Command Line Interface Reference
neighbor 192.168.100.25 advertisement-interval 180

The following command sets the default weight for all routes from the specified neighbor to 100:

neighbor 192.168.100.25 weight 100
**redistribute**

Redistributes routes into BGP. This means that any routes from another protocol are redistributed to BGP neighbors using the BGP protocol.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > BGP Configuration > BGP Address-Family Configuration

```
configure > context context_name > router bgp as_number > address-family
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-bgp-af-vpnv4)#
```

**Syntax**

```
[no] redistribute {connected | ospf | rip | static} [route-map map_name]
```

- **no**
  
  Remove the specified redistribution parameters from the BGP router configuration.

- **connected**

  Specifies that connected routes will be redistributed.

- **ospf**

  Specifies that Open Shortest Path First (OSPF) routes will be redistributed

- **rip**

  Specifies that Routing Information Protocol (RIP) routes will be redistributed. (RIP is not supported at this time.)

- **static**

  Specifies that static routes will be redistributed.

- **route-map map_name**

  Filter routes through the specified route map before redistribution.

  *map_name* specifies the name of the route-map to use and must be specified as an alphanumeric string of 1 through 79 characters.

**Usage**

Use this command to specify what routes this BGP router should redistribute into BGP.
The following command redistributes OSPF routes after filtering them through the route map named Map1:

```
redistribute ospf route-map Map1
```

The following command removes the redistribution of OSPF routes from the router’s configuration:

```
no redistribute ospf route-map Map1
```
Chapter 31
BGP Configuration Mode Commands

The Border Gateway Protocol (BGP) Configuration Mode is used to configure properties for BGP-4 routing.

Mode

Exec > Global Configuration > Context Configuration > BGP Configuration

configure > context context_name > router bgp as_number

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-bgp)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
accept-zero-as-rd

Configures to accept VPN prefixes with Router Distinguisher(RD) value having Administrator Subfield, which is an Autonomous System number 0.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > BGP Configuration
configure > context context_name > router bgp as_number

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-bgp)#

Syntax

[ no ] accept-zero-as-rd

no

Removes the configured VPN prefixes with RD value having AS number 0.

Usage
Use this command to configure VPN prefixes with RD value having Administrator Subfield, which is an Autonomous System number 0.
By default the existing behavior of ASR5K will be preserved.

Example
Following command configures to accept VPN prefixes with RD value having AS number 0:

accept-zero-as-rd
address-family ipv4

Configures the IPv4 Address Family information for the specified BGP Autonomous System (AS) number. Optionally, it also enables the Virtual Routing and Forwarding (VRF) routing information, if specified.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > BGP Configuration
configure > context context_name > router bgp as_number

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-bgp)#

Syntax

[ no ] address-family ipv4 [ vrf vrf_name]

no
Removes the configured IPv4 address family VRF mode for specific BGP AS number.

address-family ipv4
Enters the BGP Address-Family IPv4 mode to allow entry of IPv4 BGP parameters for the BGP AS number.

**Important:** The route distinguisher ID must be configured for the VRF name via the `route-distinguisher` command in BGP VRF Configuration mode, before using this keyword.

vrf vrf_name
Enables the exchange of VRF routing information. When this keyword is specified with this command, the address family mode changed to VRF address family mode for specific BGP AS number. `vrf_name` is the name of an existing VFR expressed as an alphanumeric string of 1 through 63 characters.

Usage
Use this command to configure the IPv4 or IPv6 BGP address family configuration parameters and optionally enables the exchange of VRF routing information.
Use of the `address-family ipv4` command switches the command mode to BGP Address Family Configuration Mode; the CLI prompt changes to:

[context_name>]host_name(config-bgp-af-v4)#

Use of `address-family ipv4 vrf vrf_name` command switches the command mode to BGP Address Family Configuration Mode; the CLI prompt changes to:

[context_name>]host_name(config-bgp-af-vrf)#
Example

Use the following command to enter the IPv4 BGP Address-Family configuration mode:

```
address-family ipv4
```

Use following command to enter the IPv4 VRF BGP Address-Family configuration mode for exchange of VRF routing information from VRF `route_vrf1`:

```
address-family ipv4 vrf route_vrf1
```
address-family ipv6

Configures VPNv6 BGP parameters.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > BGP Configuration
configure > context context_name > router bgp as_number

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-bgp)#

Syntax

address-family ipv6

Enters the BGP Address-Family IPv6 mode to allow entry of IPv6 BGP parameters for the BGP AS number.

Usage
Use this command to configure the IPv6 BGP address family configuration parameters for BGP router. Use of address-family ipv6 command switches the command mode to BGP Address Family Configuration Mode and changes the CLI prompt to:

[context_name>]host_name(config-bgp-af-v6)#

Example
Use the following command to enter the IPv6 BGP Address-Family configuration mode:

address-family ipv6
address-family vpv4

Configures the VPNv4 Address Family information for the specified BGP AS number.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > BGP Configuration
configure > context context_name > router bgp as_number

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-bgp)#

Syntax

address-family vpv4

address-family vpv4

Enters the BGP Address-Family VPNv4 mode to allow entry of VPN BGP parameters for the BGP AS number.

Usage
Use this command to configure the VPNv4 address family configuration parameters for BGP router. This command is also used to switch the command mode to enter the BGP Address Family Configuration Mode. Use of address-family vpv4 command switches the command mode to BGP Address Family Configuration Mode; the CLI prompt changes to:

[context_name]>host_name(config-bgp-af-vpv4)#

Example
Use the following command to enter the BGP Address-Family configuration mode for VPNv4 address parameters:

address-family vpv4
**address-family vpnv6**

Configures the VPNv6 Address Family information for the specified BGP AS number.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > BGP Configuration

`configure > context context_name > router bgp as_number`

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-bgp)#`

**Syntax**

```
address-family vpnv6
```

Enters the BGP Address-Family VPNv6 mode to allow entry of VPN BGP parameters for the BGP AS number.

**Usage**

Use this command to configure the VPNv6 address family configuration parameters for BGP router. This command is also used to switch the command mode to enter the BGP Address Family Configuration Mode. Use of `address-family vpnv6` command switches the command mode to BGP Address Family Configuration Mode; the CLI prompt changes to:

```
[context_name>]host_name(config-bgp-af-vpnv6)#
```

**Example**

Use the following command to enter the BGP Address-Family configuration mode for VPNv6 address parameters:

```
address-family vpnv6
```
**bgp**

Defines the BGP-specific parameters regarding graceful restarts.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > BGP Configuration

`configure > context context_name > router bgp as_number`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-bgp)#
```

**Syntax**

```
bgp graceful-restart { restart-time rest_time | stalepath-time stale_time | update-delay delay }
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Removes the specified administrative distance for the specific route.</td>
</tr>
<tr>
<td><code>graceful-restart restart-time rest_time</code></td>
<td>Specifies the maximum time (in seconds) required for neighbor(s) to gracefully restart. <code>rest_time</code> must be an integer from 1 through 3600.</td>
</tr>
<tr>
<td><code>graceful-restart stalepath-time stale_time</code></td>
<td>Specifies the maximum time (in seconds) to retain stale paths from restarting neighbor(s). <code>stale_time</code> must be an integer from 1 through 3600.</td>
</tr>
<tr>
<td><code>graceful-restart update-delay rest_time</code></td>
<td>Specifies the maximum time (in seconds) to defer initial route-selection. <code>update-delay</code> must be an integer from 1 through 3600.</td>
</tr>
</tbody>
</table>

**Usage**

Use this command to set BGP-specific parameters regarding graceful restarts.

**Example**

Use the following command to retain stale paths from restarting neighbor(s) for 100 seconds:

```
bgp graceful-restart stalepath-time 100
```
distance

Defines the administrative distance for routes. The administrative distance is the default priority for a specific route or type route.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > BGP Configuration
configure > context context_name > router bgp as_number

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-bgp)#

Syntax

distance { admin distance prefix prefix_addr [ route-access-list list_name ] | bgp external ebgp_dist internal ibgp_dist local local_dist }

no distance { admin distance prefix prefix_addr [ route-access-list list_name ] | bgp [ external ebgp_dist internal ibgp_dist local local_dist ] }

no

Removes the specified administrative distance for the specific route.

distance admin distance prefix prefix_addr [ route-access-list list_name ]

Sets the administrative distance to a specified value for routes with a specific IP prefix. If you also specify a route access list, the IP prefix must match the rules of that access list.
admin distance: Specifies the administrative distance that you want to apply to the IP prefix. distance must be an integer from 1 through 254.
prefix distance: Specifies the IP prefix of routes that should have the admin distance applied.
prefix_addr must be an IPv4 address in dotted-decimal notation and the number of subnet bits, representing the subnet mask in CIDR shorthand (for example, 10.1.1.1/24).
route-access-list list_name: Defines the name of a route access list that defines for which routes the administrative distance should be set.

distance bgp external ebgp_dist internal ibgp_dist local local_dist

Sets the administrative distance for external (eBGP), internal (iBGP) and local routes.
eexternal ebgp_dist: Sets the administrative distance for eBGP routes. ebgp_dist must be an integer from 1 through 254.
internal ibgp_dist: Sets the administrative distance for iBGP routes. ibgp_dist must be an integer from 1 through 254.
local local_dist: Sets the administrative distance for local routes. local_dist must be an integer from 1 through 254.
**Usage**

Use this command to set the administrative distance for specific routes to values that you specify. These values are only applied to the current router.

**Example**

Use the following command to set the administrative distance to 100 for all routes that have an IP prefix of 192.168.0.0/16 and are specified in a remote access list named *rac11*:

```
distance admin 100 prefix 192.168.0.0/16 route-access-list rac11
```
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
down
```

**Usage**

Use this command to return to the Exec mode.
enforce-first-as

Enforces the first Autonomous System (AS) for Exterior Border Gateway Protocol (eBGP) routes. An AS is a connected group of one or more Internet Protocol prefixes run by one or more network operators which has a single and clearly defined routing policy (RFC 1930).

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > BGP Configuration

`configure > context context_name > router bgp as_number`

Entering the above command sequence results in the following prompt:

```
[context_name] host_name(config-bgp)#
```

Syntax

```
[ no ] enforce-first-as
```

<table>
<thead>
<tr>
<th>no</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disables the enforcement of the first AS for Exterior Border Gateway Protocol (eBGP) routes.</td>
</tr>
</tbody>
</table>

```
enforce-first-as
```

Enables the enforcement of the first AS for Exterior Border Gateway Protocol (eBGP) routes.

Usage

Use this command to enforce the use of the first AS for EBGP routes.

Example

Use the following command to enable this functionality:

```
enforce-first-as
```
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
```
exit
```

**Usage**
Use this command to return to the parent configuration mode.
ip vrf

Adds a preconfigured IP VRF context instance to the BGP ASN and configures the BGP attributes and related parameters to the VRF. This command also switches the command mode to BGP VRF Configuration mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > BGP Configuration

configure > context context_name > router bgp as_number

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-bgp)#
```

**Syntax**

```
[ no ] ip vrf vrf_name
```

**no**

Removes an associated IP VRF from specified BGP AS number and other configured parameters.

**vrf_name**

Specifies the IP VRF context configured in the Context configuration mode and to be associated with a BGP AS number. *vrf_name* must be an alphanumeric string of 1 through 79 characters identifying an existing instance.

**Usage**

Use this command to associate the specified IP VRF context instance to the BGP AS number and configures the BGP attributes and related parameters to the VRF. This command also switches the command mode to BGP VRF Configuration mode.

This command switches the command mode to BGP IP VRF Configuration Mode; the CLI prompt changes to:

```
[context_name>]host_name(config-bgp-vrf)#
```

**Example**

The following command associates the pre-defined VRF context instance *router_mpls* to this BGP AS number:

```
ip vrf router_mpls
```
maximum-paths

Enables forwarding packets over multiple paths and specifies the maximum number of external BGP (eBGP) or internal BGP (iBGP) paths between neighbors.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > BGP Configuration

configure > context context_name > router bgp as_number

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-bgp)#
```

**Syntax**

```
maximum-paths { ebgp max_num | ibgp max_num }
[ no ] maximum-paths { ebgp | ibgp }
```

- **no**
  
  Disables forwarding packets over multiple eBGP or iBGP paths between neighbors.

- **ebgp max_num**
  
  Enables forwarding packets over multiple eBGP paths between neighbors and specifies the maximum number of eBGP paths. `max_num` must be an integer from 1 through 10 or 1 through 32 (VPC-DI only).

- **ibgp max_num**
  
  Enables forwarding packets over multiple iBGP paths between neighbors and specifies the maximum number of iBGP paths. `max_num` must be an integer from 1 through 10 or 1 through 32 (VPC-DI only).

**Usage**

Use this command to enable or disable forwarding packets over multiple paths between neighbors and specify the maximum number of EBGP or IBGP paths.

**Example**

To enable forwarding packets over multiple paths and set the maximum number of EBGP paths to 10, enter the following command:

```
maximum-paths ebgp 10
```

To disable forwarding packets over multiple EBGP paths, enter the following command:

```
no maximum-paths ebgp
```
neighbor

Configures BGP routers that interconnect to non-broadcast networks. Note that a remote AS number must be specified for a neighbor before other parameters can be configured.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > BGP Configuration

```
configure > context context_name > router bgp as_number
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-bgp)#
```

**Syntax**

```
[ no ] neighbor ip_address { activate | advertisement-interval adv_time | capability graceful-restart | default-originate [ route-map map_name ] | distribute-list dist_list { in | out } | ebgp-multihop [ max-hop number ] | encrypted password encrypted password | fall-over bfd [ multihop ] | filter-list filt_list { in | out } | max-prefix max_num [ threshold thresh_percent ] | warning-only | next-hop-self | password password | remote-as AS_num | remove-private-AS | restart-time rest_time | route-map map_name { in | out } | send-community { both | extended | standard } | shutdown | srp-activated-soft-clear | timers { [ connect-interval conn_time ] | [ keepalive-interval keep_time holdtime-interval hold_time ] } | update-source ip_address | weight value }
```

**no**

Delete the specified parameter from the router configuration.

```
neighbor ip_address
```

Specifies the IP address of a BGP neighbor. *ip_address* must be in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

```
activate
```

Enable the exchange of routes with this neighbor.

```
advertisement-interval adv_time
```

The minimum interval (in seconds) between sending BGP routing updates. *adv_time* must be an integer from 0 through 600. Default: 30

```
capability graceful-restart
```

Configures BGP graceful restart attributes.

```
default-originate [ route-map map_name ]
```

Enables the origination of default routes to this neighbor.
**route-map** `map_name`: Specifies the route-map that contains the criteria to originate default routes. 
`map_name` must be the name of an existing route-map in the current context.

**distribute-list** `dist_list` { in | out }

Filters updates to and from this neighbor based on a route access list. `dist_list`: The name or number of an existing route-access-list. Default: No filtering is performed.

- in: Indicates that incoming advertised routes should be filtered.
- out: Indicates that outgoing advertised routes should be filtered.

**ebgp-multihop** [ max-hop `number` ]

Allows EBGP neighbors that are not on directly connected networks.

- [ max-hop ] `number`: Specifies the maximum number of hops allowed to reach a neighbor. `number` must be an integer from 1 through 255. Default hop count: 255

**encrypted password** `encrypted password`

Specifies an encrypted password that is used only inside configuration files. This should be an alphanumeric string of 1 through 523 characters.

**fall-over bfd** [ multihop ]

Enables Bidirectional Forwarding Detection (BFD) multihop support for fallover.

This command adds or modifies a session in BFD for the BGP peer. If there is an existing session in BFD (same source-address/destination address), BGP or OSPF protocol will be added to the list of clients for the BFD session. BGP or OSPF will then be notified when there is a change in the BFD session state.

If there is no such BFD session, a new session is added in BFD. For MH-BFD, the session inherits the parameters including min-tx, min-rx, multiplier and authentication from the multihop-peer configuration in BFD by matching the destination address. If the parameters (interval) are not configured in BFD, then the BFD session will be in Admin-down state.

BGP adds a session in BFD only when the BGP peer is Established state. If there is a state transition in bgp where the peer is no longer in established state, then the bfd session is deleted. It will be added again, once the peer comes back to Established state.

**filter-list** `filt_list` { in | out }

Establishes BGP filters based on an AS path access list. `filt_list` is the name of an existing AS path access list.

- in: Indicates that incoming advertised routes will be filtered.
- out: Indicates that outgoing advertised routes will be filtered.

**max-prefix** `max_num` [ threshold `thresh_percent` ] [ warning-only ]

The maximum number of prefixes accepted from this peer. When the maximum is exceeded the neighbor connection is reset.

Default: No maximum prefix limit.

- `max_num`: Specifies the maximum number of prefixes permitted. This must be an integer from 1 through 4294967295.
- [ threshold `thresh_percent` ]: Specifies a percentage value of when the BGP table is full. When this value is reached, peer warnings are sent to the neighbor and the neighbor connection is reset.

- `thresh_percent`: must be an integer from 1 through 100.
- [ warning-only ]: Specifies that only a warning message is sent when the limit is exceeded. The neighbor connection is not reset.
**next-hop-self**
Disables the next hop calculation for this neighbor.

**password password**
Specifies a password that is only used inside configuration files. This should be an alphanumeric string of 1 through 24 characters.

**remote-as AS_num**
Specify the AS number of the BGP neighbor.
*AS_num*: Specifies the neighbor’s AS number as an integer from 1 through 65535.

**remove-private-AS**
Removes the private AS number from outbound updates. Default: Do not remove the private AS number.

**restart-time rest_time**
Specifies the maximum time (in seconds) required for a neighbor to restart. *rest_time* must be an integer between 1 and 3600.

**route-map map_name { in | out }**
Applies a route map to the neighbor. *map_name* is the name of an existing route-map in the current context.
*in*: Indicates that the route map applies to incoming advertisements.
*out*: Indicates that the route map applies to outgoing advertisements.

**send-community { both | extended | standard }**
Sends the community attributes to a peer router (neighbor).
*both*: Sends extended and standard community attributes.
*extended*: Sends extended community attributes.
*standard*: Sends standard community attributes.

**shutdown**
Administratively shuts down this neighbor. This disables exchanging routes or configuring parameters for this neighbor.

**srp-activated-soft-clear**
Enables BGP updates when Service Redundancy Protocol SRP-enabled resources are modified.

**timers {{ connect-interval conn_time } | { keepalive-interval keep_time holdtime-interval hold_time }}**
Specifies BGP timers for this neighbor.
*connect-interval conn_time*: Specifies the connect timer in seconds. *conn_time* must be an integer from 0 through 65535. The default is 60 seconds.
*keepalive-interval keep_time*: The frequency (in seconds) at which the current BGP router sends keepalive messages to its neighbor. *keep_time* must be an integer from 0 through 65535. The default is 30 seconds.
*Holdtime-interval hold_time*: The interval (in seconds) the router waits for a keepalive message before declaring a neighbor dead. *hold_time* must be an integer from 0 through 65535. The default is 90 seconds.
**update-source ip_address**

Binds the specified IP address to the BGP socket that is used to communicate to the peer. *ip_address* is an IPv4 address in dotted-decimal notation.

In most cases you should set the update-source address to the address of the loopback interface in the current context. By doing this, the TCP connection does not go down until there is no route for the loopback address in the peering router.

**weight value**

Sets the default weight for routes from this neighbor. *value* must be an integer from 0 through 65535. Default: 0

---

**Usage**

Use this command to set parameters for communication with a specified neighbor. The chassis supports a maximum of 64 peers per context.

**Example**

The following command specifies that the neighbor at the IP address 192.168.100.25 has an AS number of 2000:

```
neighbor 192.168.100.25 remote-as 2000
```

The following command allows BGP neighbors that are a maximum of 27 hops away:

```
neighbor 192.168.100.25 ebgp-multihop max-hop 27
```

The following command sets the minimum interval between sending routing updates to 3 minutes (180 seconds):

```
neighbor 192.168.100.25 advertisement-interval 180
```

The following command sets the default weight for all routes from the specified neighbor to 100:

```
neighbor 192.168.100.25 weight 100
```
network

Specifies a network to announce via BGP.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > BGP Configuration
configure > context context_name > router bgp as_number

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-bgp)#

Syntax

[ no ] network ip_address/mask [ route-map map_name ]

no
Delete the specified network from the configuration for the BGP router.

ip_address/mask
Specifies the IP address and netmask bits for the network to announce via BGP. ip_address is a network IPv4 address in dotted-decimal notation and mask is the number of subnet bits, representing a subnet mask in CIDR shorthand. These must be entered in the dotted-decimal notation/subnet bits format (for example, 10.1.1.1/24).

[ route-map map_name ]
Filter routes through the specified route map before announcing the network. map_name is the name of the route-map to use specified as an alphanumeric string of 1 through 79 characters.

Usage
Use this command to specify a network to announce via BGP.

Example

The following command announces the network 192.168.0.0 with a netmask of 16 via BGP:

    network 192.168.0.0/16

The following command removes the network from the BGP router configuration:

    no network 192.168.0.0/16
redistribute

Redistributes routes via BGP from another protocol to BGP neighbors.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > BGP Configuration

```bash
configure > context context_name > router bgp as_number
```

Entering the above command sequence results in the following prompt:

```bash
[context_name]host_name(config-bgp)#
```

**Syntax**

```
[ no ] redistribute { connected | ospf | rip | static } [ route-map map_name ]
```

- **no**
  Remove the specified redistribution parameters from the BGP router configuration.

- **redistribute connected**
  Specifies that connected routes will be redistributed.

- **redistribute ospf**
  Specifies that Open Shortest Path First (OSPF) routes will be redistributed.

- **redistribute rip**
  Specifies that Routing Information Protocol (RIP) routes will be redistributed. (RIP is not supported at this time.)

- **redistribute static**
  Specifies that static routes will be redistributed.

  ```
  [ route-map map_name ]
  ```

  Filter routes through the specified route map before redistribution. map_name specifies the name of the route-map to use and must be specified as an alphanumeric string of 1 through 79 characters.

**Usage**

Use this command to specify what routes this BGP router should redistribute into BGP.

**Example**

The following command redistributes OSPF routes after filtering them through the route map named Map1:

```bash
redistribute ospf route-map Map1
```
The following command removes the redistribution of OSPF routes from the router’s configuration:

```
no redistribute ospf route-map map1
```
router-id

Overrides the configured router identifier and causes BGP peers to reset.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > BGP Configuration

```
configure > context context_name > router bgp as_number
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-bgp)#
```

**Syntax**

```
router-id ip_address

no router-id [ ip_address ]
```

no
Remove the specified router ID from the router’s configuration and use the default router ID.

```
router-id ip_address
```

Specifies the IP address to use as the BGP router ID as an IPv4 address in dotted-decimal notation.

**Usage**

Use this command to configure a specific router ID that overrides the default.

**Example**

The following command sets the router ID to 192.168.100.25:

```
router-id 192.168.100.25
```
**scan-time**

Configures the BGP background scanner interval. BGP monitors the next hop of the installed routes to verify next-hop reachability and to select, install, and validate the BGP best path. By default, the BGP scanner polls the Routing Information Base (RIB) for this information every 60 seconds. During the 60-second time period between scan cycles, Interior Gateway Protocol (IGP) instabilities or other network failures can cause temporarily black holes and routing loops.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > BGP Configuration

```bash
configure > context context_name > router bgp as_number
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-bgp)#
```

**Syntax**

```
[ no ] scan-time time
```

- **no**
  - Remove the user specified scan time from the router’s configuration. The scan time is reset to the default value.

- **scan-time time**
  - Specifies the amount of time (in seconds) to wait between background scans to determine next-hop validity. `time` must be an integer from 5 through 60. Default: 60

**Usage**

Use this command to set the background scanner interval for the BGP router.

**Example**

The following command sets the background scanner interval to 30 seconds:

```
scan-time 30
```
timers

Configures BGP routing timers.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > BGP Configuration

configure > context context_name > router bgp as_number

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-bgp)#

Syntax

```
timers bgp keepalive-interval interval holdtime-interval time [ min-peer-holdtime-interval interval time ]
```

no
Remove the user specified timer values from the router’s configuration. The timer values are reset to the default values.

```
timers bgp keepalive-interval interval holdtime-interval time
```

keepalive-interval interval: Specifies the interval (in seconds) to wait between sending keepalive packets as an integer from 0 through 65535. Default: 30

holdtime-interval time: Specifies the interval (in seconds) after which the neighbor is considered dead if keepalive messages are not received as an integer from 0 through 65535.

```
[ min-peer-holdtime-interval time ]
```

Specifiers the interval (in seconds) that is the minimum acceptable hold time from a neighbor as an integer from 0 through 65535. The default is 0 so that there is no restriction on the hold time received in an OPEN message from the peer.

Usage
Use this command to configure the how long to wait between sending keepalive packets and how long to wait for a keepalive before considering a a neighbor dead.

Example
The following command sets the keepalive interval to 2 minutes (120 seconds) and the holdtime interval to 3 minutes (180 seconds):

```
timers bgp keepalive-interval 120 holdtime-interval 180 min-peer-holdtime-interval 0
```
The Border Gateway Protocol (BGP) IP VRF (Virtual Routing and Forwarding) Configuration Mode is used to configure properties for BGP-4 routing.

**Important:** The VRF must have been preconfigured using the `ip vrf` command in the Context Configuration mode before you can enter this configuration mode.

Mode

Exec > Global Configuration > Context Configuration > BGP Configuration > BGP-IP VRF Configuration

```bash
configure > context context_name > router bgp as_number > ip vrf vrf_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-bgp-vrf)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
**end**

Exits the current configuration mode and returns to the Exec mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**

Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
exit
```

Usage
Use this command to return to the parent configuration mode.
route-distinguisher

Assigns a route distinguisher (RD) for the VRF that helps identify a virtual routing domain in a provider’s network and allows for overlapping IP space. The route distinguisher must be a unique value on the router for each VRF.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > BGP Configuration > BGP-IP VRF Configuration
configure > context context_name > router bgp as_number > ip vrf vrf_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-bgp-vrf)#

Syntax

route-distinguisher { as_value | ip_address } rd_value

route-distinguisher as_value rd_value

Identifies the target VRF by an autonomous system (AS) number. ASN value is a 16-bit ASN expressed as an integer from 0 through 65535.

route-distinguisher ip_address rd_value

Identifies the target VRF by its IP address. ip_address is entered using IPv4 dotted-decimal notation.

rd_value

rd_value is a unique route distinguisher identifier and must be an integer from 0 through 4294967295.

Usage

Use this command to assign a router distinguisher (RD) for the IP VRF. The combination of AS number or IP address and RD value must be unique for every VRF configured. The RD is added to the beginning of the pool addresses to change them into globally unique VPN-IPv4 prefixes.

If the RD is not configured for a VRF, user cannot enter into the BGP Address-Family mode for that VRF to configure the neighbors or other related BGP commands.

An RD assigned to a VRF cannot be changed until the existing VRF is deleted or removed and reconfigured.

Example

The following command assigns a router distinguisher 12345 to VRF with AS number 300:

    route-distinguisher 300 12345

The following command assigns a router distinguisher 12345 to VRF with IP address 10.5.3.4:

    route-distinguisher 10.5.3.4 12345
route-target

Adds an export and/or import list of extended route target communities to the VRF. BGP uses an extended-community attribute, the route target, to filter appropriate VPN routes into the correct VRFs. You configure the export list on the VRF to specify export route targets. When BGP advertises a route from this VRF’s forwarding table, it associates the list of export route targets with the route and includes this attribute in the update message that advertises the route. You also configure a route-target import list on each VRF to specify import route targets.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > BGP Configuration > BGP-IP VRF Configuration
configure > context context_name > router bgp as_number > ip vrf vrf_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-bgp-vrf)#

Syntax

route-target { both | import | export } { as_value | ip_address } rt_value

route-target both

Creates a list of import and export route targets for the VRF with the same parameters. The list contains an AS number or IP address along with a route target (RT) value.

route-target import

Creates a list of import RTs for the VRF with the same parameters. The list contains an AS number or IP address along with an RT value.

route-target export

Creates a list of export RTs for the VRF with the same parameters. The list contains an AS number or IP address along with an RT value.

as_value

Specifies a 16-bit autonomous-system (AS) number expressed as an integer from 0 through 65535.

ip_address

Specifies an IP address in IPv4 dotted-decimal notation.

rt_value

Specifies a unique RT identifier as an integer from 0 through 4294967295.
Usage
Use this command to create the list of export and/or import route target extended communities for VRF. A maximum of 5 route targets can be defined with this command up to release 9.0. A maximum of 10 route targets can be defined with this command from release 10.0 onward.

Important: This command must be executed for each route target extended community.

Example

The following command creates an export list of route target extended community 12345 for VRF with AS number 300:

```
route-target export 300 12345
```

The following command creates an export list of route target extended community 12345 for VRF with IP address 192.168.1.2:

```
route-target export 192.168.1.2 12345
```
Chapter 33
BITS Port Configuration Mode Commands

The Building Integrated Timing Supply (BITS) port configuration mode provides the commands to configure the BITS ports on the SPIO and optionally to configure the transmit timing source.

Mode

Exec > Global Configuration > BITS Port Configuration

configure > port bits slot_number/port_number

Entering the above command sequence results in the following prompt:

[local]host_name(config-port-slot_number/port_number)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
**default**

Restores the port’s default speed and communication mode.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
- Exec > Global Configuration > BITS Port Configuration
- `configure > port bits slot_number/port_number`

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-port-slot_number/port_number)#
```

**Syntax**

```
default { mode | preferred slot }
```

- `mode`
  - Default: none
  - Sets the default for the ports framing mode.

- `preferred slot`
  - Default: non-revertive
  - Sets the port for non-revertive operation for port redundancy auto-recovery; requiring an administrative user to manually issue a port switch command to return service to the original port.

**Usage**

Restores port-level parameters to their default values.

**Example**

Use the following command to remove any setting for this port’s framing mode:

```
default mode
```
description

Defines descriptive text that provides useful information about the port.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > BITS Port Configuration

```
configure > port bits slot_number/port_number
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-port-slot_number/port_number)#
```

**Syntax**

```
description  text

no description
```

**no**
Erases the port’s description from the configuration file.

**text**
_text_ must be a string of 1 to 79 alphanumeric characters with no spaces or a string within double quotes that includes printable characters. The description is case-sensitive.

**Usage**
Set the description to provide helpful information, for example the port’s primary function, services, end users. Define any information, the only limit is the number of characters.

**Example**
Use the following command to set a sample port description in the configuration file:

```
description samplePortDescriptiveText
```

Use the following command to set a more readable description:

```
description "This is a sample description"
```
**end**

Exits the current configuration mode and returns to the Exec mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**

Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product  
All

Privilege  
Security Administrator, Administrator

Syntax  
exit

Usage  
Use this command to return to the parent configuration mode.
mode

Configures the framing mode for the port.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > BITS Port Configuration

configure > port bits slot_number/port_number

Entering the above command sequence results in the following prompt:

[local]host_name(config-port-slot_number/port_number)#

Syntax

mode { e1 | t1 } framing type

- **e1 | t1**
  - **e1** selects the SDH E1 framing mode.
  - **t1** selects the SONET T1 framing mode.

- **framing type**
  - **basic**: Selects the Frame Alignment Signal (FAS) used with E1.
  - **crcmf**: Selects the Multiframe with CRC (FAS+CRC) used with E1.
  - **esf**: Selects the extended superframe format used with T1.
  - **sf**: Selects the superframe format (D4) used with T1.

Usage

Set the ports framing mode parameters.

Example

Configure the port to support E1 with crcmf framing.

```
mode e1 framing crcmf
```
preferred slot

Identifies which card in a chassis should assume revertive (redundancy auto-recovery) functionality should the slot/port being configured go down. There are only two SPIO, one in slot 24 and the other in slot 25.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > BITS Port Configuration

configure > port bits slot_number/port_number

Entering the above command sequence results in the following prompt:

[local]host_name(config-port-slot_number/port_number)#

Syntax

preferred slot  slot#

[ default | no ] preferred slot

default
Default: non-revertive operation.

no
Disables revertive, or auto-recovery, operation for the port.

slot#
Identifies the physical slot in the chassis where the SPIO is installed.

Usage

This command enables or disables revertive port redundancy. So after a port failover, when the original port is restored to service (i.e. link up) the system will return service to that port automatically. Disabled, which is the default setting, causes non-revertive operation; requiring an administrative user to manually issue a port switch to command to return service to the original port.

Example

Use this command to set the ports on the card in slot 25 as “preferred” for port redundancy:

preferred slot 25
**recover**

Configures line-timing so the SPIO recovers timing from a port on an optical (OLC/OLC2) or channelized (CLC/CLC2) card. The recovered clock is then distributed to synchronize timing on all line cards in the chassis.

**Important:** To employ line-timing recovery, the SPIO card(s) must be equipped with the optional Stratum 3 clock module.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > BITS Port Configuration
`configure > port bits slot_number/port_number`
Entering the above command sequence results in the following prompt:

```
[local]host_name(config-port-slot_number/port_number)#
```

**Syntax**

```
recover { line1 slot# | line2 slot # }
```

```
no recover { line1 | line2 }
```

**Usage**

Define which line-timing source has priority.

**Important:** If the SPIO is connected to an external Building Integrated Timing Supply (BITS) source, BITS timing always takes precedence over line-timing.

**Example**

Configure the line card in slot 19 as the preferred source for line-timing.
recover linel 19
shutdown

Terminates all processes supporting the port or blocks the shutting down of the port. Conversely, this command with the no keyword enables the port and BITS-timing as a transmit timing source.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > BITS Port Configuration

configure > port bits slot_number/port_number

Entering the above command sequence results in the following prompt:

[local]host_name(config-port-slot_number/port_number)#

Syntax

[ no ] shutdown

no

Enables the port’s administrative state. When omitted the card is shutdown (removed from service).

Usage
Shut down a port prior to re-cabling and/or other maintenance activities. This command with the no keyword is required to bring a port into service.

Example

Use the following command to enable the port for service:

no shutdown
**snmp trap link-status**

Enables/disables the generation and sending of an SNMP (notification) trap when the port experiences a change of state (up or down).

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > BITS Port Configuration

```plaintext
configure > port bits slot_number/port_number
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-port-slot_number/port_number)#
```

**Syntax**

```
[ no ] snmp trap link-status
```

- **no**
  Disables the sending of traps for link-status changes.

**Usage**

Enable the sending of link-status change traps if there is a monitoring facility that can use the information or if there are troubleshooting activities in progress.

**Example**

Use this command to enable sending of link-status SNMP traps:

```
  snmp trap link-status
```

Use this command to disable sending of link-status SNMP traps:

```
  no snmp trap link-status
```
Chapter 34
BMSC Profile Configuration Mode Commands

The BMSC Profile Configuration Mode is used to configure Broadcast Multicast Service Center profiles for Multimedia Broadcast Multicast Service (MBMS) applications. The mode is accessed by entering the `bmsc-profile` command from the Context Configuration Mode.

**Mode**

Exec > Global Configuration > Context Configuration > BMSC Profile Configuration

`configure > context context_name > bmsc-profile profile_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-bmsc-profile)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```bash
exit
```

**Usage**
Use this command to return to the parent configuration mode.
gmb diameter dictionary

This command specifies the Diameter dictionary for the Gmb interface in the BMSC profile of an MBMS user service.

**Product**

GGSN

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > BMSC Profile Configuration

```
configure > context context_name > bmsc-profile profile_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-bmsc-profile)#
```

**Syntax**

```
gmb diameter dictionary { custom1 | custom10 | custom2 | custom3 | custom4 | custom5 | custom6 | custom7 | custom8 | custom9 | standard }
```

**default gmb diameter dictionary**

```
  custom1 ... custom10

  Custom-defined Diameter dictionary. Specific to customer requirement.

  standard

  Default: Enabled
  Specifies the standard Gmb Diameter dictionary conforming to 3GPP TS 29.061 (Rel. 7).

  default

  Sets the Diameter dictionary to standard.
```

**Usage**

Use this command to select the Gmb Diameter dictionary in BM-SC profile of MBMS user service.

**Example**

The following command sets the Gmb Diameter dictionary to TS 29.061 (Rel. 7) specific:

```
gmb diameter dictionary standard
```
gmb diameter endpoint

This command specifies the Diameter endpoint name for the Gmb interface in the BMSC profile of an MBMS user service.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > BMSC Profile Configuration

```
configure > context context_name > bmsc-profile profile_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-bmsc-profile)#
```

**Syntax**

```
gmb diameter endpoint endpoint_name
```

```
no gmb diameter endpoint
```

**Usage**

Use this command to create a Gmb Diameter endpoint for a BMSC profile.

**Example**

The following command creates a Diameter endpoint named `test1` in the BMSC profile of an MBMS user service:

```
gmb diameter endpoint test1
```
gmb diameter peer-select

This command specifies the peer ids of BM-C Diameter primary and secondary host in the BMSC profile for an MBMS user service.

Product
GGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > BMSC Profile Configuration

configure > context context_name > bmsc-profile profile_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-bmsc-profile)#

Syntax

```plaintext
  gmb diameter peer-select peer peer_name [ realm realm_name ] [ secondary-peer sec_peer_name [ realm sec_realms_name ] ]
```

**no**
Removes the previously configured BM-C Diameter peer ids configured in the BMSC profile of an MBMS user service.

**peer peer_name**
Specifies the primary diameter host id for BMSC in this BMSC profile for MBMS user service. This is a unique name that is specified for the primary peer.

**realm realm_name**
Specifies the realm or domain for the Gmb Diameter peer. The realm may typically be a company or service name.

**secondary-peer sec_peer_name**
Specifies a back-up host that is used for fail-over processing. When the route-table does not find an AVAILABLE route, the secondary host performs fail-over processing.

**realm sec_realms_name**
Specifies the realm or domain for the Gmb Diameter secondary host. The realm may typically be a company or service name.
Usage
Use this command to select a BMSC Diameter peer and realm in this BMSC profile for MBMS user service.

Example
The following command selects a Gmb Diameter peer named `test1` and a realm of `companyx`:

```
gmb diameter peer-select peer test1 realm companyx
```
**gmb user-data**

This command configures the parameters in this BMSC profile for user data for MBMS user service.

**Product**

GGSN

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > BMSC Profile Configuration

```shell
configure > context context_name > bmsc-profile profile_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-bmsc-profile)#
```

**Syntax**

```shell
gmb user-data { mode-preference { multicast | unicast } | unicast-self-address self_ip_address }

default gmb user-data mode-preference

no gmb user-data unicast-self-address
```

- **no**
  
  Removes the configured self address of GGSN for unicast in the BMSC profile for user data of MBMS user service.

- **default**
  
  Sets the user data mode to unicast in the BMSC profile for user data of MBMS user service.

- **mode-preference { multicast | unicast }**
  
  Default: unicast
  
  Specifies the preferred mode of GGSN for receiving MBMS user service data.
  
  **multicast**: specifies the preferred mode as multicast for MBMS user service.

  **Important**: Note that this **multicast** keyword is not supported in this release.

  **unicast**: specifies the preferred mode as unicast for MBMS user service.

- **unicast-self-address self_ip_address**
  
  Specifies the GGSN’s IP address for BMSC to use as the outer destination address for the IP-in-IP tunnel to send multicast data, if the configured preferred data mode is unicast.
  
  **self_ip_address** must be the IPv4 address in dotted-decimal notation.
  
  This command must be configured if GGSN's user-data mode-preference is Unicast.
Usage

Use this command to configure user data mode and other parameters in the BMSC profile for user data of MBMS user service.

GGSN can receive multicast data from BMSC in one of two modes - Multicast or Unicast. In Unicast mode, BM-SC tunnels the multicast data to the GGSN in an IP-in-IP tunnel instead of direct multicast. This command with the `mode-preference` keyword configures the GGSN's preferred mode for receiving multicast data.

**Important:** Both GGSN and BMSC must support the Unicast mode of multicast data transfer. If any GGSN or BMSC does not support Multicast mode, BMSC will transfer multicast data using Unicast mode only.

Use the `unicast-self-address` keyword to configure the GGSN's IP address which the BMSC should use as the outer destination address for the IP-in-IP tunnel to send multicast data, if the selected user data mode to receive multicast data is Unicast.

Example

The following command sets the MBMS data transfer mode to unicast:

```
default gmb user-data mode-preference
```
Chapter 35
Bulk Statistics Configuration Mode Commands

The Bulk Statistics Configuration Mode is used to manage the options for the collection, formatting and delivery of system statistics to remote nodes.

Refer to the Common Syntax Options section in this chapter for information about formatting the output of bulk statistics.

**Important:** Unless otherwise indicated, all statistics are counters. For statistics with the Int32 data type, the roll-over to zero limit is 4,294,967,295. For statistics with the Int64 data type, the roll-over to zero limit is 18,446,744,073,709,551,615.

Mode

Exec > Global Configuration > Bulk Statistics Configuration

configure > bulkstats mode

Entering the above command sequence results in the following prompt:

[local]host_name(config-bulkstats)#

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
Overview

Schema Format String Syntax

The following defines common syntax block options. These options appear in similar commands and are detailed here for easy reference.

The schema format string is used to define the structure of generated bulk statistics data. The string may contain static text, dynamic content, and bulk statistic variables, or any combination.

Static text includes any ASCII characters that are of a fixed value. Static text may also include control characters by using Escape character sequences. Supported Escape character shortcuts are “\n” for new line and “\t” for tab.

Enclosing an alphanumeric string within double quotation marks (“”) allows you to include spaces in the string.

Variables within the format string must be enclosed within “%” and “%”, for example, “%var%”. The actual variables supported are command-dependent and are described in the Statistics and Counters Reference.

Schema Format String Length

The maximum length of schema formats specified via the CLI is restricted by a limit on the CLI command. The command, which has the following syntax, cannot be more than 1021 characters long.

```<schema> schema <schema_name> format <schema_format>```

Where:

- `<schema_name>` can be a maximum of 31 characters.
- `<schema_format>` can be a maximum of “1021 minus “number of characters in rest of the command, including spaces”” characters.

Common Statistics

For a list of the statistics that are common to all schema, refer to the Statistics and Counters Overview chapter of the Statistics and Counters Reference.
**aal2 schema**

Configures the ATM adaptation layer 2 (AAL2) bulk statistics schema within an ATM virtual connection by the HNB-GW.

**Product**
HNB-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Bulk Statistics Configuration
configure > bulkstats mode

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-bulkstats)#
```

**Syntax**

```
aal2 schema schema_name format schema_format
no aal2 schema schema_name
```

*no*

Removes the specified schema.

```
schema_name
```

Specifies the schema’s name.

*schema_name* must be an alphanumeric string of 1 through 31 characters.

```
format schema_format
```

Specifies the schema’s format.

*schema_format* must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of the command, including spaces’”’ characters. For more information, see the Schema Format String Length section.

For information on the schema format’s syntax, see the Schema Format String Syntax section.

**Important:** For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

**Usage**

Use this command to define schemas for ATM adaptation layer 2 (AAL2) bulk statistics collection. Multiple AAL2 schemas can be created to further categorize HNB-GW-level bulk statistics. All of the schemas are processed at each collection interval. To create multiple AAL2 schemas, re-issue the *aal2 schema schema_name* command using a different schema name.

**Example**
The following command creates a schema named `aal2stats1` that records the number of AAL2 uplink packets transmitted and AAL2 downlink packets received by Access Link Control Application Part (ALCAP) service on HNB-GW:

```plaintext
    aal2 schema aal2stats1 format "%uplink-pkts-tx%" "%downlink-pkts-rx%"
```
alcap schema

Configures the Access Link Control Application Part (ALCAP) bulk statistics schema for an ALCAP service on an HNB-GW node.

Product
HNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Bulk Statistics Configuration
configure > bulkstats mode

Entering the above command sequence results in the following prompt:

[local]host_name(config-bulkstats)#

Syntax

alcap schema schema_name format schema_format

no alcap schema schema_name

no
Removes the specified schema.

schema_name
Specifies the schema’s name.
schema_name must be an alphanumeric string of 1 through 31 characters.

format schema_format
Specifies the schema’s format.
schema_format must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of the command, including spaces”” characters. For more information, see the Schema Format String Length section.
For information on the schema format’s syntax, see the Schema Format String Syntax section.

Important: For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

Usage

Use this command to define schemas for Access Link Control Application Part (ALCAP) service bulk statistics collection on HNB-GW node. Multiple ALCAP schemas can be created to further categorize at AAL2 channel-level bulk statistics. All of the schemas are processed at each collection interval. To create multiple ALCAP schemas, re-issue the alcap schema schema_name command using a different schema name.

Example
The following command creates a schema named `alcap1stats1` that records the number of AAL2 channels in connecting and connected state on ALCAP service:

```
alcap schema alcap1stats1 format "%num-aal2-channels-in-connecting%"
    "%num-aal2-channels-in-connected-state%"
```
apn schema

Configures the Access Point Name (APN) bulk statistics schema.

Product
GGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Bulk Statistics Configuration
configure > bulkstats mode

Entering the above command sequence results in the following prompt:

[local]host_name(config-bulkstats)#

Syntax

apn schema schema_name format schema_format

no apn schema schema_name

no

Removes the specified schema.

schema_name

Specifies the schema’s name.
schema_name must be an alphanumeric string of 1 through 31 characters.

format schema_format

Specifies the schema’s format.
schema_format must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of
the command, including spaces”“ characters. For more information, see the Schema Format String Length
section.
For information on the schema format’s syntax, see the Schema Format String Syntax section.

Important: For a complete list of the statistics that are supported for this schema, refer to the Statistics and
Counters Reference.

Usage

Use this command to define schemas for APN bulk statistics collection. Multiple APN schemas can be
created to further categorize APN-level bulk statistics. All of the schemas are processed at each collection
interval. To create multiple APN schemas, re-issue the apn schema schema_name command using a
different schema name.

Example

The following command creates a schema named apn1stats1 that records the number of sessions currently
facilitated by the APN:
apn schema apnlstats1 format "sess-curr%"
asngw schema

Configures Access Service Gateway (ASN-GW) bulk statistics schema.

**Product**
ASN-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Bulk Statistics Configuration
configure > bulkstats mode

Entering the above command sequence results in the following prompt:

[local]host_name(config-bulkstats)#

**Syntax**

asngw schema  schema_name  format  schema_format

no asngw schema  schema_name

**no**

Removes the specified schema.

**schema_name**

Specifies the schema’s name.

*schema_name* must be an alphanumeric string of 1 through 31 characters.

**format  schema_format**

Specifies the schema’s format.

*schema_format* must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of the command, including spaces”” characters. For more information, see the Schema Format String Length section.

For information on the schema format’s syntax, see the Schema Format String Syntax section.

**Important:** For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

**Usage**

Use this command to define schemas for ASN-GW bulk statistics collection. Multiple ASN-GW service schemas can be created to further categorize ASN-GW service bulk statistics. All of the schemas are processed at each collection interval. To create multiple ASN-GW service schemas, re-issue the *asngw schema  schema_name* command using a different schema name.

**Example**

To create an ASN-GW schema named *asngw_statistics* that specifies a schema format of:

- VPN context name: *vpnname*
• VPN Context Identifier: vpnid
• ASN-GW Service name: servname
• ASN-GW Service identifier: servid
• Peer IP address: peeripaddr

Use the following command:

```bash
asngw schema asngw_statistics format "VPN name: %vpnname%
VPN ID: %vpnid%
ASN-GW Service Name: %servname%
ASN-GW Service Identifier: %servid%
Peer IP Address: %peeripaddr"
```
**bcmcs schema**

Configures Broadcast and Multicast Service (BCMCS) bulk statistics schema.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Bulk Statistics Configuration

`configure > bulkstats mode`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-bulkstats)#
```

**Syntax**

```
bcmcs schema  
  schema_name format  schema_format

no bcmcs schema  
  schema_name
```

- **no**
  - Removes the specified schema.

- **schema_name**
  - Specifies the schema’s name.
  - `schema_name` must be an alphanumeric string of 1 through 31 characters.

- **format  
  schema_format**
  - Specifies the schema’s format.
  - `schema_format` must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of the command, including spaces”” characters. For more information, see the Schema Format String Length section.
  - For information on the schema format’s syntax, see the Schema Format String Syntax section.

**Important:** For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

**Usage**

Use this command to define schemas for BCMCS bulk statistics collection. Multiple BCMCS schemas can be created to further categorize BCMCS-level bulk statistics. All of the schemas are processed at each collection interval. To create multiple BCMCS schemas, re-issue the `bcmcs schema schema_name` command using a different schema name.

**Example**

The following command creates a schema named `bcmcs1stats1` that records the number of sessions currently facilitated by BCMCS:
bcmcs schema bcmcs1stats1 format "%sess-curr%"
card schema

Configures card bulk statistics schema. These are statistics for circuit cards installed in the ASR 5x00 chassis.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Bulk Statistics Configuration

```
class > bulkstats mode
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-bulkstats)#
```

**Syntax**

```
card schema schema_name format schema_format

no card schema schema_name
```

---

**no**

Removes the specified schema.

---

**schema_name**

Specifies the schema’s name.

- **schema_name** must be an alphanumeric string of 1 through 31 characters.

---

**format schema_format**

Specifies the schema’s format.

- **schema_format** must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of the command, including spaces”” characters. For more information, see the Schema Format String Length section.

For information on the schema format’s syntax, see the Schema Format String Syntax section.

---

**Important:** For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

---

**Usage**

Use this command to define schemas for card bulk statistics collection. Multiple card schemas can be created to categorize card-level bulk statistics. All of the schemas are processed at each collection interval. To create multiple card schemas, re-issue the `card schema schema_name` command using a different schema name.

---

**Important:** Not supported on all platforms
Example

The following command creates a schema named `card1stats1` that records the number of processes for all installed cards:

```
card schema card1stats1 format "%slot%-%numproc%"
```

To create a card-level schema named `cardresourcestats` that specifies a schema format of:
- Chassis slot number: `slot`
- Available Memory: `memtotal`
- Memory Used (%): `memused`
- Available CPU (%): `cpuidle`

Use the following command:

```
card schema cardresourcestats format "Chassis slot number: %slot%
Available Memory: %memtotal% Memory Used (%): %memused% Available CPU (%): %cpuidle%"
```
context schema

Configures context bulk statistics schema.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Bulk Statistics Configuration

configure > bulkstats mode

Entering the above command sequence results in the following prompt:

[local]host_name(config-bulkstats)#

Syntax

context schema  schema_name  format  schema_format

no context schema  schema_name

no

Removes the specified schema.

schema_name

Specifies the schema’s name.

schema_name must be an alphanumeric string of 1 through 31 characters.

format  schema_format

Specifies the schema’s format.

schema_format must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of the command, including spaces”“” characters. For more information, see the Schema Format String Length section.

For information on the schema format’s syntax, see the Schema Format String Syntax section.

Important: For the complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

Usage

Use this command to define schemas for Context bulk statistics collection. Multiple context schemas can be created to categorize context statistics. All of the schemas are processed at each collection interval. To create multiple context schemas, re-issue the context schema  schema_name command using a different schema name.

Example

To create a Firewall context schema named sfw_context_stats1 that specifies a schema format of:

- Total packets received by firewall: sfw-total-rxpackets
- Total packets sent by firewall: $sfw\text{-}total\text{-}txpackets$
- Total ICMP packets discarded by firewall: $fw\text{-}icmp\text{-}discardpackets$

Use the following command:

```plaintext
context schema sfw\_context\_stats1 format "Packets received Rx: %sfw\text{-}total\text{-}rxpackets\nPackets Sent Tx:: %sfw\text{-}total\text{-}txpackets\nICMP Packets discarded: %fw\text{-}icmp\text{-}discardpackets"
```
cscf schema

Configures Call Session Control Function (CSCF) bulk statistics schema.

Product
SCM

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Bulk Statistics Configuration
configure > bulkstats mode

Entering the above command sequence results in the following prompt:

[local]host_name(config-bulkstats)#

Syntax

cscf schema  schema_name  format  schema_format

no cscf schema  schema_name

no

Removes the specified schema.

schema_name

Specifies the schema’s name.
schema_name must be an alphanumeric string of 1 through 31 characters.

format  schema_format

Specifies the schema’s format.
schema_format must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of the command, including spaces’”” characters. For more information, see the Schema Format String Length section.

For information on the schema format’s syntax, see the Schema Format String Syntax section.

Important: For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

Usage

Use this command to define schemas for CSCF bulk statistics collection. Multiple CSCF-service schemas can be created to categorize CSCF-service bulk statistics. All of the schemas are processed at each collection interval. To create multiple CSCF-service schemas, re-issue the cscf schema schema_name command using a different schema name.

Example

To create a CSCF schema named cscf_statistics that specifies a schema format of:

•Call attempts received: callattrx
• Call attempts transmitted: `callatttx`
• Call successes received: `callsuccrx`
• Call successes transmitted: `callsucctx`
• Call failures received: `callfailrx`
• Call failures transmitted: `callfailtx`

Use the following command:

```
cscf schema cscf_statistics format "Call Attempts Rx: %callattrx%\nCall Attempts Tx: %callatttx%\nCall Successes Rx: %callsuccrx%\nCall Successes Tx: %callsucctx%\nCall Failures Rx: %callfailrx%\nCall Failures Tx: %callfailtx%"
```
cs-network-ranap schema


Product
HNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Bulk Statistics Configuration
configure > bulkstats mode

Entering the above command sequence results in the following prompt:

[local]host_name(config-bulkstats)#

Syntax

```
cs-network-ranap schema schema_name format schema_format

no cs-network-ranap schema schema_name
```

no
Removes the specified schema.

```
schema_name
```

Specifies the schema’s name.

`schema_name` must be an alphanumeric string of 1 through 31 characters.

```
format schema_format
```

Specifies the schema’s format.

`schema_format` must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of the command, including spaces”” characters. For more information, see the Schema Format String Length section.

For information on the schema format’s syntax, see the Schema Format String Syntax section.

**Important:** For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

**Usage**

Use this command to define schemas for RANAP procedure related bulk statistics collection in a CS network associated with HNB-GW in a Femto UMTS network. Multiple CS Networks RANAP schemas can be created to further categorize at CS network or HNB-GW-level bulk statistics. All of the schemas are processed at each collection interval. To create multiple CS Networks RANAP schemas, re-issue the `cs-network-ranap schema schema_name` command using a different schema name.

**Example**

Use this command to define schemas for RANAP procedure related bulk statistics collection in a CS network associated with HNB-GW in a Femto UMTS network. Multiple CS Networks RANAP schemas can be created to further categorize at CS network or HNB-GW-level bulk statistics. All of the schemas are processed at each collection interval. To create multiple CS Networks RANAP schemas, re-issue the `cs-network-ranap schema schema_name` command using a different schema name.
The following command creates a schema named `cs_ranap1stats1` that records the total number of Iu Release Request messages transmitted and total number of Iu Release Command message received by the HNB-GW node:

```
   cs-network-ranap schema cs_ranap1stats1 format "%iu-rel-req-tx%" "%iu-rel-cmd-rx%"
```
**cs-network-rtp schema**

Configures the Real-Time Transport Protocol (RTP) bulk statistics schema in a Circuit Switched (CS) network associated with an HNB-GW node.

**Product**
HNB-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Bulk Statistics Configuration

```
configure > bulkstats mode
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-bulkstats)#
```

**Syntax**

```
cs-network-rtp schema schema_name format schema_format

no cs-network-rtp schema schema_name
```

- `no`
  
  Removes the specified schema.

- `schema_name`
  
  Specifies the schema’s name.
  
  `schema_name` must be an alphanumeric string of 1 through 31 characters.

- `format schema_format`
  
  Specifies the schema’s format.
  
  `schema_format` must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of the command, including spaces”” characters. For more information, see the Schema Format String Length section.
  
  For information on the schema format’s syntax, see the Schema Format String Syntax section.

> **Important:** For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

**Usage**

Use this command to define schemas for RTP procedure related bulk statistics collection in a CS network associated with HNB-GW in a Femto UMTS network. Multiple CS Networks RTP schemas can be created to further categorize at CS network or HNB-GW-level bulk statistics. All of the schemas are processed at each collection interval. To create multiple CS Networks RTP schemas, re-issue the `cs-network-rtp schema schema_name` command using a different schema name.

**Example**
The following command creates a schema named `cs_rtp1statsl` that records the total number of RTP Downlink Packets received and RTP Uplink Packets transmitted by HNB-GW node in an associated CS network:

```
  cs-network-rtp schema cs_rtp1statsl format "%rtp-uplink-pkts-tx%" "%rtp-downlink-pkts-rx%"
```
**cs-network-sccp schema**

Configures the Signalling Connection Control Part (SCCP) bulk statistics schema in a Circuit Switched (CS) network associated with an HNB-GW node.

**Product**
HNB-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Bulk Statistics Configuration
`configure > bulkstats mode`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-bulkstats)#
```

**Syntax**

```
cs-network-sccp schema schema_name format schema_format
```

```
no cs-network-sccp schema schema_name
```

**no**

Removes the specified schema.

**schema_name**

Specifies the schema’s name.
`schema_name` must be an alphanumeric string of 1 through 31 characters.

**format schema_format**

Specifies the schema’s format.
`schema_format` must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of the command, including spaces”” characters. For more information, see the Schema Format String Length section.
For information on the schema format’s syntax, see the Schema Format String Syntax section.

**Important:** For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

**Usage**

Use this command to define schemas for SCCP connection related bulk statistics collection in a CS network associated with HNB-GW in a Femto UMTS network. Multiple CS Networks SCCP schemas can be created to further categorize at CS network or HNB-GW-level bulk statistics. All of the schemas are processed at each collection interval. To create multiple CS Networks SCCP schemas, re-issue the `cs-network-sccp schema schema_name` command using a different schema name.

**Example**
The following command creates a schema named `cs_sccplstats1` that records the total number of SCCP connection requests received by HNB-GW and responses sent to CN node in an associated CS network:

```
cs-network-sccp schema cs_sccplstats1 format "%sccp-conn-req-rx%" "%sccp-conn-req-tx%"
```
dcca schema

Configures Diameter Credit Control Application (DCCA) bulk statistics schema. This command is available only in StarOS 9.0 and later releases.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Bulk Statistics Configuration
configure > bulkstats mode

Entering the above command sequence results in the following prompt:

[local]host_name(config-bulkstats)#

Syntax

```
dcca schema schema_name format schema_format

no dcca schema schema_name
```

- **no**
  Removes the specified schema.

- **schema_name**
  Specifies the schema’s name. 
  `schema_name` must be an alphanumeric string of 1 through 31 characters.

- **format schema_format**
  Specifies the schema’s format. 
  `schema_format` must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of the command, including spaces”” characters. For more information, see the Schema Format String Length section. For information on the schema format’s syntax, see the Schema Format String Syntax section.

**Important:** For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

Usage

Use this command to define schemas for DCCA bulk statistics collection.
dcca-group schema

This command configures Diameter Credit Control Application (DCCA) group bulk statistics schema. Please note that the DCCA-group related bulk statistics are copied from the "system" schema to this schema "dcca-group".

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Bulk Statistics Configuration
configure > bulkstats mode

Entering the above command sequence results in the following prompt:

[local]host_name(config-bulkstats)#

Syntax

dcca-group schema schema_name format schema_format

no dcca-group schema schema_name

no
Removes the specified schema.

schema_name
Specifies the schema’s name.
schema_name must be an alphanumeric string of 1 through 31 characters.

format schema_format
Specifies the schema’s format.
schema_format must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of the command, including spaces”” characters. For more information, see the Schema Format String Length section.
For information on the schema format’s syntax, see the Schema Format String Syntax section.

Important: For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

Usage
Use this command to define schemas for DCCA group bulk statistics collection.
default

Restores the system default for the option specified.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Bulk Statistics Configuration
configure > bulkstats mode

Entering the above command sequence results in the following prompt:

[local]host_name(config-bulkstats)#

Syntax

default { limit | receiver mode | remotefile format | sample-interval | transfer-interval }

limit
Restores the memory utilization limit system default: 1000 kilobytes.

receiver mode
Restores the behavior for sending files to the receivers to the default value.
Default: secondary-on-failure

remotefile format
Restores the format of remote bulkstats file names to the default value.
Default: “%date%%time%%”

sample-interval
Restores the system default for the local polling interval for statistic sampling.
Default: 15 minutes

transfer-interval
Restores the system default for the time between transfer of data files to receivers.
Default: 480 minutes

Usage
Restore the default values when troubleshooting the system. Setting values to the system defaults places them in well known states as starting points for monitoring for problems.

Example

default limit
default transfer-interval
diameter-acct schema

Configures Diameter Accounting bulk statistics schema. This command is available only in StarOS 11.0 and later releases.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Bulk Statistics Configuration

```
configure > bulkstats mode
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-bulkstats)#
```

**Syntax**

```
diameter-acct schema schema_name format schema_format

no diameter-acct schema schema_name
```

-no

Removes the specified schema.

```
schema_name
```

Specifies the schema’s name.

`schema_name` must be an alphanumeric string of 1 through 31 characters.

```
format schema_format
```

Specifies the schema’s format.

`schema_format` must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of the command, including spaces”” characters. For more information, see the Schema Format String Length section.

For information on the schema format’s syntax, see the Schema Format String Syntax section.

**Important:** For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

**Usage**

Use this command to define schemas for Diameter Accounting bulk statistics collection.
diameter-auth schema

Configures Diameter Authentication bulk statistics schema. This command is available only in StarOS 11.0 and later releases.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Bulk Statistics Configuration
configure > bulkstats mode

Entering the above command sequence results in the following prompt:

[local]host_name(config-bulkstats)#

Syntax

diameter-auth schema schema_name format schema_format

no diameter-auth schema schema_name

no
Removes the specified schema.

schema_name
Specifies the schema’s name.
schema_name must be an alphanumeric string of 1 through 31 characters.

format schema_format
Specifies the schema’s format.
schema_format must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of the command, including spaces”” characters. For more information, see the Schema Format String Length section.
For information on the schema format’s syntax, see the Schema Format String Syntax section.

Important: For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

Usage
Use this command to define schemas for Diameter Authentication bulk statistics collection.
**dlci-util schema**

Configures the collection of statistics for the DLCI-Util (DLCI utilization) schema.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Bulk Statistics Configuration
configure > bulkstats mode

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-bulkstats)#
```

**Syntax**

```
dlci-util schema schema_name format schema_format
no dlci-util schema schema_name

no
Removes the specified schema.

schema_name
Specifies the schema’s name.
schema_name must be an alphanumeric string of 1 through 31 characters.

format schema_format
Specifies the format of the collected DLCI utilization statistics by identifying the statistics variables and ordering the variables for presentation within the bulk statistics messages.
schema_format must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of the command, including spaces’” characters. For more information, see the Schema Format String Length section.
For information on the schema format’s syntax, see the Schema Format String Syntax section.
```

**Important:** For a complete list of the statistics that are supported for the DLCI-Util schema, refer to the Statistics and Counters Reference.

**Usage**

Use this command to define schemas for DLCI-Util bulk statistics collection in the generated stats report files. Usually a schema consists of multiple variables to collect all the statistics for a particular situation. Using double quote marks and text within this command, the reported statistics can be easily identified.
Multiple schemas can be created to categorize DLCI-Util bulk statistics. All of the schemas are processed at each collection interval. To create multiple DLCI-Util schemas, re-issue the `dlci-util schema schema_name` command using a different schema name each time.

**Example**

Include the bulk statistic variable names to create a schema named `dlciutilstats_sgsn1` that specifies collection of statistics (a schema format) for:

- card
- port
- path
- DS1/E1
- DLCI
- DLCI utilization snapshot for received packets
- DLCI utilization for received packets in the last 5 minutes
- DLCI utilization for received packets in the last 15 minutes

Use the following command:

```plaintext
  gprs schema gprsstats_sgsn1 format "Card: %card%
  nPort: %port%
  nDLCI in path: %dlci_util_path%
  nDS1/E1: %dlci_util_ds1e1%
  nDLCI ID:
  %dlci_util_dlci_no%
  nCurrent Rx: %dlci_util_dlci_curr_rx%
  nRx in 5 minutes: %dlci_util_dlci_5min_rx%
  nRx in 15 minutes: %dlci_util_dlci_15min_rx%"
```
dpca schema

Configures Diameter Policy Control Application (DPCA) bulk statistics schema. This command is available only in StarOS 9.0 and later releases.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Bulk Statistics Configuration

`configure > bulkstats mode`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-bulkstats)#
```

Syntax

```
dpca schema schema_name format schema_format

no dpca schema schema_name
```

---

**no**

Removes the specified schema.

---

**schema_name**

Specifies the schema’s name.

`schema_name` must be an alphanumeric string of 1 through 31 characters.

---

**format schema_format**

Specifies the schema’s format.

`schema_format` must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of the command, including spaces”” characters. For more information, see the Schema Format String Length section.

For information on the schema format’s syntax, see the Schema Format String Syntax section.

---

**Important:** For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

---

**Usage**

Use this command to define schemas for DPCA bulk statistics collection.
ecs schema

Configures Enhanced Charging Service (ECS) bulk statistics schema.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Bulk Statistics Configuration

configure > bulkstats mode

Entering the above command sequence results in the following prompt:

[local]host_name(config-bulkstats)#

Syntax

escs schema schema_name format schema_format

no ecs schema schema_name

no
Removes the specified schema.

schema_name
Specifies the schema’s name.

schema_name must be an alphanumeric string of 1 through 31 characters.

format schema_format

Specifies the schema’s format.

schema_format must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of the command, including spaces”“ characters. For more information, see the Schema Format String Length section.

For information on the schema format’s syntax, see the Schema Format String Syntax section.

Important: For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

Usage

Use this command to define schemas for ECS bulk statistics collection. Multiple ECS schemas can be created to categorize ECS bulk statistics. All of the schemas are processed at each collection interval. To create multiple ECS schemas, re-issue the ecs schema schema_name command using a different schema name.
egtpc schema

Configures the enhanced GTP-C statistics schema for naming conventions of data files.

Product
MME
P-GW
S-GW
SAEGW
SGSN

Privilege
Administrator

Mode
Exec > Global Configuration > Bulk Statistics Configuration
configure > bulkstats mode

Entering the above command sequence results in the following prompt:

[local]host_name(config-bulkstats)#

Syntax

egtpc schema schema_name format schema_format

no egtpc schema schema_name

no
Removes the specified schema.

schema_name
Specifies the schema’s name.
schema_name must be an alphanumeric string of 1 through 31 characters.

format schema_format
Specifies the schema’s format.
schema_format must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of the command, including spaces”” characters. For more information, see the Schema Format String Length section.
For information on the schema format’s syntax, see the Schema Format String Syntax section.

Important: For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.
egtpc schema

Usage

Use this command to define schemas for enhanced GTP-C bulk statistics collection. Multiple eGTP-C service schemas can be created to categorize eGTP-C service bulk statistics. All of the schemas are processed at each collection interval. To create multiple eGTP-C service schemas, re-issue the `egtpc schema schema_name` command using a different schema name.

Example

For an eGTP-C-level schema named `egtpcservicestats` that specifies a schema format of:

- Tunnel - Create Session Request Sent: `tun-sent-cresess`
- Tunnel - Create Session Request Received: `tun-recv-cresess`

Use the following command:

```
egtpc schema egtpcservicestats format "Number of GTP Tunnel Requests Sent: %tun-sent-cresess\nNumber of GTP Tunnel Requests Received: %tun-recv-cresess\n"
```
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Use this command to return to the parent configuration mode.
**fa schema**

Configures Foreign Agent (FA) bulk statistics schema.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Bulk Statistics Configuration

configure > bulkstats mode

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-bulkstats)#
```

**Syntax**

```
fa schema schema_name format schema_format

no fa schema schema_name
```

<table>
<thead>
<tr>
<th><strong>no</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Removes the specified schema.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>schema_name</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the schema’s name.</td>
</tr>
<tr>
<td><code>schema_name</code> must be an alphanumeric string of 1 through 31 characters.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>format schema_format</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the schema’s format.</td>
</tr>
<tr>
<td><code>schema_format</code> must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of the command, including spaces”” characters. For more information, see the <strong>Schema Format String Length</strong> section.</td>
</tr>
<tr>
<td>For information on the schema format’s syntax, see the <strong>Schema Format String Syntax</strong> section.</td>
</tr>
</tbody>
</table>

**Important:** For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

**Usage**

Use this command to define schemas for FA bulk statistics collection. Multiple FA service schemas can be created to categorize FA service bulk statistics. All of the schemas are processed at each collection interval. To create multiple FA service schemas, re-issue the `fa schema schema_name` command using a different schema name.

**Example**
To create a FA-level schema named faservicestats that separates the date, time, and vpnname by tabs, enter the following command:

```
fa schema faservicestats format %date%\t%time%\t%vpnname%
```

The schema format appears as follows:

```
date time vpnname
```
file

Enters the Bulk Statistics File Configuration Mode which supports the configuration of “files” used for grouping bulk statistic configuration information.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Bulk Statistics Configuration
configure > bulkstats mode

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-bulkstats)#
```

**Syntax**

```
[ no ] file number
```

- **no**
  Removes a previously configured bulk statistic file.

- **number**
  Specifies a number for the bulkstatistics file as an integer from 1 through 4. This number is how the file is recognized by the system.

**Usage**

Bulk statistics “files” are used to group bulk statistic schema, delivery options, and receiver configuration. Because multiple “files” can be configured, this functionality provides greater flexibility in that it allows you to configure different schemas to go to different receivers. A Maximum of four files can be assigned for bulk statistics collection.

Executing this command allows you to enter the Bulk Statistics File Configuration Mode. This mode supports all of the commands from the Bulk Statistics Configuration mode except `limit`, `local-directory`, `sample-interval`, and `transfer-interval` (these commands are configured globally for all “files”.)

---

**Important:** Use of bulk statistics “files” is optional. If you do not wish to configure bulk statistic “files”, you can perform a standard configuration using the commands in the Bulk Statistic Configuration Mode. Note, however, that the system logically assigns “file 1” to the standard configuration. Therefore, if you wish to configure bulk statistics “files” at a later time, “file 1” will already be used.

---

**Caution:** If the Web Element Manager application is used to collect and process (XML parsing, graphing, etc.) bulk statistics data, “file 1” is used by the Web Element Manager’s default bulk statistics collection information and schemas. To avoid errors in processing by the Web Element Manager, do not configure “file 1” via the CLI. However, it is possible to configure files 1 through 4 using the system’s CLI, regardless of whether or not the Web Element Manager is actively collecting data.
Manager is configured as a receiver. In this case, the bulk statistics data is written to the server but not processed by the Web Element Manager application.

Example

The following command creates a bulk statistics file numbered 2 and enters the Bulk Statistics File Configuration Mode:

```
file 2
```
fng schema

Configures Femto Network Gateway (FNG) bulk statistics schema.

**Product**
FNG

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Bulk Statistics Configuration

```
configure > bulkstats mode
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-bulkstats)#
```

**Syntax**

```
fng schema  schema_name format  schema_format

no fng schema  schema_name
```

- **no**
  Removes the specified schema.

- **schema_name**
  Specifies the schema’s name.
  `schema_name` must be an alphanumeric string of 1 through 31 characters.

- **format  schema_format**
  Specifies the schema’s format.
  `schema_format` must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of the command, including spaces”” characters. For more information, see the Schema Format String Length section.
  For information on the schema format’s syntax, see the Schema Format String Syntax section.

**Important**: For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.
footer

Configures the footer string placed at the end of the generated bulk statistics data files.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Bulk Statistics Configuration
configure > bulkstats mode

Entering the above command sequence results in the following prompt:

[local]host_name(config-bulkstats)#

Syntax

footer format schema_format

no footer format

no

Clears the footer format string which results in the default file footer being used in generated data files.

format schema_format

Specifies the footer format string for use in generated data files.

schema_format must be an alphanumeric string from 1 through 2047 characters. The format string syntax is described in the Schema Format String Syntax section. Default: “” (an empty footer)

The following variables are supported:

Table 17. footer Command Format String Variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
<th>Data Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>date</td>
<td>The date that the collection file was created in YYYYMMDDD format where YYYY represents the year, MM represents the month and DD represents the day.</td>
<td>String</td>
</tr>
<tr>
<td>host</td>
<td>The system hostname that created the file</td>
<td>String</td>
</tr>
<tr>
<td>ipaddr</td>
<td>The default management (local context) IP address in ###.###.###.### format. An empty string is inserted if no address is available.</td>
<td>String</td>
</tr>
<tr>
<td>sysuptime</td>
<td>The uptime (in seconds) of the system that created the file.</td>
<td>32-bit signed</td>
</tr>
<tr>
<td>time</td>
<td>The time that the collection file was created in HHMMSS format where HH represents the hours, MM represents the minutes, and SS represents the seconds.</td>
<td>String</td>
</tr>
</tbody>
</table>
Usage

Define a unique footer in data files which allows for easy identification of which system generated the data file or any other useful information. The use of the variables is suggested so as to allow for a uniform footer across all systems. The hostname variable should be used to identify the source of the data in the footer and all remaining items can be formatted consistently across all chassis.

Example

The following commands define different footer formats:

```
footer format northStreet

footer format “Created on: %date%-%time% by %host%”

no footer format
```


**gather-on-standby**

Controls whether or not statistics are gathered when a system is in the standby state.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Bulk Statistics Configuration

configure > bulkstats mode

Entering the above command sequence results in the following prompt:

[local]host_name(config-bulkstats)#

**Syntax**

```
[ no | default ] gather-on-standby
```

- **no**
  
  Does not gather bulk statistics when the system is in the standby state.

- **default**
  
  Resets this command to its default action of gathering bulk statistics when the system is in the standby state.

**Usage**

Use this command to configure a system to either gather or not gather statistics when the system is in the standby state. This is useful for systems configured for Interchassis Session Recovery (ICSR). See the *System Administration Guide* for more details on this feature.

If a chassis transitions to standby state and it has accumulated but not yet transferred bulk statistics data, the previously accumulated data is transferred at the first opportunity. However, no additional statistics gathering takes place.

**Example**

The following command disables gathering statistics when the system is in the standby state:

```
no gather-on-standby
```

The following command enables the gathering of statistics when the system is in the standby state:

```
gather-on-standby
```
**gprs schema**

Configures the collection of statistics for the GPRS schema.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Bulk Statistics Configuration

```
configure > bulkstats mode
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-bulkstats)#
```

**Syntax**

```
gprs schema schema_name format schema_format
```

```
no gprs schema schema_name
```

no

Removes the specified schema.

```
schema_name
```

Specifies the schema’s name.

*schema_name* must be an alphanumeric string of 1 to 31 characters.

```
format schema_format
```

Specifies the format of the collected GPRS statistics by identifying the statistics variables and ordering the variables for presentation within the bulk statistics messages.

*schema_format* must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of the command, including spaces”” characters. For more information, see the [Schema Format String Length](#) section.

For information on the schema format’s syntax, see the [Schema Format String Syntax](#) section.

**Important:** For a complete list of the statistics that are supported for the GPRS schema, refer to the [Statistics and Counters Reference](#).

**Usage**

Use this command to define schemas for GPRS bulk statistics collection in the generated stats report files.

Usually a schema consists of multiple variables to collect all the statistics for a particular situation. Using double quote marks and text within this command, the reported statistics can be easily identified.

Multiple GPRS schemas can be created to categorize GPRS bulk statistics. All of the schemas are processed at each collection interval. To create multiple GPRS schemas, re-issue the **gprs schema schema_name** command using a different schema name each time.
Example

Include the bulk statistic variable names to create a GPRS schema named gprssstats_sgsn1 that specifies collection of statistics (a schema format) for:

- context name
- GPRS service name
- number of LLC packets dropped

Use the following command:

```bash
gprs schema gprssstats_sgsn1 format "Context Name: %vpnname%
GPRS Service Name: %servname%
Total LLC Packets Dropped: %bssgp-total-usr-req-drop%
"```
gtpc schema

Configures GPRS Tunneling Protocol-Control (GTPC) message statistics schema.

Product
- GGSN
- P-GW
- S-GW
- SAEGW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Bulk Statistics Configuration

**configure > bulkstats mode**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-bulkstats)#
```

Syntax

```
gtpc schema schema_name format schema_format
no gtpc schema schema_name
```

- **no**
  Removes the specified schema.

- **schema_name**
  Specifies the schema’s name.
  **schema_name** must be an alphanumeric string of 1 through 31 characters.

- **format schema_format**
  Specifies the schema’s format.
  **schema_format** must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of the command, including spaces’” characters. For more information, see the Schema Format String Length section.
  For information on the schema format’s syntax, see the Schema Format String Syntax section.

**Important:** For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

Usage

Use this command to define schemas for GTPC bulk statistics collection. Multiple GTPC schemas can be created to categorize GTPC bulk statistics. All of the schemas are processed at each collection interval. To
create multiple GTPC schemas, re-issue the `gtpc schema schema_name` command using a different schema name.

**Example**

To create a GTPC-level schema named `gtpc_stats` that specifies a schema format of:
- Context Name: `vpnname`
- GGSN Service Name: `servname`
- Total PDP Contexts Processed: `setup-total`

Use the following command:

```bash
gtpc schema gtpc_stats format "Context Name: %vpnname%nGGSN Service Name: %servname%nTotal PDP Contexts Processed: %setup-total%n"
```
gtpp schema

Configures GPRS Tunneling Protocol-Prime (GTPP) statistics schema.

Product
- GGSN
- SGSN
- P-GW
- S-GW
- SAEGW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Bulk Statistics Configuration
configure > bulkstats mode

Entering the above command sequence results in the following prompt:

[local]host_name(config-bulkstats)#

Syntax

gtpp schema schema_name format schema_format

no gtpp schema schema_name

no
Removes the specified schema.

schema_name
Specifies the schema’s name.
schema_name must be an alphanumeric string of 1 through 31 characters.

format schema_format
Specifies the schema’s format.
schema_format must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of the command, including spaces”” characters. For more information, see the Schema Format String Length section.
For information on the schema format’s syntax, see the Schema Format String Syntax section.

Important: For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.
Usage

Use this command to define schemas for GTPP bulk statistics collection. Multiple GTPP schemas can be created to categorize GTPP bulk statistics. All of the schemas are processed at each collection interval. To create multiple GTPP schemas, re-issue the `gtpp schema schema_name` command using a different schema name.

Example

To create a GTPP schema named `gtpp_statistics` that specifies a schema format of:

- Time: `time`
- Total Redirection Requests Received: `redir-rcvd`

Use the following command:

```
gtpp schema gtpp_statistics format "Time: %time%
Total Redirection Requests Received: %redir-rcvd\n"
```
gtpu schema

Configures GTP-U bulk statistics schema.

Product
GGSN
HNB-GW
P-GW
S-GW
SAEGW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Bulk Statistics Configuration
configure > bulkstats mode

Entering the above command sequence results in the following prompt:

[local]host_name(config-bulkstats)#

Syntax

```
gtpu schema schema_name format schema_format
no gtpu schema schema_name
```

no
Removes the specified schema.

`schema_name`
Specifies the schema’s name.
`schema_name` must be an alphanumeric string of 1 through 31 characters.

`format schema_format`
Specifies the format of the collected GTP-U statistics by identifying the statistics variables and ordering the variables for presentation within the bulk statistics messages.
`schema_format` must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of the command, including spaces”” characters. For more information, see the Schema Format String Length section.
For information on the schema format’s syntax, see the Schema Format String Syntax section.

**Important:** For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.
Usage

Use this command to define schemas for GTP-U bulk statistics collection in the generated stats report files. Usually a schema consists of multiple variables to collect all the statistics for a particular situation. Using double quote marks and text within this command, the reported statistics can be easily identified. Multiple GTP-U schemas can be created to categorize GTP-U bulk statistics. All of the schemas are processed at each collection interval. To create multiple GTP-U schemas, re-issue the `gtpu schema schema_name` command using a different schema name each time.
ha schema

Configures Home Agent (HA) bulk statistics schema.

**Product**
HA

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Bulk Statistics Configuration

```plaintext
configure > bulkstats mode
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-bulkstats)#
```

**Syntax**

```plaintext
ha schema schema_name format schema_format

no ha schema schema_name
```

---

`no`

Removes the specified schema.

`schema_name`

Specifies the schema’s name.
`schema_name` must be an alphanumeric string of 1 through 31 characters.

`format schema_format`

Specifies the schema’s format.
`schema_format` must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of the command, including spaces”” characters. For more information, see the [Schema Format String Length section](#).

For information on the schema format’s syntax, see the [Schema Format String Syntax section](#).

---

**Important**: For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

---

**Usage**

Use this command to define schemas for HA bulk statistics collection. Multiple HA service schemas can be created to categorize HA service bulk statistics. All of the schemas are processed at each collection interval.

To create multiple HA service schemas, re-issue the `ha schema schema_name` command using a different schema name.

**Example**

For an HA schema named `haservicestats` that specifies a schema format of:
• Number of HA authentication failures: `reply-hauthfail`
• Number of Mobile Node authentication failures: `reply-mauthfail`

Use the following command:

```
ha schema haservicestats format "Number of HA authentication failures: %reply-hauthfail
Number of Mobile Node authentication failures: %reply-mauthfail"
```
header

Configures the header string placed at the beginning of the generated bulk statistics data files.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Bulk Statistics Configuration

```
configure > bulkstats mode
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-bulkstats)#
```

Syntax

```
header format schema_format

no header format
```

no

Clears the header format string which results in the default file header being used in generated data files.

```
format schema_format
```

Specifies the header format string for use in generated data files.

*schema_format* must be an alphanumeric string of 1 through 2047 characters. The format string syntax is described in the Schema Format String Syntax section. Default: "" (an empty header)

The following variables are supported:

Table 18. header Command Format String Variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
<th>Data Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>date</td>
<td>The UTC date that the collection file was created in YYYYMMDD format where YYYY represents the year, MM represents the month and DD represents the day.</td>
<td>String</td>
</tr>
<tr>
<td>date3</td>
<td>The UTC date that the collection file was created in YYMMDD format where YY represents the year, MM represents the month and DD represents the day.</td>
<td>String</td>
</tr>
<tr>
<td>host</td>
<td>The system hostname that created the file</td>
<td>String</td>
</tr>
<tr>
<td>ipaddr</td>
<td>The default management (local context) IP address in ###.###.###.### format. An empty string is inserted if no address is available.</td>
<td>String</td>
</tr>
<tr>
<td>sysuptime</td>
<td>The uptime (in seconds) of the system that created the file.</td>
<td>32-bit signed</td>
</tr>
<tr>
<td>time</td>
<td>The time that the collection file was created in HHMMSS format where HH represents the hours, MM represents the minutes, and SS represents the seconds.</td>
<td>String</td>
</tr>
</tbody>
</table>
Usage

Define a unique header in data files which allows for easy identification as to which system generated the data file or any other useful information. Using the variables described above allows for a uniform header across all systems. The hostname variable should be used to identify the source of the data in the header and all remaining items can be formatted consistently across all chassis.

Example

The following commands define different header formats:

```
header format northStreet

header format "Created on: %date%-%time% by %host%"

no header format
```
### hnbgw-hnbap schema

Configures bulk statistics schema for HNB-Application Part (HNB-AP) message statistics collection in HNB-GW session instance.

**Product**  
HNB-GW

**Privilege**  
Security Administrator, Administrator

**Mode**  
Exec > Global Configuration > Bulk Statistics Configuration  
configure > bulkstats mode

Entering the above command sequence results in the following prompt:

```plaintext
[local]host_name(config-bulkstats)#
```

**Syntax**

```
hnbgw-hnbap schema schema_name schema_format  

no hnbgw-hnbap schema schema_name
```

- **Schema Name**
  - Specifies a name for the HNB-GW-HNB-AP schema.  
  - `schema_name` must be an alphanumeric string of 1 through 31 characters.

- **Format**
  - Specifies the schema’s format.  
  - `schema_format` must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of the command, including spaces”” characters. For more information, see the `Schema Format String Length` section.  
  - For information on the schema format’s syntax, see the `Schema Format String Syntax` section.

**Important:** For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

**Usage**

This command defines schemas used for HNB-AP statistics collection. Multiple HNB-AP schemas can be created to further categorize bulk statistics. All of the schemas are processed at each collection interval. To create multiple schemas, re-issue the `hnbgw-hnbap schema schema_name` command using a different schema name.

**Example**
The following command creates a schema named `hnbap1stats1` that records the number of registered UEs and registered HNBs along with Context name, Context Id, and HNB-GW service name:

```
hnbgw-hnbap schema hnbap1stats1 format "%vpnname%-%vpnid%-%servname-%
%registered-hnb%-%registered-ue%"
```

To create a schema named `hnbapuestats` that specifies a schema format of:

- Number of UEs with CS and PS Core Network Connections: `ue-with-ps-cs-conn`
- Number of UEs in Idle Condition: `idle-ue`

Use the following command:

```
hnbgw-hnbap schema hnbapuestats format "Number of UEs with CS and PS Core Network Connections: %ue-with-ps-cs-conn%\nNumber of UEs in Idle Condition: %idle-ue%"
```
**hnbgw-hnbap-access-closed schema**

Configures bulk statistics schema for HNB-Application Part (HNB-AP) message statistics collection in HNB-GW session instance for closed access mode.

**Product**

HNB-GW

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Bulk Statistics Configuration

configure > bulkstats mode

Entering the above command sequence results in the following prompt:

[local]host_name(config-bulkstats)#

**Syntax**

```
 hnbgw-hnbap-access-closed schema schema_name schema_format

no hnbgw-hnbap-access-closed schema schema_name
```

- **no**
  
  Removes the configured HNB-GW-HNB-AP-ACCESS-CLOSED schema.

- **schema_name**
  
  Specifies a name for the HNB-GW-HNB-AP-ACCESS-CLOSED schema. 
  `schema_name` must be an alphanumeric string of 1 through 31 characters.

- **format schema_format**
  
  Specifies the schema's format. 
  `schema_format` must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of the command, including spaces”” characters. For more information, see the Schema Format String Length section. 
  For information on the schema format’s syntax, see the Schema Format String Syntax section.

**Important:** For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

**Usage**

This command defines schemas used for HNB-AP statistics collection in closed access mode. Multiple HNB-AP-ACCESS-CLOSED schemas can be created to further categorize bulk statistics. All of the schemas are processed at each collection interval. To create multiple schemas, re-issue the `hnbgw-hnbap-access-closed schema schema_name` command using a different schema name.

**Example**
The following command creates a schema named `hnbapclosed1stats1` that records the number of registered UEs and registered HNBs along with Context name, Context Id, and HNB-GW service name:

```
hnbgw-hnbap-access-closed schema hnbapclosed1stats1 format "%vpnname%-%vpnid%-%servname%-%registered-hnb%-%registered-ue%"
```

To create a schema named `hnbapaccesscloseduestats` that specifies a schema format of:

- Number of UEs with CS and PS Core Network Connections: `ue-with-ps-cs-conn`
- Number of UEs in Idle Condition: `idle-ue`

Use the following command:

```
hnbgw-hnbap-access-closed schema hnbapaccesscloseduestats format "Number of UEs with CS and PS Core Network Connections: %ue-with-ps-cs-conn\nNumber of UEs in Idle Condition: %idle-ue"
```
hnbgw-hnbap-access-hybrid schema

Configures bulk statistics schema for HNB-Application Part (HNB-AP) message statistics collection in HNB-GW session instance for hybrid access mode.

Product
HNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Bulk Statistics Configuration
configure > bulkstats mode

Entering the above command sequence results in the following prompt:

[local]host_name(config-bulkstats)#

Syntax

```
  hnbgw-hnbap-access-hybrid schema  schema_name  schema_format
  no hnbgw-hnbap-access-hybrid schema  schema_name
```

- **no**
  - Removes the configured HNB-GW-HNB-AP-ACCESS-HYBRID schema.
  
  **schema_name**
  - Specifies a name for the HNB-GW-HNB-AP-ACCESS-HYBRID schema.
  
  **schema_format**
  - Specifies the schema’s format.

  `schema_format` must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of the command, including spaces”” characters. For more information, see the Schema Format String Length section.

  For information on the schema format’s syntax, see the Schema Format String Syntax section.

**Important:** For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

Usage

This command defines schemas used for HNB-AP statistics collection in hybrid access mode. Multiple HNB-AP-ACCESS-HYBRID schemas can be created to further categorize bulk statistics. All of the schemas are processed at each collection interval. To create multiple schemas, re-issue the `hnbgw-hnbap-access-hybrid schema  schema_name` command using a different schema name.

Example
The following command creates a schema named `hnbaphyblstats1` that records the number of registered UEs and registered HNBs along with Context name, Context Id, and HNB-GW service name:

```
hnbgw-hnbap-access-hybrid schema hnbaphyblstats1 format "%vpname%-%vpnid%-%servname%-%registered-hnb%-%registered-ue"
```

To create a schema named `hnbapaccesshybuestats` that specifies a schema format of:

- Number of UEs with CS and PS Core Network Connections: `ue-with-ps-cs-conn`
- Number of UEs in Idle Condition: `idle-ue`

Use the following command:

```
hnbgw-hnbap-access-hybrid schema hnbapaccesshybuestats format "Number of UEs with CS and PS Core Network Connections: %ue-with-ps-cs-conn\nNumber of UEs in Idle Condition: %idle-ue"
```
**hnbgw-hnbap-access-open schema**

Configures bulk statistics schema for HNB-Application Part (HNB-AP) message statistics collection in HNB-GW session instance for open access mode.

**Product**
HNB-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Bulk Statistics Configuration
configure > bulkstats mode

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-bulkstats)#
```

**Syntax**

```
hnbgw-hnbap-access-open schema schema_name schema_format
no hnbgw-hnbap-access-open schema schema_name
```

**no**
Removes the configured HNB-AP-ACCESS-OPEN schema.

**schema_name**
Specifies a name for the HNB-AP-ACCESS-OPEN schema.
*schema_name* must be an alphanumeric string of 1 through 31 characters.

**format schema_format**
Specifies the schema’s format.
*schema_format* must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of the command, including spaces”’” characters. For more information, see the Schema Format String Length section. For information on the schema format’s syntax, see the Schema Format String Syntax section.

**Important:** For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

**Usage**

This command defines schemas used for HNB-AP statistics collection in open access mode. Multiple HNB-AP-ACCESS-OPEN schemas can be created to further categorize bulk statistics. All of the schemas are processed at each collection interval. To create multiple schemas, re-issue the *hnbgw-hnbap-access-open schema schema_name* command using a different schema name.

**Example**
The following command creates a schema named *hnbapopen1stats1* that records the number of registered UEs and registered HNBs along with Context name, Context Id, and HNB-GW service name:

```
hnbgw-hnbap-access-open schema hnbapopen1stats1 format "%vpnname%-%vpnid%-%servname-%registered-hnb-%registered-ue%"
```

To create a schema named *hnbapaccessopenuestats* that specifies a schema format of:

- Number of UEs with CS and PS Core Network Connections: *ue-with-ps-cs-conn*
- Number of UEs in Idle Condition: *idle-ue*

Use the following command:

```
hnbgw-hnbap-access-open schema hnbapaccessopenuestats format "Number of UEs with CS and PS Core Network Connections: %ue-with-ps-cs-conn%\nNumber of UEs in Idle Condition: %idle-ue%"
```
hnbgw-ranap schema


Product
HNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Bulk Statistics Configuration

configure > bulkstats mode

Entering the above command sequence results in the following prompt:

[local]host_name(config-bulkstats)#

Syntax

hnbgw-ranap schema  schema_name  format  schema_format

no  hnbgw-ranap schema  schema_name

no

Removes the configured HNB-GW-RANAP schema.

schema_name

Specifies a name for the HNB-GW-RANAP schema.

schema_name must be an alphanumeric string of 1 through 31 characters.

format  schema_format

Specifies the schema’s format.

schema_format must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of the command, including spaces”” characters. For more information, see the Schema Format String Length section.

For information on the schema format’s syntax, see the Schema Format String Syntax section.

Important: For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

Usage

This command defines schemas used for RANAP messaging statistics collection. Multiple RANAP schemas can be created to further categorize bulk statistics. All of the schemas are processed at each collection interval. To create multiple schemas, re-issue the hnbgw-ranap schema  schema_name command using a different schema name.

Example
The following command creates a schema named `ranap1stats1` that records the number of CS-Direct-Transfer messages sent and received on RANAP along with Context name, Context Id, and HNB-GW service name:

```
hnbgw-ranap schema ranap1stats1 format "\%vpnname\%-\%vpnid\%-\%servname\%-\%cs-dir-transfer-rx\%-\%cs-dir-transfer-tx\%"
```

To create a schema named `ranappagingstats` that specifies a schema format of:

- Number of paging requests sent on RANAP from CS Core Network Connections: `cs-paging-req-tx`
- Number of paging requests sent on RANAP from PS Core Network Connections: `ps-paging-req-tx`

Use the following command:

```
hnbgw-ranap schema ranappagingstats format "Number of paging requests sent on RANAP from CS Core Network Connections: %cs-paging-req-tx\nNumber of paging requests sent on RANAP from PS Core Network Connections: %ps-paging-req-tx\%"
```
**hnbgw-ranap-access-closed schema**


**Product**
HNB-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Bulk Statistics Configuration

`configure > bulkstats mode`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-bulkstats)#
```

**Syntax**

```
hnbgw-ranap-access-closed schema schema_name format schema_format

no hnbgw-ranap-access-closed schema schema_name
```

**no**
Removes the configured HNB-GW-RANAP-ACCESS-CLOSED schema.

```
schema_name
```

Specifies a name for the HNB-GW-RANAP-ACCESS-CLOSED schema. `schema_name` must be an alphanumeric string of 1 through 31 characters.

```
format schema_format
```

Specifies the schema’s format. `schema_format` must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of the command, including spaces”” characters. For more information, see the Schema Format String Length section.

For information on the schema format’s syntax, see the Schema Format String Syntax section.

**Important:** For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

**Usage**

This command defines schemas used for RANAP messaging statistics collection in closed access mode. Multiple HNB-GW-RANAP-ACCESS-CLOSED schemas can be created to further categorize bulk statistics. All of the schemas are processed at each collection interval. To create multiple schemas, re-issue the `hnbgw-ranap-access-closed schema schema_name` command using a different schema name.

**Example**
The following command creates a schema named `ranapclosed1stats1` that records the number of CS-Direct-Transfer messages sent and received on RANAP along with Context name, Context Id, and HNB-GW service name:

```
hnbgw-ranap-access-closed schema ranapclosed1stats1 format "%vpnname%-%vpnid%-%servname%-%cs-dir-transfer-rx%-%cs-dir-transfer-tx%"
```

To create a schema named `ranapclosedpagingstats` that specifies a schema format of:

- Number of paging requests sent on RANAP from CS Core Network Connections: `cs-paging-req-tx`
- Number of paging requests sent on RANAP from PS Core Network Connections: `ps-paging-req-tx`

Use the following command:

```
hnbgw-ranap-access-closed schema ranapclosedpagingstats format "Number of paging requests sent on RANAP from CS Core Network Connections: %cs-paging-req-tx\nNumber of paging requests sent on RANAP from PS Core Network Connections: %ps-paging-req-tx"
```
hnbgw-ranap-access-hybrid schema


Product
HNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Bulk Statistics Configuration

configure > bulkstats mode

Entering the above command sequence results in the following prompt:

[local]host_name(config-bulkstats)#

Syntax

hnbgw-ranap-access-hybrid schema schema_name format schema_format

no hnbgw-ranap-access-hybrid schema schema_name

Syntax

no

Removes the configured HNB-GW-RANAP-ACCESS-HYBRID schema.

schema_name

Specifies a name for the HNB-GW-RANAP-ACCESS-HYBRID schema.

schema_name must be an alphanumeric string of 1 through 31 characters.

format schema_format

Specifies the schema’s format.

schema_format must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of the command, including spaces”” characters. For more information, see the Schema Format String Length section.

For information on the schema format’s syntax, see the Schema Format String Syntax section.

Important: For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

Usage

This command defines schemas used for RANAP messaging statistics collection in hybrid access mode. Multiple HNB-GW-RANAP-ACCESS-HYBRID schemas can be created to further categorize bulk statistics. All of the schemas are processed at each collection interval. To create multiple schemas, re-issue the hnbgw-ranap-access-hybrid schema schema_name command using a different schema name.

Example
The following command creates a schema named `ranaphyblstats1` that records the number of CS-Direct-Transfer messages sent and received on RANAP along with Context name, Context Id, and HNB-GW service name:

```
hnbgw-ranap-access-hybrid schema ranaphyblstats1 format "%vpnname%-%vpnid%-%servname%-%cs-dir-transfer-rx%-%cs-dir-transfer-tx%"
```

To create a schema named `ranaphybpagingstats` that specifies a schema format of:

- Number of paging requests sent on RANAP from CS Core Network Connections: `cs-paging-req-tx`
- Number of paging requests sent on RANAP from PS Core Network Connections: `ps-paging-req-tx`

Use the following command:

```
hnbgw-ranap-access-hybrid schema ranaphybpagingstats format "Number of paging requests sent on RANAP from CS Core Network Connections: %cs-paging-req-tx\nNumber of paging requests sent on RANAP from PS Core Network Connections: %ps-paging-req-tx"
```
Bulk Statistics Configuration Mode Commands

hnbgw-ranap-access-open schema

Configures bulk statistics schema for Radio Access Network-Application Part (RANAP) message statistics collection in HNB-GW session instance for open access mode.

Product
HNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Bulk Statistics Configuration
configure > bulkstats mode

Entering the above command sequence results in the following prompt:

[local]host_name(config-bulkstats)#

Syntax

hnbgw-ranap-access-open schema schema_name format schema_format

no hnbgw-ranap-access-open schema schema_name

no

Removes the configured HNB-GW-RANAP-ACCESS-OPEN schema.

schema_name

Specifies a name for the HNB-GW-RANAP-ACCESS-OPEN schema.
schema_name must be an alphanumeric string of 1 through 31 characters.

format schema_format

Specifies the schema’s format.
schema_format must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of the command, including spaces”” characters. For more information, see the Schema Format String Length section.
For information on the schema format’s syntax, see the Schema Format String Syntax section.

Important: For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

Usage

This command defines schemas used for RANAP messaging statistics collection in open access mode. Multiple HNB-GW-RANAP-ACCESS-OPEN schemas can be created to further categorize bulk statistics. All of the schemas are processed at each collection interval. To create multiple schemas, re-issue the hnbgw-ranap-access-open schema schema_name command using a different schema name.

Example
The following command creates a schema named `ranapopen1stats1` that records the number of CS-Direct-Transfer messages sent and received on RANAP along with Context name, Context Id, and HNB-GW service name:

```
hnbgw-ranap-access-open schema ranapopen1stats1 format "%vpnname%-%vpnid%-%servname%-%cs-dir-transfer-rx%-%cs-dir-transfer-tx%"
```

To create a schema named `ranapopenpagingstats` that specifies a schema format of:

- Number of paging requests sent on RANAP from CS Core Network Connections: `cs-paging-req-tx`
- Number of paging requests sent on RANAP from PS Core Network Connections: `ps-paging-req-tx`

Use the following command:

```
hnbgw-ranap-access-open schema ranapopenpagingtats format "Number of paging requests sent on RANAP from CS Core Network Connections: %cs-paging-req-tx\nNumber of paging requests sent on RANAP from PS Core Network Connections: %ps-paging-req-tx"
```
**hnbgw-rtp schema**


**Product**
HNB-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Bulk Statistics Configuration

**Syntax**

```
hnbgw-rtp schema schema_name format schema_format
```

```
no hnbgw-rtp schema schema_name
```

- **no**
  Removes the configured HNB-GW-RTP schema.

- **schema_name**
  Specifies a name for the HNB-GW-RTP schema.
  *schema_name* must be an alphanumeric string of 1 through 31 characters.

- **format schema_format**
  Specifies the schema’s format.
  *schema_format* must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of the command, including spaces”” characters. For more information, see the Schema Format String Length section.
  For information on the schema format’s syntax, see the Schema Format String Syntax section.

**Important:** For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

**Usage**

This command defines schemas used for RTP messaging statistics collection. Multiple RTP schemas can be created to further categorize bulk statistics. All of the schemas are processed at each collection interval. To create multiple schemas, re-issue the *hnbgw-rtp schema schema_name* command using a different schema name.

**Example**
The following command creates a schema named `rtpstats1` that records the number of RTP uplink packets dropped and number of RTCP application report messages received on RTP link along with Context name, Context Id, and HNB-GW service name:

```
hnbgw-rtp schema rtpstats1 format "%vpnnname%-%vpnid%-%servname%-%rtp-uplink-pkts-dropped%-%rtcp-app-report-rx"
```
**hnbgw-rtp-access-closed schema**

Configures bulk statistics schema for Real-Time Protocol (RTP) message statistics collection in HNB-GW session instance for closed access mode.

**Product**
HNB-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Bulk Statistics Configuration
configure > bulkstats mode

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-bulkstats)#
```

**Syntax**

```
hnbgw-rtp-access-closed schema schema_name format schema_format

no hnbgw-rtp-access-closed schema schema_name
```

**no**
Removes the configured HNB-GW-RTP-ACCESS-CLOSED schema.

**schema_name**
Specifies a name for the HNB-GW-RTP-ACCESS-CLOSED schema.
*schema_name* must be an alphanumeric string of 1 through 31 characters.

**format schema_format**
Specifies the schema’s format.
*schema_format* must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of the command, including spaces”” characters. For more information, see the Schema Format String Length section.
For information on the schema format’s syntax, see the Schema Format String Syntax section.

**Important:** For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

**Usage**

This command defines schemas used for RTP messaging statistics collection in closed access mode. Multiple HNB-GW-RTP-ACCESS-CLOSED schemas can be created to further categorize bulk statistics. All of the schemas are processed at each collection interval. To create multiple schemas, re-issue the `hnbgw-rtp-access-closed schema schema_name` command using a different schema name.

**Example**
Bulk Statistics Configuration Mode Commands

The following command creates a schema named `rtpclosed1stats1` that records the number of RTP uplink packets dropped and number of RTCP application report messages received on RTP link along with Context name, Context Id, and HNB-GW service name:

```
hnbgw-rtp-access-closed schema rtpclosed1stats1 format "%vpnname%-%vpnid%-%servname%-%rtp-uplink-pkts-dropped%-%rtcp-app-report-rx"
```
hnbgw-rtp-access-hybrid schema

Configures bulk statistics schema for Real-Time Protocol (RTP) message statistics collection in HNB-GW session instance for hybrid access mode.

Product
HNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Bulk Statistics Configuration
configure > bulkstats mode

Entering the above command sequence results in the following prompt:

[local]host_name(config-bulkstats)>

Syntax

hnbgw-rtp-access-hybrid schema schema_name format schema_format

no hnbgw-rtp-access-hybrid schema schema_name

no

Removes the configured HNB-GW-RTP-ACCESS-HYBRID schema.

schema_name

Specifies a name for the HNB-GW-RTP-ACCESS-HYBRID schema.
schema_name must be an alphanumeric string of 1 through 31 characters.

format schema_format

Specifies the schema’s format.
schema_format must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of the command, including spaces”” characters. For more information, see the Schema Format String Length section.
For information on the schema format’s syntax, see the Schema Format String Syntax section.

Important: For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

Usage

This command defines schemas used for RTP messaging statistics collection in hybrid access mode. Multiple HNB-GW-RTP-ACCESS-HYBRID schemas can be created to further categorize bulk statistics. All of the schemas are processed at each collection interval. To create multiple schemas, re-issue the hnbgw-rtp-access-hybrid schema schema_name command using a different schema name.
The following command creates a schema named `rtphyblstats1` that records the number of RTP uplink packets dropped and number of RTCP application report messages received on RTP link along with Context name, Context Id, and HNB-GW service name:

```
  hnbgw-rtp-access-hybrid schema rtphyblstats1 format "%vpname%-%vpnid-%servname%-%rtp-uplink-pkts-dropped%-rtcp-app-report-rx"
```
hnbgw-rtp-access-open schema

Configures bulk statistics schema for Real-Time Protocol (RTP) message statistics collection in HNB-GW session instance for open access mode.

Product
HNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Bulk Statistics Configuration
configure > bulkstats mode

Entering the above command sequence results in the following prompt:

[local]hostname(config-bulkstats)#

Syntax

hnbgw-rtp-access-open schema schema_name format schema_format

no hnbgw-rtp-access-open schema schema_name

no
Removes the configured HNB-GW-RTP-ACCESS-OPEN schema.

schema_name
Specifies a name for the HNB-GW-RTP-ACCESS-OPEN schema.
schema_name must be an alphanumeric string of 1 through 31 characters.

format schema_format
Specifies the schema’s format.
schema_format must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of the command, including spaces”” characters. For more information, see the Schema Format String Length section.
For information on the schema format’s syntax, see the Schema Format String Syntax section.

Important: For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

Usage
This command defines schemas used for RTP messaging statistics collection in open access mode. Multiple HNB-GW-RTP-ACCESS-OPEN schemas can be created to further categorize bulk statistics. All of the schemas are processed at each collection interval. To create multiple schemas, re-issue the hnbgw-rtp-access-open schema schema_name command using a different schema name.

Example
The following command creates a schema named `rtpopen1stats1` that records the number of RTP uplink packets dropped and number of RTCP application report messages received on RTP link along with Context name, Context Id, and HNB-GW service name:

```
hnbgw-rtp-access-open schema rtpopen1stats1 format "%vpnname%-%vpnid-%servname-%rtp-uplink-pkts-dropped-%rtcp-app-report-rx"
```
**hnbgw-rua schema**

Configures bulk statistics schema for RANAP User Adaptation (RUA) protocol message statistics collection in HNB-GW session instance.

**Product**
HNB-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Bulk Statistics Configuration
```
configure > bulkstats mode
```

Entering the above command sequence results in the following prompt:
```
[local]host_name(config-bulkstats)#
```

**Syntax**
```

hnbgw-rua schema schema_name format schema_format

no hnbgw-rua schema schema_name

```

<table>
<thead>
<tr>
<th>no</th>
</tr>
</thead>
<tbody>
<tr>
<td>Removes the configured HNB-GW-RUA schema.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>schema_name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies a name for the HNB-GW-RUA schema.</td>
</tr>
</tbody>
</table>

*schema_name* must be an alphanumeric string of 1 through 31 characters.

<table>
<thead>
<tr>
<th>format schema_format</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the schema’s format.</td>
</tr>
</tbody>
</table>

*schema_format* must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of the command, including spaces”” characters. For more information, see the Schema Format String Length section.

For information on the schema format’s syntax, see the Schema Format String Syntax section.

---

**Important:** For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

---

**Usage**

This command defines schemas used for RUA protocol messaging statistics collection. Multiple RUA schemas can be created to further categorize bulk statistics. All of the schemas are processed at each collection interval. To create multiple schemas, re-issue the *hnbgw-rua schema schema_name* command using a different schema name.

---

**Example**
The following command creates a schema named `ruastats1` that records the number of CS-Connect messages received and sent on RUA link along with Context name, Context Id, and HNB-GW service name:

```
hnbgw-rua schema rua1stats1 format "%vpnname%-%vpnid%-%servname%-%cs-connect-rx%-%cs-connect-tx%"
```
**hnbgw-rua-access-closed schema**

Configures bulk statistics schema for RANAP User Adaptation (RUA) protocol message statistics collection in HNB-GW session instance in closed access mode.

**Product**

HNB-GW

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Bulk Statistics Configuration

```
configure > bulkstats mode
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-bulkstats)#
```

**Syntax**

```
hnbgw-rua-access-closed schema schema_name format schema_format

no hnbgw-rua-access-closed schema schema_name
```

- **no**
  
  Removes the configured HNB-GW-RUA-ACCESS-CLOSED schema.

- **schema_name**
  
  Specifies a name for the HNB-GW-RUA-ACCESS-CLOSED schema. 
  
  `schema_name` must be an alphanumeric string of 1 through 31 characters.

- **format schema_format**
  
  Specifies the schema’s format.
  
  `schema_format` must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of the command, including spaces” characters. For more information, see the Schema Format String Length section.
  
  For information on the schema format’s syntax, see the Schema Format String Syntax section.

**Important:** For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

**Usage**

This command defines schemas used for RUA protocol messaging statistics collection in closed access mode. Multiple HNB-GW-RUA-ACCESS-CLOSED schemas can be created to further categorize bulk statistics. All of the schemas are processed at each collection interval. To create multiple schemas, re-issue the `hnbgw-rua-access-closed schema schema_name` command using a different schema name.

**Example**
The following command creates a schema named `ruaclosed1stats1` that records the number of CS-Connect messages received and sent on RUA link along with Context name, Context Id, and HNB-GW service name:

```
hnbgw-rua-access-closed schema ruaclosed1stats1 format "%vpnname%-%vpnid-%servname-%cs-connect-rx-%cs-connect-tx"
```
**hnbgw-rua-access-hybrid schema**

Configures bulk statistics schema for RANAP User Adaptation (RUA) protocol message statistics collection in HNB-GW session instance in hybrid access mode.

**Product**

HNB-GW

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Bulk Statistics Configuration

`configure > bulkstats mode`

Entering the above command sequence results in the following prompt:

`[local]host_name(config-bulkstats)#`

**Syntax**

```
hnbgw-rua-access-hybrid schema schema_name format schema_format
```

```
no hnbgw-rua-access-hybrid schema schema_name
```

---

**no**

Removes the configured HNB-GW-RUA-ACCESS-HYBRID schema.

```
schema_name
```

Specifies a name for the HNB-GW-RUA-ACCESS-HYBRID schema. 

`schema_name` must be an alphanumeric string of 1 through 31 characters.

```
format schema_format
```

Specifies the schema’s format.

`schema_format` must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of the command, including spaces”“ characters. For more information, see the Schema Format String Length section.

For information on the schema format’s syntax, see the Schema Format String Syntax section.

---

**Important:** For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

---

**Usage**

This command defines schemas used for RUA protocol messaging statistics collection in hybrid access mode. Multiple HNB-GW-RUA-ACCESS-HYBRID schemas can be created to further categorize bulk statistics. All of the schemas are processed at each collection interval. To create multiple schemas, re-issue the `hnbgw-rua-access-hybrid schema schema_name` command using a different schema name.

---

**Example**

```bash
hnbgw-rua-access-hybrid schema MySchema format MyFormat
```
The following command creates a schema named `ruahyb1stats1` that records the number of CS-Connect messages received and sent on RUA link along with Context name, Context Id, and HNB-GW service name:

```
hnbgw-rua-access-hybrid schema ruahyb1stats1 format "%vpnname%-%vpnid-%servname%-cs-connect-rx%-cs-connect-tx"
```
**hnbgw-rua-access-open schema**

Configures bulk statistics schema for RANAP User Adaptation (RUA) protocol message statistics collection in HNB-GW session instance in open access mode.

**Product**

HNB-GW

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Bulk Statistics Configuration

`configure > bulkstats mode`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-bulkstats)#
```

**Syntax**

```
hnbgw-rua-access-open schema schema_name format schema_format

no hnbgw-rua-access-open schema schema_name
```

- **no**
  
  Removes the configured HNB-GW-RUA-ACCESS-OPEN schema.

- **schema_name**
  
  Specifies a name for the HNB-GW-RUA-ACCESS-OPEN schema.
  `schema_name` must be an alphanumeric string of 1 through 31 characters.

- **format schema_format**
  
  Specifies the schema’s format.
  `schema_format` must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of the command, including spaces”” characters. For more information, see the Schema Format String Length section.
  For information on the schema format’s syntax, see the Schema Format String Syntax section.

**Important:** For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

**Usage**

This command defines schemas used for RUA protocol messaging statistics collection in open access mode. Multiple HNB-GW-RUA-ACCESS-OPEN schemas can be created to further categorize bulk statistics. All of the schemas are processed at each collection interval. To create multiple schemas, re-issue the `hnbgw-rua-access-open schema schema_name` command using a different schema name.

**Example**
The following command creates a schema named `ruaopen1stats1` that records the number of CS-Connect messages received and sent on RUA link along with Context name, Context Id, and HNB-GW service name:

```
hnbgw-rua-access-open schema ruaopen1stats1 format "%vpnname%-%vpnid-%servname%-cs-connect-rx%-cs-connect-tx"
```
hnbgw-sctp schema


Product
HNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Bulk Statistics Configuration
configure > bulkstats mode

Entering the above command sequence results in the following prompt:

[local]host_name(config-bulkstats)#

Syntax

hnbgw-sctp schema schema_name format schema_format

no hnbgw-sctp schema schema_name

<table>
<thead>
<tr>
<th>no</th>
</tr>
</thead>
<tbody>
<tr>
<td>Removes the configured SCTP schema.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>schema_name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies a name for the SCTP schema.</td>
</tr>
<tr>
<td><em>schema_name</em> must be an alphanumeric string of 1 through 31 characters.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>format schema_format</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the schema’s format.</td>
</tr>
<tr>
<td><em>schema_format</em> must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of the command, including spaces”” characters. For more information, see the Schema Format String Length section.</td>
</tr>
<tr>
<td>For information on the schema format’s syntax, see the Schema Format String Syntax section.</td>
</tr>
</tbody>
</table>

**Important:** For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*. 

Usage

This command defines schemas used for SCTP protocol messaging statistics collection. Multiple SCTP schemas can be created to further categorize bulk statistics. All of the schemas are processed at each collection interval. To create multiple schemas, re-issue the `hnbgw-sctp schema schema_name` command using a different schema name.

Example
The following command creates a schema named `sctp1stats1` that records the number of bytes received from lower layer and number of bytes sent to lower layer over SCTP connection along with Context name, Context Id, and HNB-GW service name:

```
hnbgw-sctp schema sctp1stats1 format "%vpnname%-%vpnid%-%servname%-%
%total-bytes-sent-to-lower-layer%-%total-bytes-rcvd-from-lower-layer%"
```
**hsgw schema**

Configures HRPD Serving Gateway (HSGW) bulk statistics schema.

**Product**

HSGW

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Bulk Statistics Configuration

*configure > bulkstats mode*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-bulkstats)#
```

**Syntax**

```
hsgw schema schema_name format schema_format
```

```
no hsgw schema schema_name
```

- **no**
  - Removes the specified schema.

- **schema_name**
  - Specifies the schema’s name.
  - *schema_name* must be an alphanumeric string of 1 through 31 characters.

- **format schema_format**
  - Specifies the format of the collected HSGW statistics by identifying the statistics variables and ordering the variables for presentation within the bulk statistics messages.
  - *schema_format* must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of the command, including spaces”” characters. For more information, see the Schema Format String Length section.
  - For information on the schema format’s syntax, see the Schema Format String Syntax section.

**Important:** For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

**Usage**

Use this command to define schemas for HSGW bulk statistics collection in the generated stats report files. Usually a schema consists of multiple variables to collect all the statistics for a particular situation. Using double quote marks and text within this command, the reported statistics can be easily identified.

Multiple HSGW schemas can be created to categorize HSGW bulk statistics. All of the schemas are processed at each collection interval. To create multiple HSGW schemas, re-issue the `**hsgw schema schema_name**` command using a different schema name each time.
**hss schema**

Configures Home Subscriber Service (HSS) bulk statistics schema.

**Product**
MME

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Bulk Statistics Configuration
```
configure > bulkstats mode
```
Entering the above command sequence results in the following prompt:

```
[local]host_name(config-bulkstats)#
```

**Syntax**

```
hss schema schema_name format schema_format

no hss schema schema_name
```

- **schema_name**
  Specifies the schema’s name.
  *schema_name* must be an alphanumeric string of 1 through 31 characters.

- **format schema_format**
  Specifies the schema’s format.
  *schema_format* must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of the command, including spaces”” characters. For more information, see the Schema Format String Length section.
  For information on the schema format’s syntax, see the Schema Format String Syntax section.

**Important:** For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

**Usage**

Use this command to define schemas for HSS bulk statistics collection. Multiple HSS schemas can be created to further categorize HSS bulk statistics. All of the schemas are processed at each collection interval. To create multiple HSS schemas, re-issue the `hss schema schema_name` command using a different schema name.

**Example**
To create an hss schema named \textit{hss\_stats} that specifies a schema format of:

- Message Stats: Number of Cancel Location Request messages sent: \textit{msg-cl-req}
- Message Stats: Number of Cancel Location Answer messages sent: \textit{msg-cl-ans}

Use the following command:

\begin{verbatim}
  hss schema hss_stats format "Message Stats: Number of Cancel Location Request messages sent: %msg-cl-req\nMessage Stats: Number of Cancel Location Answer messages sent: %msg-cl-ans\n"
\end{verbatim}
imsa schema


Product
GGSN
HA
HSGW
IPSG
PDSN
P-GW
S-GW
SAEGW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Bulk Statistics Configuration
configure > bulkstats mode

Entering the above command sequence results in the following prompt:

[local]host_name(config-bulkstats)#

Syntax

imsa schema schema_name format schema_format

no imsa schema schema_name

---

no

Removes the specified schema.

---

schema_name

Specifies the schema’s name.

schema_name must be an alphanumeric string of 1 through 31 characters.

---

format schema_format

Specifies the schema’s format.

schema_format must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of the command, including spaces”” characters. For more information, see the Schema Format String Length section.

For information on the schema format’s syntax, see the Schema Format String Syntax section.

---

Important: For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.
Usage

Use this command to define schemas for IMSA bulk statistics collection in the generated stats report files. Usually a schema consists of multiple variables to collect all the statistics for a particular situation. Using double quote marks and text within this command, the reported statistics can be easily identified. Multiple IMSA schemas can be created to categorize IMSA bulk statistics. All of the schemas are processed at each collection interval. To create multiple IMSA schemas, re-issue the `imsa schema schema_name` command using a different schema name each time.
**ippool schema**

Configures IP pool bulk statistics schema.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Bulk Statistics Configuration

```
configure > bulkstats mode
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-bulkstats)#
```

**Syntax**

```
ippool schema schema_name format schema_format

no ippool schema schema_name
```

- **no**
  Removes the specified schema.

  ```
  schema_name
  ```

  Specifies the schema’s name. `schema_name` must be an alphanumeric string of 1 through 31 characters.

- **format schema_format**
  Specifies the schema’s format. `schema_format` must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of the command, including spaces”” characters. For more information, see the `Schema Format String Length` section. For information on the schema format’s syntax, see the `Schema Format String Syntax` section.

**Important:** For a complete list of the statistics that are supported for this schema, refer to the `Statistics and Counters Reference`.

**Usage**

Use this command to define schemas for IP pool bulk statistics collection. Multiple IP pool schemas can be created to further categorize IP pool bulk statistics. All of the schemas are processed at each collection interval. To create multiple IP pool schemas, re-issue the `ippool schema schema_name` command using a different schema name.

**Example**

To create an IP pool schema named `ippoolstats` that specifies a schema format of:
- Number of IP addresses on hold: hold
- Number of free IP addresses: free

Use the following command:

```bash
ippool schema ippoolstats format "Number of IP addresses on hold: %hold%
Number of free IP addresses: %free%"
```
**ipsg schema**

Configures IP Services Gateway (IPSG) bulk statistics schema.

**Product**
IPSG

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Bulk Statistics Configuration

```
configure > bulkstats mode
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-bulkstats)#
```

**Syntax**

```
ipsg schema  schema_name format  schema_format
```

```
no ipsg schema  schema_name
```

- **no**
  Removes the specified schema.

- **schema_name**
  Specifies the schema’s name.

  - **schema_name** must be an alphanumeric string of 1 through 31 characters.

- **format schema_format**
  Specifies the schema’s format.

  - **schema_format** must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of the command, including spaces”” characters. For more information, see the Schema Format String Length section.
  
  For information on the schema format’s syntax, see the Schema Format String Syntax section.

**Important:** For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

**Usage**

Use this command to define the schemas used for IPSG bulk statistics collection. Multiple IPSG schemas can be created to categorize IPSG bulk statistics. All of the schemas are processed at each collection interval. To create multiple schemas, re-issue the `ipsg schema  schema_name` command using a different schema name.

**Example**

To create an IPSG schema named `ipsgstats` that specifies a schema format of:

- Context name: `vvpnname`
• Service name: servname
• Total responses sent: total-rsp-sent

Use the following command:

```plaintext
ipsg schema ippoolstats format "Context name: %vpnname%\nService name: %servname%\nTotal responses sent: %total-rsp-sent%\n"
```
**lac schema**

Configures LAC (L2TP Access Concentrator) bulk statistics schema.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Bulk Statistics Configuration

configure > bulkstats mode

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-bulkstats)#
```

**Syntax**

```
lac schema schema_name format schema_format

no lac schema schema_name
```

- **no**
  Removes the specified schema.

- **schema_name**
  Specifies the schema’s name.
  `schema_name` must be an alphanumeric string of 1 through 31 characters.

- **format schema_format**
  Specifies the schema’s format.
  `schema_format` must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of the command, including spaces”” characters. For more information, see the **Schema Format String Length** section.
  For information on the schema format’s syntax, see the **Schema Format String Syntax** section.

**Important:** For a complete list of the statistics that are supported for this schema, refer to the **Statistics and Counters Reference**.

**Usage**

Use this command to define schemas for LAC bulk statistics collection. Multiple LAC schemas can be created to categorize LAC bulk statistics. All of the schemas are processed at each collection interval. To create multiple schemas, re-issue the `lac schema schema_name` command using a different schema name.

**Example**

The following command creates a schema named `lac1stats1` that records the number of active subscriber sessions and the number of sessions that failed or were disconnected due to the maximum tunnel limit being reached:

```
lac schema lac1stats1 format %d %d
```
lac schema lac1stats1 format "%sess-curactive%-%sess-maxtunnel%"

To create a schema named lacresourcestats that specifies a schema format of:
• Number of Successful Session Connections: sess-successful
• Number of Session Attempts That Failed: sess-failed
• Number of Sessions Currently Active: sess-curative

Use the following command:

lac schema lacresourcestats format "Number of Successful Session Connections: %sess-successful\nNumber of Session Attempts That Failed: %sess-failed\nNumber of Sessions Currently Active: %sess-curative"
**limit**

Configures the maximum amount of system memory bulk statistics may utilize.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Bulk Statistics Configuration

```
configure > bulkstats mode
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-bulkstats)#
```

**Syntax**

```
limit kilobytes
```

*kilobytes*

Specifies the maximum amount of memory (in kilobytes) that may be used for bulk statistics as an integer from 1 through 32000. Default: 100

**Usage**

Adjust bulk statics memory usage when considering the sampling interval adjustments.

⚠️ **Caution:** Bulk statistics are stored in Random Access Memory (RAM) on the SPC/SMC/MIO. In the event of power loss or system failure, the statistics will be lost. If the maximum storage limit has been reached before the system's configured transfer-interval is reached, the oldest information stored in the collection will be overwritten.

**Example**

```
limit 2048
```
Ima schema

Configures the Local Mobility Anchor (LMA) statistics schema for the naming conventions of data files.

**Product**
P-GW
SAEGW

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Bulk Statistics Configuration

```configure > bulkstats mode```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-bulkstats)#
```

**Syntax**

```
lma schema schema_name format schema_format
no lma schema schema_name
```

- **no**
  - Removes the specified schema.

- **schema_name**
  - Specifies the schema’s name.
  - `schema_name` must be an alphanumeric string of 1 through 31 characters.

- **format schema_format**
  - Specifies the schema’s format.
  - `schema_format` must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of the command, including spaces’”” characters. For more information, see the Schema Format String Length section.
  - For information on the schema format’s syntax, see the Schema Format String Syntax section.

**Important:** For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

**Usage**

Use this command to define schemas for LMA bulk statistics collection. Multiple LMA service schemas can be created to categorize LMA service bulk statistics. All of the schemas are processed at each collection interval. To create multiple LMA service schemas, re-issue the `lma schema schema_name` command using a different schema name.

**Example**

For an LMA-level schema named `lmaservicestats` that specifies a schema format of:
• Binding Update Received: bindupd
• Binding Update Received - Denied: bindupd-denied

Use the following command:

```bash
lma schema lmaservicestats format "Number of Binding Updates Received: %bindupd%
Number of Binding Updates Received and Denied: %bindupd-denied%
"
```
Ins schema

Configures LNS (L2TP Network Server) bulk statistics schema.

Product: LNS

Privilege: Security Administrator, Administrator

Mode: Exec > Global Configuration > Bulk Statistics Configuration
configure > bulkstats mode

Entering the above command sequence results in the following prompt:

[local]host_name(config-bulkstats)#

Syntax

```
lns schema schema_name format schema_format
no lns schema schema_name
```

- **no**
  - Removes the specified schema.

- **schema_name**
  - Specifies the schema’s name.
  - `schema_name` must be an alphanumeric string of 1 through 31 characters.

- **format schema_format**
  - Specifies the format of the collected LNS statistics by identifying the statistics variables and ordering the variables for presentation within the bulk statistics messages.
  - `schema_format` must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of the command, including spaces”” characters. For more information, see the Schema Format String Length section.
  - For information on the schema format’s syntax, see the Schema Format String Syntax section.

**Important:** For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

Usage

Use this command to define schemas for LNS bulk statistics collection in the generated stats report files. Usually a schema consists of multiple variables to collect all the statistics for a particular situation. Using double quote marks and text within this command, the reported statistics can be easily identified.

Multiple LNS schemas can be created to categorize LNS bulk statistics. All of the schemas are processed at each collection interval. To create multiple LNS schemas, re-issue the `lns schema schema_name` command using a different schema name each time.
local-directory

Sets the local directory for storing bulkstats collection files.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Bulk Statistics Configuration

configure > bulkstats mode

Entering the above command sequence results in the following prompt:

[local]host_name(config-bulkstats)#

Syntax

local-directory pathname

no local-directory

no
Delete the setting for local-directory.

pathname
Specifies the local path of the directory in which to store bulkstats collection files.
pathname must be an alphanumeric string of 1 through 127 characters. Pathnames are case sensitive.

Usage
Use this command to designate a directory on a local file system in which collection files with bulkstats information are stored. The directory specified must already exist. Use the Exec Mode command mkdir to create a directory.

Example
To specify that bulkstats collection files are stored in the local directory /flash/bulkstats, enter the following command:

    local-directory /flash/bulkstats
mag schema

Configures the Mobile Access Gateway (MAG) statistics schema for naming conventions of data files.

**Product**
HSGW  
S-GW  
SAEGW

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Bulk Statistics Configuration
configure > bulkstats mode

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-bulkstats)#
```

**Syntax**

```
mag schema  schema_name  format  schema_format

no mag schema  schema_name
```

- **no**
  Removes the specified schema from MAG bulk statistics generation.

- **schema_name**
  Specifies the schema’s name.
  `schema_name` must be an alphanumeric string of 1 through 31 characters.

- **format  schema_format**
  Specifies the schema’s format.
  `schema_format` must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of the command, including spaces”” characters. For more information, see the *Schema Format String Length* section.
  For information on the schema format’s syntax, see the *Schema Format String Syntax* section.

**Important**: For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

**Usage**

Use this command to define schemas for MAG bulk statistics collection. Multiple MAG service schemas can be created to categorize MAG service bulk statistics. All of the schemas are processed at each collection interval. To create multiple MAG service schemas, re-issue the `mag schema  schema_name` command using a different schema name.
Example

For a MAG-level schema named `magservicestats` that specifies a schema format of:

- Binding Update Sent: `bindupd`
- Binding Acknowledgement Received: `bindack`

Use the following command:

```
mag schema magservicestats format "Number of Binding Updates Sent: %bindupd%
Number of Binding Acknowledgements Received: %bindack%"
```
### mipv6ha schema

Configures MIPv6 HA (home Agent) bulk statistics schema.

**Product**

HA

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Bulk Statistics Configuration  
`configure > bulkstats mode`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-bulkstats)#
```

**Syntax**

```
mipv6ha schema  schema_name  format  schema_format
```

```
no  mipv6ha schema  schema_name
```

- **no**
  
  Removes the specified schema.

- **schema_name**
  
  Specifies the schema’s name.
  
  `schema_name` must be an alphanumeric string of 1 through 31 characters.

- **format  schema_format**
  
  Specifies the schema’s format.
  
  `schema_format` must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of the command, including spaces”” characters. For more information, see the **Schema Format String Length** section.
  
  For information on the schema format’s syntax, see the **Schema Format String Syntax** section.

**Important:** For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

**Usage**

Use this command to define schemas for MIPv6 HA bulk statistics collection. Multiple MIPv6 HA bulk statistics schemas can be created to categorize MIPv6 HA bulk statistics. All of the schemas are processed at each collection interval. To create multiple MIPv6 HA service schemas, re-issue the `mipv6ha schema schema_name` command using a different schema name.

**Example**

The following command creates a schema named `mipv6haservicestats` that records the number of authorization attempt failures due to access rejects from AAA:
mipv6ha schema mipv6haservicestats format "%aaa-actauthfail%"
mme schema

Configures MME (Mobility Management Entity) bulk statistics schema.

Product
MME

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Bulk Statistics Configuration
configure > bulkstats mode

Entering the above command sequence results in the following prompt:

[local]host_name(config-bulkstats)#

Syntax

mme schema schema_name format schema_format

no mme schema schema_name

- no
  Removes the specified schema.

- schema_name
  Specifies the schema’s name.
  schema_name must be an alphanumeric string of 1 through 31 characters.

- format schema_format
  Specifies the schema’s format.
  schema_format must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of the command, including spaces”” characters. For more information, see the Schema Format String Length section.
  For information on the schema format’s syntax, see the Schema Format String Syntax section.

**Important:** For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

Usage

Use this command to define schemas for MME bulk statistics collection. Multiple MME bulk statistics schemas can be created to categorize MME bulk statistics. All of the schemas are processed at each collection interval. To create multiple MME service schemas, re-issue the mme schema schema_name command using a different schema name.

Example

The following command creates a schema named mmeservice_s1ap_cfg_transfers that records the total number of S1AP - transmit data - configuration transfers:
mme schema mmeservice_slap_cfg_transfersformat "slap-trnsdata-cfg-tfr"
mvs schema

Configures MVS (Mobile Videoscape) bulk statistics schema.

**Product**
MVG

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Bulk Statistics Configuration

`configure > bulkstats mode`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-bulkstats)#
```

**Syntax**

```
mvs schema  schema_name  format  schema_format

no mvs schema  schema_name
```

- **no**
  Removes the specified schema.

- **schema_name**
  Specifies the schema’s name.
  `schema_name` must be an alphanumeric string of 1 through 31 characters.

- **format  schema_format**
  Specifies the schema’s format.
  `schema_format` must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of the command, including spaces”” characters. For more information, see the Schema Format String Length section.
  For information on the schema format’s syntax, see the Schema Format String Syntax section.

**Important:** For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.
nat-realm schema

Creates and configures Network Address Translation (NAT) realm statistics schema.

Product
NAT

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Bulk Statistics Configuration
configure > bulkstats mode
Entering the above command sequence results in the following prompt:

[local]host_name(config-bulkstats)#

Syntax

nat-realm schema schema_name format schema_format

no nat-realm schema schema_name

schema_name
Specifies the schema’s name.
schema_name must be an alphanumeric string of 1 through 31 characters.

format schema_format
Specifies the schema’s format.
schema_format must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of
the command, including spaces”” characters. For more information, see the Schema Format String Length
section.
For information on the schema format’s syntax, see the Schema Format String Syntax section.

Important: For a complete list of the statistics that are supported for this schema, refer to the Statistics and
Counters Reference.

Usage
Use this command to define schemas for NAT Realm bulk statistics collection. Multiple NAT realm schemas
can be created to further categorize NAT realm level bulk statistics. All of the schemas are processed at each
collection interval. To create multiple NAT Realm schemas, re-issue the nat-realm schema
schema_name command using a different schema name.

Example
The following command creates a NAT realm schema with the VPN name, realm name, and flows
information:

nat-realm schema realm1 format “%vpnname% %realmname% %nat-rlm-flows%”
p2p schema

Creates and configures P2P (Peer-to-Peer) statistics schema.

Product
ADC

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Bulk Statistics Configuration
configure > bulkstats mode

Entering the above command sequence results in the following prompt:
[local]host_name(config-bulkstats)#

Syntax

p2p schema schema_name format schema_format

no p2p schema schema_name

**schema_name**

Specifies the schema’s name.
**schema_name** must be an alphanumeric string of 1 through 31 characters.

**format schema_format**

Specifies the schema’s format.
**schema_format** must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of the command, including spaces”” characters. For more information, see the **Schema Format String Length** section.
For information on the schema format’s syntax, see the **Schema Format String Syntax** section.

**Important:** For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

Usage

Use this command to define schemas for P2P bulk statistics collection. Multiple P2P schemas can be created to further categorize P2P-level bulk statistics. All of the schemas are processed at each collection interval. To create multiple P2P schemas, re-issue the **p2p schema schema_name** command using a different schema name.

Example

The following command creates a schema named **p2pstats** to record the total number of bytes detected in uplink and downlink direction:

```
p2p schema p2pstats format “%p2p-uplnk-bytes-name% %p2p-uplnk-bytes-value% %p2p-dwlnk-bytes-name% %p2p-dwlnk-bytes-value%”
```
**pcc-af schema**

Configures Policy and Charging Control-Application Function (PCC-AF) service bulk statistics schema.

**Product**
IPCF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Bulk Statistics Configuration

```
configure > bulkstats mode
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-bulkstats)#
```

**Syntax**

```
pcc-af schema schema_name format schema_format

no pcc-af schema schema_name
```

- **no**
  Removes the specified schema.

- **schema_name**
  Specifies the schema’s name.
  ```
  schema_name must be an alphanumeric string of 1 through 31 characters.
  ```

- **format schema_format**
  Specifies the schema’s format.
  ```
  schema_format must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of
  the command, including spaces”” characters. For more information, see the Schema Format String Length
  section.
  ```
  ```
  For information on the schema format’s syntax, see the Schema Format String Syntax section.
  ```

**Important:** For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

**Usage**

Use this command to define schemas for PCC-AF service bulk statistics collection. Multiple PCC-AF service schemas can be created to categorize PCC-AF service bulk statistics. All of the schemas are processed at each collection interval. To create multiple PCC-AF service schemas, re-issue the pcc-af schema schema_name command using a different schema name.

**Example**
The following command creates a schema named `pcc_aflstats1` that records the total number of Rx STR
messages received and total number of Rx AAR Accept messages sent along with Context name, Context Id,
and PCC-AF service name:

```
pcc-af schema pcc_aflstats1 format "%vpname%-%vpnid%-%servname%-%total-
rx-ccai-accept-sent%-%total-rx-aar-accept-sent%"
```
pcc-policy schema

Configures Policy and Charging Control-Policy (PCC-Policy) service bulk statistics schema.

Product
IPCF

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Bulk Statistics Configuration

configure > bulkstats mode

Entering the above command sequence results in the following prompt:

[local]host_name(config-bulkstats)#

Syntax

pcc-policy schema schema_name format schema_format

no pcc-policy schema schema_name

no

Removes the specified schema.

schema_name

Specifies the schema’s name.

schema_name must be an alphanumeric string of 1 through 31 characters.

format schema_format

Specifies the schema’s format.

schema_format must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of the command, including spaces”” characters. For more information, see the Schema Format String Length section. For information on the schema format’s syntax, see the Schema Format String Syntax section.

Important: For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

Usage

Use this command to define schemas for PCC-Policy service bulk statistics collection. Multiple PCC-Policy service schemas can be created to categorize PCC-Policy service bulk statistics. All of the schemas are processed at each collection interval. To create multiple PCC-Policy service schemas, re-issue the pcc-policy schema schema_name command using a different schema name.

Example
The following command creates a schema named `pcc_plcy1stats1` that records the total number of Gx messages sent and total number of Gx CCR messages received along with Context name, Context Id, and PCC-Policy service name:

```
  pcc-policy schema pcc_plcy1stats1 format "%vpnname%-%vpnid%-%servname%-
  %total-gx-outbound-msgs%-%total-gx-ccr-rcvd%"
```
**pcc-profile schema**

Configures Policy and Charging Control Profile (PCC-Profile) bulk statistics schema.

**Product**
IPCF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Bulk Statistics Configuration

```
configure > bulkstats mode
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-bulkstats)#
```

**Syntax**

```
pcc-profile schema schema_name format schema_format
no pcc-profile schema schema_name
```

- `no` - Removes the specified schema.
- `schema_name` - Specifies the schema’s name. `schema_name` must be an alphanumeric string of 1 through 31 characters.
- `format schema_format` - Specifies the schema’s format. `schema_format` must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of the command, including spaces”” characters. For more information, see the Schema Format String Length section.

For information on the schema format’s syntax, see the Schema Format String Syntax section.

**Important:** For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

**Usage**

Use this command to define schemas for PCC-Profile bulk statistics collection. Multiple PCC-Profile schemas can be created to categorize PCC-Profile bulk statistics. All of the schemas are processed at each collection interval. To create multiple PCC-Profile schemas, re-issue the `pcc-profile schema schema_name` command using a different schema name.

**Example**
The following command creates a schema named `pcc_profile1stats1` that records the total number of SGSN changes and QoS changes occurred for particular PCC profile along with Context name, Context Id, and PCC-Service name:

```
pcc-profile schema pcc_profile1stats1 format "%vpnname%-%vpnid%-%servname%-%total-sgsn-change%-%total-qos-change%"
```
pcc-sp-endpt schema

Configures the bulkstats schema at the Sp interface endpoint for PCC procedures with Subscriber Service Controller/Subscriber Policy Register (SSC/SPR).

Product

IPCF

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > Bulk Statistics Configuration

configure > bulkstats mode

Entering the above command sequence results in the following prompt:

[local]host_name(config-bulkstats)#

Syntax

```
pcc-sp-endpt schema schema_name format schema_format

no pcc-sp-endpt schema schema_name
```

no

Removes the specified schema.

```
schema_name
```

Specifies the schema’s name.

`schema_name` must be an alphanumeric string of 1 through 31 characters.

```
format schema_format
```

Specifies the schema’s format.

`schema_format` must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of the command, including spaces”” characters. For more information, see the Schema Format String Length section.

For information on the schema format’s syntax, see the Schema Format String Syntax section.

**Important:** For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

Usage

Use this command to define schemas for PCC-Sp-Endpoint bulk statistics collection. Multiple PCC-Sp-Endpoint schemas can be created to categorize PCC-Sp-Endpoint bulk statistics. All of the schemas are processed at each collection interval. To create multiple PCC-Sp-Endpoint schemas, re-issue the `pcc-sp-endpt schema schema_name` command using a different schema name.

Example
The following command creates a schema named `pcc_sp1stats1` that records the total number of SPRMgr Sh session close and open requests received from PCCMgr and processed by PCC-Sp-Endpoint along with Context name, Context Id, and PCC-Sp-Endpoint name:

```
pcc-sp-endpt schema pcc_svc1stats1 format "%vpnname%-%vpnid-%endpt-name%-%req-open%-%req-close%"
```
pcc-service schema

Configures Policy and Charging Control-Service (PCC-Service) bulk statistics schema.

Product
IPCF

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Bulk Statistics Configuration
configure > bulkstats mode

Entering the above command sequence results in the following prompt:

[local]host_name(config-bulkstats)#

Syntax

pcc-service schema schema_name format schema_format

no pcc-service schema schema_name

no
Removes the specified schema.

schema_name
Specifies the schema’s name.

schema_name must be an alphanumeric string of 1 through 31 characters.

format schema_format
Specifies the schema’s format.

schema_format must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of the command, including spaces”” characters. For more information, see the Schema Format String Length section.

For information on the schema format’s syntax, see the Schema Format String Syntax section.

Important: For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

Usage
Use this command to define schemas for PCC-Service bulk statistics collection. Multiple PCC-Service schemas can be created to categorize PCC-Service bulk statistics. All of the schemas are processed at each collection interval. To create multiple PCC-Service schemas, re-issue the pcc-service schema schema_name command using a different schema name.

Example
The following command creates a schema named pcc_svc1stats1 that records the total number of Gx and Gy request processed by PCC-Service along with Context name, Context Id, and PCC-Service name:
pcc-service schema pcc_svc1st_format "%vpnname%-%vpnid%-%servname%-%total-gx-processed%-%total-gy-processed%"
pdif schema

Configures Packet Data Interworking Function (PDIF) bulk statistics schema.

**Product**
PDIF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Bulk Statistics Configuration

```
configure > bulkstats mode
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-bulkstats)#
```

**Syntax**

```
pdif schema schema_name format schema_format
no pdif schema schema_name
```

- **no**
  Removes the specified schema.

- **schema_name**
  Specifies the schema’s name.
  `schema_name` must be an alphanumeric string of 1 through 31 characters.

- **format schema_format**
  Specifies the schema’s format.
  `schema_format` must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of the command, including spaces”” characters. For more information, see the Schema Format String Length section.
  For information on the schema format’s syntax, see the Schema Format String Syntax section.

**Important:** For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

**Usage**

Use this command to define schemas for PDIF bulk statistics collection. Multiple PDIF schemas can be created to categorize PDIF bulk statistics. All of the schemas are processed at each collection interval. To create multiple schemas, re-issue the `pdif schema schema_name` command using a different schema name.

**Example**

The following command creates a schema named `pdifschemal` for the category current active ipv4 sessions:
pdif schema pdifschemal format %sess-curactip4%
pgw schema

Configures Packet Data Network Gateway (P-GW) bulk statistics schema.

Product

P-GW
SAEGW

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > Bulk Statistics Configuration
configure > bulkstats mode

Entering the above command sequence results in the following prompt:

[local]host_name(config-bulkstats)#

Syntax

pgw schema schema_name format schema_format

no pgw schema schema_name

---

no

Removes the specified schema.

---

schema_name

Specifies the schema’s name.
schema_name must be an alphanumeric string of 1 through 31 characters.

---

format schema_format

Specifies the schema’s format.
schema_format must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of the command, including spaces”” characters. For more information, see the Schema Format String Length section.
For information on the schema format’s syntax, see the Schema Format String Syntax section.

---

Important: For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

---

Usage

Use this command to define schemas for P-GW bulk statistics collection in the generated stats report files. Usually a schema consists of multiple variables to collect all the statistics for a particular situation. Using double quote marks and text within this command, the reported statistics can be easily identified. Multiple P-GW schemas can be created to categorize P-GW bulk statistics. All of the schemas are processed at each collection interval. To create multiple P-GW schemas, re-issue the pgw schema schema_name command using a different schema name each time.
port schema

Configures port bulk statistics schema.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Bulk Statistics Configuration
configure > bulkstats mode

Entering the above command sequence results in the following prompt:

[local]host_name(config-bulkstats)#

Syntax

```
port schema schema_name format schema_format
no port schema schema_name
```

no

Removes the specified schema.

```
schema_name
```

Specifies the schema’s name.

```
schema_name
```

must be an alphanumeric string of 1 through 31 characters.

```
format schema_format
```

Specifies the schema’s format.

```
schema_format
```

must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of the command, including spaces”” characters. For more information, see the Schema Format String Length section.

For information on the schema format’s syntax, see the Schema Format String Syntax section.

**Important:** For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

Usage

Use this command to define schemas for port bulk statistics collection. Multiple port schemas can be created to categorize port-level bulk statistics. All of the schemas are processed at each collection interval. To create multiple port schemas, re-issue the `port schema schema_name` command using a different schema name.

**Important:** The `card` variable in the Port schema is not supported on all platforms.
Example

To create a port-level schema named `portstats1` that separates the `card/port`, `bcast_inpackets`, and `bcast_outpackets` variables by hyphens (“-”), enter the following command:

```plaintext
port schema portstats1 format "%card%/%port% - %bcast_inpackets% - %bcast_outpackets%"
```
ppp schema

Configures Point-to-Point Protocol (PPP) bulk statistics schema.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Bulk Statistics Configuration
configure > bulkstats mode

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-bulkstats)#
```

**Syntax**

```
ppp schema schema_name format schema_format

no ppp schema schema_name
```

- **no**
  Removes the specified schema.

- **schema_name**
  Specifies the schema’s name.
  `schema_name` must be an alphanumeric string of 1 through 31 characters.

- **format schema_format**
  Specifies the schema’s format.
  `schema_format` must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of the command, including spaces”” characters. For more information, see the Schema Format String Length section.
  For information on the schema format’s syntax, see the Schema Format String Syntax section.

**Important:** For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

**Usage**

Use this command to define schemas for point-to-point protocol bulk statistics collection. Multiple PPP-service schemas can be created to categorize PPP-service bulk statistics. All of the schemas are processed at each collection interval. To create multiple PPP-service schemas, re-issue the `ppp schema schema_name` command using a different schema name.

**Example**

To create a ppp-level schema named `pppstats` that specifies a schema format of:
- CHAP: (Challenge Handshake Authentication Protocol)
- Auth. Attempts: auth-attempt-chap
- Successes: auth-success-chap

- PAP: (Password Authentication Protocol)

- Auth. Attempts: auth-attempt-pap
- Successes: auth-success-pap

Use the following command:

```plaintext
ppp schema pppstats format "CHAP:
Auth. Attempts: %auth-attempt-chap
Successes: %auth-success-chap
PAP:
Auth. Attempts: %auth-attempt-pap
Successes: %auth-success-pap"
```
ps-network-gtpu schema

Configures the GTP-U bulk statistics schema in a Packet Switched (PS) network associated with an HNB-GW node.

Product
HNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Bulk Statistics Configuration
configure > bulkstats mode

Entering the above command sequence results in the following prompt:

[local]host_name(config-bulkstats)\

Syntax

ps-network-gtpu schema  schema_name format  schema_format

no ps-network-gtpu schema  schema_name

no

Removes the specified schema.

schema_name
Specifies the schema’s name.
schema_name must be an alphanumeric string of 1 through 31 characters.

format  schema_format
Specifies the schema’s format.
schema_format must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of the command, including spaces”” characters. For more information, see the Schema Format String Length section.
For information on the schema format’s syntax, see the Schema Format String Syntax section.

Important: For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

Usage

Use this command to define schemas for GTP-U connection related bulk statistics collection in a PS network associated with HNB-GW in a Femto UMTS network. Multiple PS Networks GTP-U schemas can be created to further categorize at PS network or HNB-GW-level bulk statistics. All of the schemas are processed at each collection interval. To create multiple PS Networks GTPU schemas, re-issue the ps-network-gtpu schema  schema_name command using a different schema name.

Example
The following command creates a schema named `ps_gtpulstats1` that records the total number of GTP-U packets received by HNB-GW from CN and sent to CN node in an associated PS network:

```plaintext
ps-network-gtpu schema ps_gtpulstats1 format "%gtpu-pkt-rx%" "%gtpu-pkt-tx%"
```
ps-network-ranap schema


Product
HNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Bulk Statistics Configuration
configure > bulkstats mode

Entering the above command sequence results in the following prompt:

[local]host_name(config-bulkstats)#

Syntax

```
ps-network-ranap schema schema_name format schema_format

no ps-network-ranap schema schema_name
```

no

Removes the specified schema.

```
schema_name
```

Specifies the schema’s name.

`schema_name` must be an alphanumeric string of 1 through 31 characters.

```
format schema_format
```

Specifies the schema’s format.

`schema_format` must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of the command, including spaces”” characters. For more information, see the Schema Format String Length section.

For information on the schema format’s syntax, see the Schema Format String Syntax section.

**Important:** For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

Usage

Use this command to define schemas for RANAP procedure related bulk statistics collection in a PS network associated with HNB-GW in a Femto UMTS network. Multiple PS Networks RANAP schemas can be created to further categorize at PS network or HNB-GW-level bulk statistics. All of the schemas are processed at each collection interval. To create multiple PS Networks RANAP schemas, re-issue the `ps-network-ranap schema schema_name` command using a different schema name.

Example
The following command creates a schema named `ps_ranap1stats1` that records the total number of Iu Release Request messages transmitted and total number of Iu Release Command message received by HNB-GW node:

```
ps-network-ranap schema ps_ranap1stats1 format "%iu-rel-req-tx%" "%iu-rel-cmd-rx%"
```
ps-network-sccp schema

Configures the Signalling Connection Control Part (SCCP) bulk statistics schema in a Packet Switched (PS) network associated with an HNB-GW node.

**Product**
HNB-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Bulk Statistics Configuration

```
configure > bulkstats mode
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-bulkstats)#
```

**Syntax**

```
ps-network-sccp schema schema_name format schema_format

no ps-network-sccp schema schema_name
```

- **no**
  Removes the specified schema.

- **schema_name**
  Specifies the schema’s name.
  `schema_name` must be an alphanumeric string of 1 through 31 characters.

- **format schema_format**
  Specifies the schema’s format.
  `schema_format` must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of the command, including spaces”” characters. For more information, see the Schema Format String Length section.

  For information on the schema format’s syntax, see the Schema Format String Syntax section.

**Important:** For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

**Usage**

Use this command to define schemas for SCCP connection related bulk statistics collection in a PS network associated with HNB-GW in a Femto UMTS network. Multiple PS Networks SCCP schemas can be created to further categorize at PS network or HNB-GW-level bulk statistics. All of the schemas are processed at each collection interval. To create multiple PS Networks SCCP schemas, re-issue the `ps-network-sccp schema schema_name` command using a different schema name.

**Example**

```
The following command creates a schema named `ps_sccplstats1` that records the total number of SCCP connection requests received by HNB-GW and responses sent to CN node in an associated PS network:

```
ps-network-sccp schema ps_sccplstats1 format "%sccp-conn-req-rx%" "%sccp-conn-req-tx%"
```
radius schema

Configures RADIUS bulk statistics schema.

**Product**
PDSN
GGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Bulk Statistics Configuration

configure > bulkstats mode

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-bulkstats)#
```

**Syntax**

```
radius schema schema_name format schema_format
```

```
no radius schema schema_name
```

**no**
Removes the specified schema.

```
schema_name
```
Specifies the schema’s name.

```
schema_name
```
must be an alphanumeric string of 1 through 31 characters that is case sensitive.

```
format schema_format
```
Specifies the schema’s format.

```
schema_format
```
must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of the command, including spaces’”’ characters. For more information, see the Schema Format String Length section.

For information on the schema format’s syntax, see the Schema Format String Syntax section.

**Important:** For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

**Usage**
Use this command to define schemas for RADIUS bulk statistics collection. Multiple RADIUS schemas can be created to categorize RADIUS bulk statistics. All of the schemas are processed at each collection interval. To create multiple RADIUS schemas, re-issue the `radius schema schema_name` command using a different schema name.

**Example**
To create a RADIUS schema named `radius_statistics` that specifies a schema format of:
• Server: ipaddr
• Authentication Requests Sent: auth-req-sent
• Accounting Requests Sent: acc-req-sent

Use the following command:

```
radius schema radius_statistics format "Server: %ipaddr%
Authentication Requests Sent: %auth-req-sent%
Accounting Requests Sent: %acc-req-sent%"
```
radius-group schema

Configures RADIUS group bulk statistics schema.

Product
PDSN
GGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Bulk Statistics Configuration
configure > bulkstats mode

Entering the above command sequence results in the following prompt:

[local]host_name(config-bulkstats)#

Syntax

radius-group schema schema_name format schema_format

no radius-group schema schema_name

- no
  Removes the specified schema.

  schema_name
  Specifies the schema’s name.
  schema_name must be an alphanumeric string of 1 through 31 characters that is case sensitive.

  format schema_format
  Specifies the schema’s format.
  schema_format must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of the command, including spaces’”’ characters. For more information, see the Schema Format String Length section.
  For information on the schema format’s syntax, see the Schema Format String Syntax section.

Important: For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

Usage

Use this command to define schemas for RADIUS group bulk statistics collection. Multiple RADIUS group schemas can be created to categorize RADIUS group bulk statistics. All of the schemas are processed at each collection interval. To create multiple RADIUS group schemas, re-issue the radius-group schema schema_name command using a different schema name.

Example

To create a RADIUS group schema named radius_statistics that specifies a schema format of:
• Server: ipaddr
• Authentication Requests Sent: auth-req-sent
• Accounting Requests Sent: acc-req-sent

Use the following command:

```
radius-group schema radius_statistics format "Server: %ipaddr%\nAuthentication Requests Sent: %auth-req-sent%\nAccounting Requests Sent: %acc-req-sent%"
```
receiver

Configures a host system to receive bulkstats information through Trivial File Transfer Protocol (TFTP), File Transfer Protocol (FTP) or SSH File Transfer Protocol (SFTP).

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Bulk Statistics Configuration
call
configure > bulkstats mode

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-bulkstats)#
```

**Syntax**

```
receiver { mode { redundant | secondary-on-failure } | ip_address { primary | secondary } [ mechanism { { { ftp | sftp } login user_name [ encrypted ] password pwd } | tftp } } ]
```

```
no receiver ip_address
```

**no**
Removes the receiver specified from the list of receivers where data files are sent.

**mode { redundant | secondary-on-failure }**
Determines how bulkstats are delivered to the primary and secondary receivers.
Default: secondary-on-failure

- **redundant**: Files are transferred to both the primary and secondary receivers. If either transfer is not currently possible, the file is transferred when possible. The system continues to hold in memory as much data as possible until the data has been successfully transferred to both receivers. Data is only discarded if the in-memory data reaches the configured limit. Refer to the `limit` command.
- **secondary-on-failure**: Files are transferred to the secondary receiver if the primary receiver fails. In-memory data is erased once the data is transferred to either the primary or secondary receiver. This is the default behavior.

**ip_address**
Specifies the IP address of the receiver of interest using IPv4 dotted-decimal notation.

**primary | secondary**
Primary and secondary are used to indicate the order in which receivers are connected. The secondary is used when the primary is unreachable.

- **primary**: indicates the receiver is the primary receiver of data.
- **secondary**: indicates the receiver is the secondary receiver of data.
mechanism { ( { ftp | sftp } login user_name [ encrypted ] password pwd ) | tftp }

Specifies the method by which data is transferred to the receiver.

**ftp login user_name [ encrypted ] password pwd:** the FTP protocol shall be used for data file transfer. *user_name* specifies the user to provide for remote system secure logins and must be an alphanumeric string of 1 through 31 characters. The password to use for remote system authentication is specified as *pwd* and must be from 1 to 31 characters or 1 to 64 characters if the *encrypted* keyword is also specified.

**sftp login user_name [ encrypted ] password pwd:** the SFTP protocol shall be used for data file transfer. *user_name* specifies the user to provide for remote system secure logins and must be an alphanumeric string of 1 through 31 characters. The password to use for remote system authentication is specified as *pwd* and must be from 1 to 31 characters or 1 to 64 characters if the *encrypted* keyword is also specified.

**tftp:** the TFTP protocol is to be used to transfer files.

The *encrypted* keyword is intended only for use by the system while saving configuration scripts. The system displays the *encrypted* keyword in the configuration file as a flag that the variable following the *password* keyword is the encrypted version of the plain text password. Only the encrypted password is saved as part of the configuration file.

### Usage

Use TFTP methods to reduce transfer times if excessive system resources are being used across the network for transfer of data.

FTP transfer method allows for login which then provides system logging within the enabled FTP logs. The initial connection is attempted to the primary receiver. If the primary receiver is unreachable for any reason, the secondary receiver is used. If the secondary receiver is also unreachable, the system retries after a delay period where it again attempts to connect to the primary receiver followed by the secondary receiver as necessary.

**Important:** For redundant receivers, configuration changes to the receivers are applied to all existing and all subsequent data sets pending transfer. If no receiver is configured, bulk statistics will be collected and stored on the system until the maximum amount of memory is used; they will not be transferred to the receiver(s). When the storage limit has been reached the oldest information is overwritten. When a receiver is configured for the primary and secondary target, this command will use both receivers as default if no receiver is specified.

### Example

```
receiver 10.2.3.4 primary mechanism tftp
receiver 10.2.3.5 secondary
no receiver 10.2.3.4
```
remotefile

Configures the naming convention with support for multiple file format to multiple receivers when storing the data files on the remote receiver(s).

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Bulk Statistics Configuration

configure > bulkstats mode

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-bulkstats)#
```

**Syntax**

```
remotefile format schema_format [ both-receivers | primary-receiver | secondary-receiver ]
```

```no remotefile format```

**no**

Resets the remote file naming convention to the system default.

```format schema_format```

Specifies the naming convention format to use.

`schema_format` must be an alphanumeric string of 1 through 127 characters. The format string syntax is described in the [Schema Format String Syntax](#) section. Default: “%date%-%time%”

**Important:** The remote file naming format should only use static text and bulk statistic variables to avoid any possible file creation issues on the receivers.

The following variables are supported:

**Table 19. remote file Command Naming Format Variables**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
<th>Data Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>date</td>
<td>The UTC date that the collection file was created in YYYYMMDD format where YYYY represents the year, MM represents the month and DD represents the day.</td>
<td>String</td>
</tr>
<tr>
<td>date3</td>
<td>The UTC date that the collection file was created in YYMMDD format where YY represents the year, MM represents the month and DD represents the day.</td>
<td>String</td>
</tr>
<tr>
<td>host</td>
<td>The system hostname that created the file</td>
<td>String</td>
</tr>
</tbody>
</table>
### Variable Description

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
<th>Data Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>sysuptime</td>
<td>The uptime (in seconds) of the system that created the file.</td>
<td>32-bit signed</td>
</tr>
<tr>
<td>time</td>
<td>The time that the collection file was created in HHMMSS format where HH represents the hours, MM represents the minutes, and SS represents the seconds.</td>
<td>String</td>
</tr>
</tbody>
</table>

---

`both-receivers | primary-receiver | secondary-receiver`

Sets the remote file creation target to both receivers, primary receiver or secondary receiver. Default: Both receivers.

#### Usage

Set the remote file naming format to ensure consistent data file naming across a network or adjusting a single system’s format for easy identification.

This command specifies whether the format should be used in conjunction with both receivers, only the primary receiver, or only the secondary receiver.

---

**Important:** For redundant receivers, the filenames for the output data files are applied when the information is first gathered. If the name format is modified, the change takes effect for the next data set. The current data set name remains unchanged. even if has not yet been transferred.

#### Example

```
remotefile format simpleFormat
remotefile format "\%host\%-\%date\%-\%time\%"
remotefile format "\%host\%-\%date\%-\%time\%" both-receivers
remotefile format "\%host\%-\%date\%" primary-receiver
no remotefile format
```
**rlf schema**

Configures the aggregated information for Rate Limiting Function (RLF) context statistics schema.

**Product**
GGSN
P-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Bulk Statistics Configuration
configure > bulkstats mode

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-bulkstats)#
```

**Syntax**

```
rlf schema schema_name format schema_format
no rlf schema schema_name
```

- **no**
  Removes the specified schema.

- **schema_name**
  Specifies the schema’s name.
  *schema_name* must be an alphanumeric string of 1 through 31 characters.

- **format**
  Specifies the schema’s format.
  *schema_format* must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of the command, including spaces’” characters. For more information, see the Schema Format String Length section.
  For information on the schema format’s syntax, see the Schema Format String Syntax section.

**Important:** For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

**Usage**

Use this command to define schemas for RLF bulk statistics collection. Multiple RLF schemas can be created to categorize RLF bulk statistics. All of the schemas are processed at each collection interval. To create multiple RLF schemas, re-issue the rlf schema schema_name command using a different schema name.

**Example**

To create an RLF-level schema named *rlfstats* that specifies a schema format of:

- Date: *date*
Bulk Statistics Configuration Mode Commands

- Time: time
- Number of Authentication Denials: deny-auth

Use the following command:

```bash
rlf schema rlfstats format "Date: %date%nTime: %time%nNumber of Authentication Denials: %deny-auth%n"
```
**rlf-detailed schema**

Configures the detailed instance level information for RLF context statistics schema.

**Product**
GGSN
P-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Bulk Statistics Configuration
configure > bulkstats mode

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-bulkstats)#
```

**Syntax**

```
rlf-detailed schema schema_name format schema_format
no rlf-detailed schema schema_name
```

**no**
Removes the specified schema.

```
schema_name
```
Specifies the schema’s name.
```
schema_name must be an alphanumeric string of 1 through 31 characters.
```

```
format schema_format
```
Specifies the schema’s format.
```
schema_format must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of the command, including spaces’”” characters. For more information, see the Schema Format String Length section.
```
For information on the schema format’s syntax, see the Schema Format String Syntax section.

**Important:** For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

**Usage**
Use this command to define schemas for detailed RLF bulk statistics collection. Multiple rlf-detailed schemas can be created to categorize RLF detailed bulk statistics. All of the schemas are processed at each collection interval. To create multiple rlf-detailed schemas, re-issue the `rlf-detailed schema schema_name` command using a different schema name.

**Example**
To create an rlf-detailed level schema named `rlfdetailedstats` that specifies a schema format of:
• Date: \textit{date}
• Time: \textit{time}
• Number of Authentication Denials: \textit{deny-auth}

Use the following command:

\begin{verbatim}
rlf-detailed schema rlfstats format "Date: %date%\nTime: %time%\nNumber of Authentication Denials: %deny-auth%"
\end{verbatim}
rp schema

Configures R-P bulk statistics schema.

Product
PDSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Bulk Statistics Configuration
configure > bulkstats mode

Entering the above command sequence results in the following prompt:

[local]host_name(config-bulkstats)#

Syntax

rp schema schema_name format schema_format

no rp schema schema_name

no

Removes the specified schema.

schema_name

Specifies the schema’s name.

schema_name must be an alphanumeric string of 1 through 31 characters.

format schema_format

Specifies the schema’s format.

schema_format must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of the command, including spaces”” characters. For more information, see the Schema Format String Length section.

For information on the schema format’s syntax, see the Schema Format String Syntax section.

Important: For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

Usage

Use this command to define schemas for R-P bulk statistics collection. Multiple PDSN service schemas can be created to categorize PDSN service bulk statistics. All of the schemas are processed at each collection interval. To create multiple PDSN service schemas, re-issue the rp schema schema_name command using a different schema name.

Example

To create an PDSN-level schema named pdnservicestats that specifies a schema format of:

• Date: date
- Time: time
- Number of Authentication Denials: deny-auth

Use the following command:

```
rp schema rpservicestats format "Date: %date\nTime: %time\nNumber of Authentication Denials: %deny-auth\n"
```
**saegw schema**

Configures System Architecture Evolution Gateway (SAEGW) bulk statistics schema.

**Product**
SAEGW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Bulk Statistics Configuration
configure > bulkstats mode

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-bulkstats)#
```

**Syntax**

```
saegw schema schema_name format schema_format
no saegw schema schema_name
```

- **schema_name**
  Specifies the schema’s name.
  *schema_name* must be an alphanumeric string of 1 through 31 characters.

- **format schema_format**
  Specifies the schema’s format.
  *schema_format* must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of the command, including spaces”” characters. For more information, see the **Schema Format String Length** section.
  For information on the schema format’s syntax, see the **Schema Format String Syntax** section.

**Important:** For a complete list of the statistics that are supported for this schema, refer to the **Statistics and Counters Reference**.

**Usage**

Use this command to define schemas for SAEGW bulk statistics collection in the generated stats report files. Usually a schema consists of multiple variables to collect all the statistics for a particular situation. Using double quote marks and text within this command, the reported statistics can be easily identified.

Multiple SAEGW schemas can be created to categorize SAEGW bulk statistics. All of the schemas are processed at each collection interval. To create multiple SAEGW schemas, re-issue the **saegw schema** command using a different schema name each time.
sample-interval

Configures the time interval between collecting local statistics.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Bulk Statistics Configuration

```bash
configure > bulkstats mode
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-bulkstats)#
```

**Syntax**

```bash
sample-interval minutes
```

*minutes*

Specifies the frequency (in minutes) of polling for local statistics as an integer from 1 through 1440.

**Usage**

Adjust the sampling interval to tune the system response as shorter periods can cause undue system overhead whereas longer periods have less of a statistical importance when analyzing data.

The system is shipped from the factory with the sampling interval set to 15 minutes.

**Example**

```bash
sample-interval 120
```
sccp schema

Configures the collection of statistics for the SCCP schema.

**Product**

SGSN
HNB-GW

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Bulk Statistics Configuration
configure > bulkstats mode

Entering the above command sequence results in the following prompt:

[local]host_name(config-bulkstats)#

**Syntax**

```
sccp schema schema_name format schema_format
```

```
no sccp schema schema_name
```

**no**

Removes the specified schema.

```
schema_name
```

Specifies the schema’s name.

*schema_name* must be an alphanumeric string of 1 through 31 characters.

```
format schema_format
```

Specifies the schema’s format.

*schema_format* must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of the command, including spaces’” characters. For more information, see the Schema Format String Length section.

For information on the schema format’s syntax, see the Schema Format String Syntax section.

**Important:** For a complete list of the statistics that are supported for the SCCP schema, refer to the Statistics and Counters Reference.

**Usage**

Use this command to define schemas for SCCP bulk statistics collection in the generated stats report files.

Usually a schema consists of multiple variables to collect all the statistics for a particular situation. Using double quote marks and text within this command, the reported statistics can be easily identified.

Multiple SCCP schemas can be created to categorize SCCP bulk statistics. All of the schemas are processed at each collection interval. To create multiple SCCP schemas, re-issue the *sccp schema schema_name* command using a different schema name each time.
Example

Include the bulk statistic variable names to create an SCCP schema named `sccpstats11` that specifies collection of statistics (a schema format) for:

- Subsystem available messages sent from the SCCP
- Subsystem available messages received by the SCCP

Use the following command:

```
sccp schema sccpstats11 format "Subsys avail SCCP Tx: %ssa-txed\nSubsys avail SCCP Rx: %ssa-rcvd\n"
```
schema

Configures the system-level bulk statistics schema.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Bulk Statistics Configuration
configure > bulkstats mode

Entering the above command sequence results in the following prompt:

[local]host_name(config-bulkstats)#

Syntax

schema schema_name format schema_format

no schema schema_name

---

no

Removes the specified schema.

---

schema_name

Specifies the schema’s name.
schema_name must be an alphanumeric string of 1 through 31 characters.

---

format schema_format

Specifies the schema’s format.
schema_format must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of the command, including spaces”” characters. For more information, see the Schema Format String Length section.
For information on the schema format’s syntax, see the Schema Format String Syntax section.

---

Important: For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

Usage

Use this command to define schemas for system-level bulk statistics collection. Multiple schemas can be created to categorize system-level bulk statistics. All of the schemas are processed at each collection interval. To create multiple system schemas, re-issue the schema schema_name command using a different schema name.

Example

The following command creates a schema named systemstats1 that records the number of current Simple IP and the number of current Mobile IP sessions:
To create a system-level schema named `bulksysstats` that specifies a schema format of:

- Number of currently active sessions: `sess-curactcall`
- Number of currently dormant sessions: `sess-curdormcall`

Use the following command:

```
schema bulksysstats format "Number of currently active sessions: %sess-curactcall\nNumber of currently dormant sessions: %sess-curdormcall\n"
```
**sgs schema**

Configures the collection of statistics for the SGs schema.

**Product**

MME

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Bulk Statistics Configuration

```
configure > bulkstats mode
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-bulkstats)#
```

**Syntax**

```
sgs schema schema_name format schema_format
```

```
no sgs schema schema_name
```

- **no**
  - Removes the specified SGs schema from statistics collection.

- **schema_name**
  - Specifies the schema’s name.
  - `schema_name` must be an alphanumeric string of 1 through 31 characters.

- **format schema_format**
  - Specifies the schema’s format.
  - `schema_format` must be an alphanumeric string of `1021 minus “number of characters in rest of the command, including spaces” characters`. For more information, see the [Schema Format String Length](#) section.
  - For information on the schema format’s syntax, see the [Schema Format String Syntax](#) section.

**Important:** For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

**Usage**

Use this command to define schemas for SGs bulk statistics collection in the generated stats report files. Usually a schema consists of multiple variables to collect all the statistics for a particular situation. Using double quote marks and text within this command, the reported statistics can be easily identified.

Multiple SGs schemas can be created to categorize SGs bulk statistics. All of the schemas are processed at each collection interval. To create multiple SGs schemas, re-issue the `sgs schema schema_name` command using a different schema name each time.

**Example**

...
Include the bulk statistic variable names to create an SGs schema named `stats_SGs_release` that specifies a collection of statistics (a schema format) for the total number of release messages transmitted, retransmitted, and received:

Use the following command:

```bash
sgs schema stats_SGs_release format "Total transmitted: %rel-req-tx\nTotal retransmitted: %rel-req-retx\nTotal received: %rel-req-rx\n"
```
**sgs-vlr schema**

Configures the collection of statistics for the SGs-VLR schema.

**Product**
MME

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Bulk Statistics Configuration

**configure > bulkstats mode**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-bulkstats)#
```

**Syntax**

```
sgs-vlr schema  schema_name  format  schema_format
```

```
no  sgs  schema  schema_name
```

- **schema_name**
  Specifies the schema’s name.
  - *schema_name* must be an alphanumeric string of 1 through 31 characters.

- **format  schema_format**
  Specifies the schema’s format.
  - *schema_format* must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of the command, including spaces”” characters. For more information, see the Schema Format String Length section.
  - For information on the schema format’s syntax, see the Schema Format String Syntax section.

**Important:** For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

**Usage**

Use this command to define schemas for SGs-VLR bulk statistics collection in the generated stats report files. Usually a schema consists of multiple variables to collect all the statistics for a particular situation. Using double quote marks and text within this command, the reported statistics can be easily identified.

Multiple SGs-VLR schemas can be created to categorize SGs-VLR bulk statistics. All of the schemas are processed at each collection interval. To create multiple SGs-VLR schemas, re-issue the *sgs-vlr schema schema_name* command using a different schema name each time.

**Example**
Include the bulk statistic variable names to create an SGs-VLR schema named `stats_SGsVLR_release` that specifies a collection of statistics (a schema format) for the total number of release messages transmitted, retransmitted, and received:

Use the following command:

```
sgs-vlr schema stats_SGsVLR_release format "Total Paging requests transmitted: %pag-req-tx\nTotal Paging requests retransmitted: %pag-req-retx\nTotal Paging requests received: %pag-req-rx\n"
```
sgsn schema

Configures the collection of statistics for the SGSN schema.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Bulk Statistics Configuration
configure > bulkstats mode
Entering the above command sequence results in the following prompt:

[local]host_name(config-bulkstats)#

Syntax

sgsn schema schema_name format schema_format

no sgsn schema schema_name

no
Removes the specified SGSN schema from statistics collection.

schema_name
Specifies the schema’s name.
schema_name must be an alphanumeric string of 1 through 31 characters.

format schema_format
Specifies the schema’s format.
schema_format must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of the command, including spaces”” characters. For more information, see the Schema Format String Length section.
For information on the schema format’s syntax, see the Schema Format String Syntax section.

Important: For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

Usage
Use this command to define schemas for SGSN bulk statistics collection in the generated stats report files. Usually a schema consists of multiple variables to collect all the statistics for a particular situation. Using double quote marks and text within this command, the reported statistics can be easily identified.
Multiple SGSN schemas can be created to categorize SGSN bulk statistics. All of the schemas are processed at each collection interval. To create multiple SGSN schemas, re-issue the sgsn schema schema_name command using a different schema name each time.

Example
Include the bulk statistic variable names to create an SGSN schema named `stats_3Gsgsn1` that specifies collection of statistics (a schema format) for the total number of 3G Attaches per LAC/RAC per MCC&MNC:

Use the following command:

```
sgsn schema stats_3Gsgsn1 format "MCC: %mcc%
MNC: %mnc%
LAC: %lac%
RAC: %rac%
Total 3G Subs Attached: %3G-attached%
"
```
**sgtp schema**

Configures the collection of the SGSN’s GTP-C and GTP-U activity statistics.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Bulk Statistics Configuration
configure > bulkstats mode

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-bulkstats)#
```

**Syntax**

```
sgtp schema schema_name format schema_format

no sgtp schema schema_name
```

**Syntax**

```
no
```

Removes the specified SGTP schema from statistics collection.

```
schema_name
```

Specifies the schema’s name.

**Important:**
For a complete list of the statistics that are supported for this schema, refer to the *Statistics and Counters Reference*.

```
schema_format
```

Specifies the schema’s format.

**Usage**

Use this command to define schemas for SGTP bulk statistics collection in the generated stats report files.

Usually a schema consists of multiple variables to collect all the statistics for a particular situation. Using double quote marks and text within this command, the reported statistics can be easily identified.

Multiple SGTP schemas can be created to categorize SGTP bulk statistics. All of the schemas are processed at each collection interval. To create multiple SGTP schemas, re-issue the `sgtp schema schema_name` command using a different schema name each time.

**Example**
Include the bulk statistic variable names to create an SGTP schema named `$sgtpstats_sgsn1` that specifies collection of statistics (a schema format) will be by IuPS service interface and by RNC for the total number of GTP-C Create PDP Context Request messages received.

Use the following command:

```bash
sgtp schema $sgtpstats_sgsn1 format "IuPS Service ID: %iups-service%nRNC: %rnc-address%nTotal CPCR Rx: %sgtpc-total-cpc-req%n"
```
sgw schema

Configures the collection of the S-GW activity statistics.

Product
S-GW
SAEGW

Privilege
Administrator

Mode
Exec > Global Configuration > Bulk Statistics Configuration
configure > bulkstats mode

Entering the above command sequence results in the following prompt:
[local]host_name(config-bulkstats)#

Syntax

sgw schema schema_name format schema_format

no sgw schema schema_name

---

no

Removes the specified S-GW schema from statistics collection.

---

schema_name

Specifies the schema’s name.
schema_name must be an alphanumeric string of 1 through 31 characters.

---

format schema_format

Specifies the schema’s format.
schema_format must be an alphanumeric string of 1 through 1021 characters minus the number of characters in rest of the command, including spaces and double quotes (" ") characters. For more information, see the Schema Format String Length section.
For information on the schema format’s syntax, see the Schema Format String Syntax section.

---

Important: For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

Usage

Use this command to define schemas for S-GW bulk statistics collection in the generated stats report files. Usually a schema consists of multiple variables to collect all the statistics for a particular situation. Using double quote marks and text within this command, the reported statistics can be easily identified. Multiple S-GW schemas can be created to categorize S-GW bulk statistics. All of the schemas are processed at each collection interval. To create multiple S-GW schemas, re-issue the sgw schema schema_name command using a different schema name each time.
Example

Include the bulk statistic variable names to create an S-GW schema named `sgwstats_sgw1` that specifies collection of statistics (a schema format) will be by S-GW service interface for the total number of currently idle and active UEs.

Use the following command:

```bash
sgw schema sgwstats_sgw1 format "SGW Service ID: %servname%\nTotal Current Idle UEs: %sessstat-totcur-ueidle%\nTotal Current Active UEs: %sessstat-totcur-ueactive%"
```
show variables

Displays the bulk statistics variable information based on schema names.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Bulk Statistics Configuration
configure > bulkstats mode

Entering the above command sequence results in the following prompt:

[local]host_name(config-bulkstats)#

Syntax

show variables [ schema_name ] [ obsolete ]

show variables schema_name

Displays all valid bulkstat schema statistics, or only the statistics for the specified schema.

schema_name specifies the name of the schemas available on the system. Following is the list of available schemas in this release.

- aal2
- alcap
- apn
- asngw
- asnpc
- bcmcs
- card
- closedrp
- common
- context
- cs-network-ranap
- cs-network-rtp
- cscf
- cscfintf
- dcca
- dcca-group
- diameter-acct
• diameter-auth
• dlci-util
• dpcap
• ecs
• egtpc
• epdg
• fa
• fng
• gprs
• gtpc
• gtpp
• gtpu
• ha
• hnbw-hnbap
• hnbw-ranap
• hnbw-rtp
• hnbw-rua
• hnbw-sctp
• hsgw
• imsa
• ippool
• ipsg
• lac
• lma
• lns
• mag
• map
• mipv6ha
• mme
• mvs
• nat-realm
• p2p
• pcc-af
• pcc-policy
Bulk Statistics Configuration Mode Commands

show variables

- pcc-service
- pcc-sp-endpt
- pdg
- pdif
- pgw
- phsgw
- phspc
- port
- ppp
- ps-network-ranap
- radius
- radius-group
- rlf
- rlf-detailed
- rp
- saegw
- sccp
- sgs
- sgsn
- sgtp
- sgw
- ss7link
- ss7rd
- system
- vpn

obsolete
Displays obsolete (but still available) schema variables. An asterisk (*) is displayed next to schema variables that have been obsoleted.

Usage
Use this command to list supported bulk statistic variables. Variables can be listed for a specified schema. If no schema is specified, all supported variables are listed on a per-schema basis.

Example
The following command displays the bulkstat variables only for the card schema:

```
show variables card
```
ss7link schema

Configures the collection of the SS7 link activity statistics.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Bulk Statistics Configuration

`configure > bulkstats mode`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-bulkstats)#
```

**Syntax**

```
ss7link schema schema_name format schema_format

no ss7link schema schema_name
```

**no**
Removes the specified SS7 Link schema from statistics collection.

**schema_name**
Specifies the schema’s name.

- `schema_name` must be an alphanumeric string of 1 through 31 characters.
- `schema_name` must be an alphanumeric string of 1 through 31 characters.

**format schema_format**
Specifies the schema’s format.

- `schema_format` must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of the command, including spaces”” characters. For more information, see the [Schema Format String Length](#) section.
- For information on the schema format’s syntax, see the [Schema Format String Syntax](#) section.

**Important:** For a complete list of the statistics that are supported for this schema, refer to the [Statistics and Counters Reference](#).

**Usage**

Use this command to define schemas for SS7 link and linkset bulk statistics collection per SS7 routing domain in a generated stats report file. Usually a schema consists of multiple variables to collect all the statistics for a particular situation. Using double quote marks and text within this command, the reported statistics can be easily identified.
Multiple collection schemas can be created to categorize SS7 link bulk statistics. All of the schemas are processed at each collection interval. To create multiple SS7 link schemas, re-issue the `ss7link schema schema_name` command using a different schema name each time.

**Example**

The following command creates a schema named `ss7lnklstats1` that records the changeover orders sent and received per linkset and link and per SS7 routing domain:

```
ss7link schema ss7lnklstats1 format "%ss7rd-number-%ss7-linkset-id-%ss7-link-id-%ss7rd-asp_instance-%ss7-link-mtp3-changeover-order-tx-%ss7-link-mtp3-changeover-order-rx"
```
ss7rd schema

Configures the collection of bulk statistics for SS7 routing domain services, which include the activity statistics for SCTP, MTP, and M3UA data.

Product
SGSN
HNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Bulk Statistics Configuration
configure > bulkstats mode

Entering the above command sequence results in the following prompt:

[local]host_name(config-bulkstats)#

Syntax

ss7rd schema schema_name format schema_format
no ss7rd schema schema_name

no
Removes the specified SS7 routing domain schema from statistics collection.

schema_name
Specifies the schema’s name.
schema_name must be an alphanumeric string of 1 through 31 characters.

format schema_format
Specifies the schema’s format.
schema_format must be an alphanumeric string of 1 through “1021 minus “number of characters in rest of the command, including spaces”” characters. For more information, see the Schema Format String Length section.
For information on the schema format’s syntax, see the Schema Format String Syntax section.

Important: For a complete list of the statistics that are supported for this schema, refer to the Statistics and Counters Reference.

Usage

Use this command to define schemas for collection of SS7 routing domain statistics to be included in the generated stats report file. Usually a schema consists of multiple variables to collect all the statistics for a particular situation. Using double quote marks and text within this command, the reported statistics can be easily identified.
Multiple collection schemas can be created to categorize SS7 routing domain bulk statistics. All of the schemas are processed at each collection interval. To create multiple SS7 routing domain schemas, re-issue the `ss7rd schema schema_name` command using a different schema name each time.

**Example**

The following command creates a schema named `ss7rd1stats1` that identifies the SS7 routing domain and records the Application Server Process instance in the SS7 routing domain, along with the total number of sent and received SHUTDOWN messages per SS7 routing domain:

```bash
ss7rd schema ss7rd1stats1 format "%ss7rd-number%-%ss7rd-asr_instance%-%ss7rd-sctp-shutdown-tx%-%ss7rd-sctp-shutdown-rx%"
```
**transfer-interval**

Configures the frequency of transfer of collected statistics to the receiver.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Bulk Statistics Configuration
configure > bulkstats mode

Entering the above command sequence results in the following prompt:

[local]host_name(config-bulkstats)#

**Syntax**

```
transfer-interval minutes
```

*minutes*

Specifies the number of minutes between the transfer of collected statistics to the receivers as an integer from 1 through 999999.

**Usage**

Modify the transfer interval based upon the number of sessions per second. As the number of session requests per second increases it may become necessary to increase the transfer interval to reduce the processing overhead frequency for statistics delivery. This is tempered by the impact reduced resolution of statistical data has on usefulness of data when the interval gets larger than the least busy hours and most busy hours of the day.

The system is shipped from the factory with the transfer interval set to 480 minutes.

**Example**

```
transfer-interval 1440
```
**vlan-npu schema**

Configures the collection of VLAN-NPU activity statistics.

---

**Important:** The VLAN-NPU counters will only be displayed if the **logical-port-statistics** command has been enabled at the interface level under the Ethernet Interface Configuration mode.

---

**Product**

All

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Bulk Statistics Configuration

`configure > bulkstats mode`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-bulkstats)#
```

**Syntax**

```
vlan-npu schema  schema_name format  schema_format
no vlan-npu schema  schema_name
```

---

**no**

Removes the specified VLAN-NPU schema from statistics collection.

**schema_name**

Specifies the schema’s name.

*schema_name* must be an alphanumeric string of 1 through 31 characters.

**format  schema_format**

Specifies the schema’s format.

*schema_format* must be an alphanumeric string of 1 through 3599 characters minus the number of characters in rest of the command, including spaces and double quotation mark (""”) characters. For more information, see the **Schema Format String Length** section. For information on the schema format’s syntax, see the **Schema Format String Syntax** section.

---

**Important:** For a complete list of the statistics that are supported for this schema, refer to the **Statistics and Counters Reference**.

---

**Usage**

Use this command to define schemas for VLAN-NPU bulk statistics collection in the generated stats report files. Usually a schema consists of multiple variables to collect all the statistics for a particular situation. Using double quote marks and text within this command, the reported statistics can be easily identified.
Multiple VLAN-NPU schemas can be created to categorize VLAN-NPU bulk statistics. All of the schemas are processed at each collection interval. To create multiple VLAN-NPU schemas, re-issue the `vlan-npu schema schema_name` command using a different schema name each time.

**Example**

Include the bulk statistic variable names to create a VLAN-NPU schema named `vlanstats_vlan12` that specifies collection of statistics (a schema format) will be by VLAN-NPU interface for the total number of frames and bytes received with no Access Control List (ACL) match.

```
vlan-npu schema vlanstats_vlan12 format "VLAN12: %interfacename%\nTotal Frames Recv’d with no ACL match: %no-acl-match-rx-frames%\nTotal Bytes Recv’d with no ACL match: %no-acl-match-rx-bytes%\n"
```
Chapter 36
Bulk Statistics File Configuration Mode Commands

This section describes a bulk statistic “file” under which to group the bulk statistic configuration. The Bulk Statistics File Configuration mode supports the configuration of “files” used for organizing bulk statistics schema, delivery options, and receiver information.

Because multiple “files” can be configured, this functionality provides greater flexibility in that it allows you to configure different schemas to go to different receivers.

**Important:** Use of bulk statistics “files” is optional. However system logically assigns “file 1” to the standard configuration. Therefore, if you wish to configure bulk statistics “files” at a later time, “file 1” can be used.

**Caution:** If the Web Element Manager application is used to collect and process (XML parsing, graphing, etc.) bulk statistics data, “file 1” is used by the Web Element Manager’s default bulk statistics collection information and schemas. To avoid errors in processing by the Web Element Manager, do not configure “file 1” via the CLI. However, it is possible to configure files 1 through 4 using the system’s CLI, regardless of whether or not the Web Element Manager is configured as a receiver. In this case, the bulk statistics data is written to the server but not processed by the Web Element Manager application.

**Mode**

Exec > Global Configuration > Bulk Statistics Configuration > Bulk-File Configuration

`configure > bulkstats config_mode file file_number`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-bulkstats-file-number)#
```

**Important:** The commands in this configuration mode are identical to the same commands in the “Bulk Statistics Configuration Mode Commands” chapter.

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
Chapter 37
Call Control Profile Configuration Mode

Call Control Profile configuration mode defines call-handling rules which can be combined with other profiles – such as an APN profile (see the APN Profile Configuration Mode Commands chapter) – when using the Operator Policy feature. The call control profile is a key element in the Operator Policy feature and the profile is not valid until it is associated with an operator policy (see the associate command in the Operator Policy Configuration Mode Commands chapter).

The MME and SGSN each support a maximum of 1,000 call control profiles; only one profile can be associated with an operator policy.

By configuring a call control profile, the operator fine tunes any desired restrictions or limitations needed to control call handling per subscriber or for a group of callers across IMSI (International Mobile Subscriber Identity) ranges.

Mode

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-call-control-profile-profile_name)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
**access-restriction-data**

Enables the operator to assign a failure code to be included in reject messages if the attach rejection is due to access restriction data (ARD) checking in the incoming subscriber data (ISD) messages. The operator can also disable the ARD checking behavior.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-call-control-profile-profile_name)#

**Syntax**

access-restriction-data { eutran-not-allowed | failure-code cause_code | no-check }

remove access-restriction-data { failure-code | eutran-not-allowed }

---

**eutran-not-allowed**

Overrides the eutran-not-allowed flag received in ISD/ULA messages from the HLR/HSS received during the Attach process. The overridden value will be sent to the RNC during PDP context activation (in RAB Assignment Request messages) so that the RNC subsequently avoids performing a handover to E-UTRAN. Configuration of the eutran-not-allowed parameter is valid only if SRNS relocation first has been configured in Call Control Profile Configuration Mode via the srns-inter and/or srns-intra commands. The call-control-profile then must be associated with an operator policy in Operator Policy Configuration Mode using the associate command. Once the operator policy is associated with the call-control-profile, inclusion of the E-UTRAN Service Handover Information Element in RAB Assignment Request and Relocation Request RANAP messages must be enabled. This is done by executing the ranap eutran-service-handover-ie command in RNC Configuration Mode.

**failure-code cause_code**

cause_code: Enter an integer from 2 through 111; default code is 13 (roaming not allowed in this location area [LA]).

Refer to the GMM failure cause codes listed below (from section 10.5.5.14 of the 3GPP TS 124.008 v7.2.0 R7):

- 2 - IMSI unknown in HLR
- 3 - Illegal MS
- 6 - Illegal ME
- 7 - GPRS services not allowed
8 - GPRS services and non-GPRS services not allowed
9 - MSID cannot be derived by the network
10 - Implicitly detached
11 - PLMN not allowed
12 - Location Area not allowed
13 - Roaming not allowed in this location area
14 - GPRS services not allowed in this PLMN
15 - No Suitable Cells In Location Area
16 - MSC temporarily not reachable
17 - Network failure
20 - MAC failure
21 - Synch failure
22 - Congestion
23 - GSM authentication unacceptable
40 - No PDP context activated
48 to 63 - retry upon entry into a new cell
95 - Semantically incorrect message
96 - Invalid mandatory information
97 - Message type non-existent or not implemented
98 - Message type not compatible with state
99 - Information element non-existent or not implemented
100 - Conditional IE error
101 - Message not compatible with the protocol state
111 - Protocol error, unspecified

no-check
Including this keyword with the command disables the ARD checking behavior.

Usage
By default, the SGSN checks access restriction data (ARD) within incoming insert subscriber data (ISD) messages. This enables operator to selectively restrict subscribers in either 3G (UTRAN) or 2G (GERAN). The SGSN ARD checking behavior occurs during the attach procedure and if a reject occurs, the SGSN sends the subscriber an Attach Reject message with a configurable failure cause code.

Example
For this call control profile, the following command disables the ARD checking function:

```
access-restriction-data no-check
```
accounting context

Defines the name of the accounting context and optionally associates a GTPP group with this call control profile.

Product
- ePDG
- S-GW
- SAEGW
- SGSN
- SaMOG

Privilege
- Security Administrator, Administrator

Mode
- Exec > Global Configuration > Call Control Profile Configuration
- configure > call-control-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-call-control-profile-profile_name)#

Syntax

accounting context  ctx_name [ aaa-group  grp_name ] [ gtp group  grp_name ]

remove accounting context [ aaa-group | gtp ]

remove

Removes the accounting configuration from this profile’s configuration.

ctx_name

Specifies the accounting context as an alphanumeric string of 1 through 79 characters.

aaa-group  grp_name

Configures AAA Group for MRME.

grp_name is a string of 1 to 63 characters (any combination of letters and digits) to identify the aaa-group created with the aaa-group command in the Context configuration mode.

gtp group  grp_name

Identifies the GTPP group, where the GTPP related parameters have been configured in the GTPP Group Configuration mode, to associate with this call control profile.

grp_name is a string of 1 to 63 characters (any combination of letters and digits) to identify the GTPP group created with the gtp group command in the Context configuration mode.
Usage
This command can be used to associate a predefined GTPP server group - including all its associated configuration - with a specific call control profile. The GTPP group would have been defined with the `gtpp group` command (see the `Context Configuration Mode Commands` chapter).
If the GTPP group is not specified, then a default GTPP group in the accounting context will be used.
If this command is not specified, use the name of the accounting context configured in the SGSN service configuration mode (for 3G) or the GPRS service configuration mode (for 2G), either will automatically use a “default” GTPP group generated in that accounting context.
If the accounting context is specified in the GPRS service or SGSN service and in a call control profile, the priority is given to the accounting context of the call control profile.

Example
For this call control profile, the following command identifies an accounting context called `acctng1` and associates a GTPP server group named `roamers` with defined charging gateway accounting functionality.

```
accounting context acctng1 gtpp group roamers
```
accounting mode

Configures the mode to be used for accounting – GTPP (default), RADIUS/Diameter or None.

**Product**  
S-GW  
SAEGW

**Privilege**  
Administrator

**Mode**  
Exec > Global Configuration > Call Control Profile Configuration  

```
configure > call-control-profile profile_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

**Syntax**

```
accounting mode { gtpp | none | radius-diameter }
```

**remove accounting mode**

- **remove**
  
  Removes the accounting mode.

- **gtpp**
  
  Specifies that GTPP accounting is performed. This is the default method.

- **none**
  
  Specifies that no accounting will be performed for the call control profile.

- **radius-diameter**
  
  Specifies that RADIUS/Diameter will be performed for the call control profile.

**Usage**

Use this command to specify the accounting mode for a call control profile. For additional information on accounting mode and its relationship to operator policy, refer to the *System Administration Guide*.

**Example**

The following command specifies that RADIUS/Diameter accounting will be used for the call control profile:

```
accounting mode radius-diameter
```
accounting stop-trigger

Configures the trigger point for accounting stop CDR. Default is on session deletion request.

**Product**
S-GW
SAEGW

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Call Control Profile Configuration
configure > call-control-profile profile_name

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

**Syntax**

```
accounting stop-trigger custom

default accounting stop-trigger

default
Accounting stop CDR triggered once Delete Session/Delete Bearer Request is received at S-GW.

custom
Accounting stop CDR triggered once Delete Session/Delete Bearer Response is received at S-GW.
```

**Usage**

Use this command to specify the trigger point for accounting stop CDR for a call control profile.

**Example**

The following command specifies that accounting stop trigger would be at response of session deletion:

```
accounting stop-trigger custom
```
allocate-ptmsi-signature

Enables or disables the allocation of a P-TMSI (Packet Temporary Mobile Subscriber Identity) signature.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Call Control Profile Configuration

    configure > call-control-profile profile_name

Entering the above command sequence results in the following prompt:

    [local]host_name(config-call-control-profile-profile_name)#

Syntax

[ no | default ] allocate-ptmsi-signature

no
Disables the allocation of the P-TMSI signature.

default
Resets the configuration value to the default, which is to allocate the P-TMSI signature.

Usage
Use this command to enable or disable the allocation of the P-TMSI signature.

Example

    allocate-ptmsi-signature
apn-restriction

Enables the APN restriction feature and configures the instruction for the SGSN on the action to take when an APN restriction value is received from the GGSN during an Update PDP Context procedure.

Product

SGSN

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > Call Control Profile Configuration
configure > call-control-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-call-control-profile-profile_name)#

Syntax

apn-restriction update-policy deactivate restriction

default apn-restriction

default

Creates a default APN restriction configuration.

update-policy deactivate restriction

Specifies one of the two restriction types to define the appropriate action if the APN restriction value received conflicts with the stored value:

*least-restrictive* set the least restrictive value applicable when there are no already active PDP context(s).

*most-restrictive* sets the most stringent restriction required by any already active PDP context(s).

Usage

When this feature is enabled, the SGSN will send the maximum APN restriction value in every CPC Request message sent to the GGSN. The SGSN expects to receive an APN restriction value in each PDP Context received from the GGSN. The SGSN stores and compares received APN restriction values to check for conflicts. In the case of a conflict, the SGSN rejects the PDP Context with appropriate messages and error codes to the MS.

If an APN restriction value is not assigned by the GGSN, the SGSN assumes the value of “1” (least restrictive) to allow APN restriction rules will be possible when valid values are assigned for new PDP Context(s) from the same MS.

Example

The following command applies the lowest level of APN restrictions:

    apn-restriction update-policy deactivate least-restrictive
associate

Associates various MME-specific lists and databases with this call control profile. On an SGSN, this command can be used to associate some of these MME-related items to GPRS and/or SGSN services in support of S4 functionality.

Product

ePDG
MME
SGSN

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-call-control-profile-profile_name)#

Syntax

associate { ho-restrict-list list_name | hss-peer-service service_name [ s13-interface | s6a-interface | s13-prime-interface | s6d-interface ] | tai-mgmt-db tai-db_name }

remove associate { ho-restrict-list | hss-peer-service [ s13-interface | s6a-interface | s13-prime-interface | s6d-interface ] | tai-mgmt-db }

remove

Remove the specified association definition from the call control profile.

---

**ho-restrict-list list_name**

MME only.

Identifies the handover restriction list that should be associated with this call control profile.

`list_name` is a string of 1 to 64 characters (any combination of letters and digits).

---

**hss-peer-service service_name**

Associates a home subscriber server (HSS) peer service with this call control profile.

`service_name` is an existing HSS peer service expressed as a string of 1 to 63 characters (any combination of letters and digits).

---

[ s13-interface | s6a-interface | s13-prime-interface | s6d-interface ]

Optionally, identify the interface to be associated with the HSS service in this call control profile.

The `s13-interface` and the `s6a-interface` options apply to the MME only.

The `s13-prime-interface` and `s6d-interface` options apply to the SGSN only.

The `s6d-interface` is used by the SGSN to communicate with the HSS. It is a Diameter-based interface which supports location management, subscriber data handling, authentication, and fault recovery procedures.
The **s13-prime-interface** is used by the SGSN to communicate with the equipment identity register (EIR). It is a Diameter-based interface which performs the mobile equipment (ME) identity check procedure.

**Important:** The **s13-prime-interface** can only be used if an **s6d-interface** is configured.

```
tai-mgmt-db tai-db_name
```

Identifies the tracking area identifier (TAI) database that should be associated with this call control profile. 

* `tai-db_name` is a string of 1 to 64 characters (any combination of letters and digits).

This configuration overrides the S-GW selection and TAI list assignment functionality for a call that uses an operator policy associated with this call control profile. The TAI management object provides a TAI list for calls and provides S-GW selection functionality if a DNS is not configured for S-GW discovery for this operator policy or if a DNS discovery fails.

If a TAI management database is associated with a call-control-profile, and if DNS is used for S-GW lookups, then the DNS configuration for S-GW lookups must also be configured within the same call-control-profile using the **dns-sgw** command in the call-control-profile configuration mode.

On the S4-SGSN, use this option to associate a locally configured S-GW address for the RAI address for selection if operators wish to bypass DNS resolution of RAI FQDN. This option is valid only after the following commands have been executed on the S4-SGSN:

- The **tai-mgmt-db** command in **LTE Policy Configuration Mode**
- The **tai-mgmt-obj** command in **LTE TAI Management Database Configuration Mode**.
- The **tai** and **sgw-address** commands in **LTE TAI Management Object Configuration Mode**.

**Usage**

Use this command to associate handover restriction lists, HSS service (and interfaces), and a TAI database with the call control profile. This ensures that the information is available for application when a Request is received.

Repeat the command as needed to associate each feature.

**Example**

Link HO restriction list named **HOrestrict1** with this call control profile:

```
associate ho-restrict-list HOrestrict1
```

The following command associates this SaMOG call control profile with an accounting policy called **acct1**:

```
```
attach access-type

Defines attach-related configuration parameters for this call control profile based on the access-type (GPRS, UMTS, or both) and location area list.

**Important:** SGSN only: Before using this command, ensure that the appropriate location area code (LAC) information has been defined via the `location-area-list` command.

**Product**
- MME
- SGSN

**Privilege**
- Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Call Control Profile Configuration
`configure > call-control-profile profile_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

**Syntax**

```
attach access-type { gprs | umts } { all | location-area-list instance list_id } { failure-code code | user-device-release { before-r99 failure code code | r99-or-later failure code code } }

default attach access-type { eps | gprs | umts } { all | location-area-list instance list_id } { failure-code | user-device-release { before-r99 failure code code | r99-or-later failure code code } }

default

Restores the default values for the for the specified parameter.

**access-type type**

Defines the type of access to be allowed or restricted.
- *gprs*
- *umts*

**all**

Instructs the SGSN or MME to apply the command action to all location area lists. Location area lists should already have been created with the `location-area-list` command. The location area list consists of one or more LACs, location area codes, where the MS is when placing the call.
location-area-list instance list_id

Instructs the SGSN to apply the command action to a specific location area list. Location area lists should already have been created with the location-area-list command. The location area list consists of one or more LACs, location area codes, where the MS is when placing the call. Using this keyword with either the allow or restrict keywords enables you to configure with more granularity.

list_id: Enter an integer between 1 and 5.

failure-code code

Specify a GMM failure cause code to identify the reason an attach did not occur. This GMM cause code will be sent in the reject message to the MS.

Default: 14.

fail-code: Enter an integer from 2 to 111. Refer to the GMM failure cause codes listed below (from section 10.5.5.14 of the 3GPP TS 124.008 v7.2.0 R7):

- 2 - IMSI unknown in HLR
- 3 - Illegal MS
- 6 - Illegal ME
- 7 - GPRS services not allowed
- 8 - GPRS services and non-GPRS services not allowed
- 9 - MSID cannot be derived by the network
- 10 - Implicitly detached
- 11 - PLMN not allowed
- 12 - Location Area not allowed
- 13 - Roaming not allowed in this location area
- 14 - GPRS services not allowed in this PLMN
- 15 - No Suitable Cells In Location Area
- 16 - MSC temporarily not reachable
- 17 - Network failure
- 20 - MAC failure
- 21 - Synch failure
- 22 - Congestion
- 23 - GSM authentication unacceptable
- 40 - No PDP context activated
- 48 to 63 - retry upon entry into a new cell
- 95 - Semantically incorrect message
- 96 - Invalid mandatory information
- 97 - Message type non-existent or not implemented
- 98 - Message type not compatible with state
- 99 - Information element non-existent or not implemented
- 100 - Conditional IE error
Call Control Profile Configuration Mode

- attach access-type

- 101 - Message not compatible with the protocol state
- 111 - Protocol error, unspecified

```
user-device-release { before-r99 | r99-or-later } failure-code code
```

Default: disabled
Enables the SGSN to reject an Attach procedure based on the detected 3GPP release version of the MS equipment and selectively send a failure cause code in the reject message. The SGSN uses the following procedure to implement this configuration:

1. When Attach Request is received, the SGSN checks the subscriber’s IMSI and current location information.
2. Based on the IMSI, an operator policy and call control profile are found that relate to this Attach Request.
3. Profile is checked for access limitations.
4. Attach Request is checked to see if the revision indicator bit is set
   - if not, then the configured common failure code for reject is sent;
   - if set, then the 3GPP release level is verified and action is taken based on the configuration of this parameter

One of the following options must be selected and completed:
- `before-r99`: Indicates the MS would be a 3GPP release prior to R99 and an appropriate failure code should be defined.
  ```
  failure-code code: Enter an integer from 2 to 111.
  ```
- `r99-or-later`: Indicates the MS would be a 3GPP Release 99 or later and an appropriate failure code should be defined.
  ```
  failure-code code: Enter an integer from 2 to 111.
  ```

Usage

Once the IMSI of an incoming call is known and matched with a specific operator policy, according to the filter definition of the `mcc` command, then the associated call control profile is selected to determine how the incoming call is handled.

By default, all attaches are allowed. If no access limitations are needed, do not use the `attach` command.

**Important:** Before using this command, ensure that the appropriate LAC information has been defined with the `location-area-list` command.

Use this command to define attach limitations for the call control profile.

Use this command to fine-tune the attach configuration specifying which calls/subscribers can attach and which calls are restricted from attaching and what failure code is included in the Reject message.

Attachment restrictions can be based on any one or combination of the options, such as location area code or access type. It is even possible to restrict all attaches.

The command can be repeated using different keyword values to further fine-tune the attachment configuration.

**Related Commands**

- Use the `attach restrict` command to restrict attaches.
Use the `attach allow` command to re-enable restrictions after an `attach restrict` command has been used.

**Example**

The following example sets all restrictions for access-type gprs and specified release version to the default setting.

```bash
default attach access-type gprs all user-device-release before-r99 failure-code
```
attach allow

Configures the system to re-enable attaches that were previously restricted using the attach restrict command.

**Important:** SGSN only: Before using this command, ensure that the appropriate location area code (LAC) information has been defined via the location-area-list command.

**Product**
MME
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Call Control Profile Configuration
configure > call-control-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-call-control-profile-profile_name)#

**Syntax**

```
[ no ] attach allow access-type { eps | gprs | umts } location-area-list instance list_id
```

- **no**
  Deletes the specified attach configuration.

- **allow**
  Enables attaches in the configuration after an attach restrict command has been used.

- **access-type type**
  Defines the type of access to be allowed.
  - eps
  - gprs
  - umts

- **location-area-list instance list_id**
  Instructs the SGSN to apply the command action to a specific location area list. Location area lists should already have been created with the location-area-list command. The location area list consists of one or more LACs, location area codes, where the MS is when placing the call.
  
  *list_id:* Enter an integer between 1 and 5.
Call Control Profile Configuration Mode

attach allow

Usage

Once the IMSI of an incoming call is known and matched with a specific operator policy, according to the filter definition of the mcc command, then the associated call control profile is selected to determine how the incoming call is handled.

By default, all attaches are allowed. If no access limitations are needed, then do not use the attach command.

Important: Before using this command, ensure that the appropriate LAC information has been defined with the location-area-list command.

Use this command to define attach limitations for the call control profile.

Use this command to fine-tune the attach configuration specifying which calls/subscribers can attach and which calls are restricted from attaching and what failure code is included in the Reject message.

Attachment restrictions can be based on any one or combination of the options, such as location area code or access type. It is even possible to restrict all attaches.

The command can be repeated using different keyword values to further fine-tune the attachment configuration.

Related Commands

- Use the attach access-type command to define the type of access to restrict or allow.
- Use the attach restrict command to restrict attaches.

Example

For calls under the purview of this call control profile, the following command allows attaches of all subscribers using the GPRS access type.

```
attach allow access-type gprs all
```
**attach imei-query-type**

Defines device Attach limitations for this call control profile if an IMEI is not already present in the Attach Request.

**Product**
- MME
- SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Call Control Profile Configuration

```
configure > call-control-profile profile_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

**Syntax**

```
attach imei-query-type { imei | imei-sv | none } [ verify-equipment-identity [ allow-on-eca-timeout | deny-greylisted | deny-unknown | verify-emergency ] + ]
```

```
remove attach imei-query-type
```

**remove**

Deletes the specified attach configuration.

```
imei-query-type { imei | imei-sv | none }
```

Configures system behavior during Attach procedures if an IMEI is not already present in the Attach Request.

- **imei**: Specifies that the system is required to query the UE for its International Mobile Equipment Identity (IMEI).
- **imei-sv**: Specifies that the system is required to query the UE for its International Mobile Equipment Identity - Software Version (IMEI-SV).
- **none**: Specifies that the system does not need to query for IMEI or IMEI-SV.

```
verify-equipment-identity [ allow-on-eca-timeout | deny-greylisted | deny-unknown | verify-emergency ]
```

Specifies that the identification (IMEI or IMEI-SV) of the UE is to be performed by the Equipment Identity Register (EIR) over the S13 interface.

- **allow-on-eca-timeout**: Configures the MME to allow equipment that has timed-out on ECA during the attach procedure.
- **deny-greylisted**: Configures the MME to deny grey-listed equipment during the attach procedure.
- **deny-unknown**: Configures the MME to deny unknown equipment during the attach procedure.
- **verify-emergency**: Configures the MME to ignore the IMEI validation of the equipment during the attach procedure in emergency cases. This keyword is only supported in release 12.2 and higher.
Usage
Configures system settings related to the UE Attach procedure for the specified call control profile. The command can be repeated using different keyword values to further fine-tune the attachment configuration.

Example
The following command configures the system to query the UE for its IMEI and to verify the UE equipment identity with an Equipment.

```bash
attach imei-query-type imei verify-equipment-identity
```
**attach restrict**

Configures the system to restrict attaches based on access type and location areas (either all or specified location area list) for this call control profile.

**Important:** SGSN only: Before using this command, ensure that the appropriate location area code (LAC) information has been defined via the `location-area-list` command.

**Product**
- MME
- SGSN

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration > Call Control Profile Configuration
  - `configure > call-control-profile profile_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

**Syntax**

```
```

- `no`
  - Deletes the specified attach configuration.

- `access-type type`
  - Defines the type of access to be allowed or restricted.
    - `eps`
    - `gprs`
    - `umts`

- `emm-cause-code code`
  - Specifies the EPS Mobility Management (EMM) cause code to return to the UE:
    - `eps-service-disallowed`
    - `eps-service-not-allowed-in-this-plmn`
    - `no-suitable-cell-in-tracking-area`
    - `plmn-not-allowed`
    - `roaming-not-allowed-in-this-tracking-area`
Call Control Profile Configuration Mode

attach restrict

*tracking-area-not-allowed*

The default cause code is `no-suitable-cell-in-tracking-area`.

**Important:** The `tracking-area-not-allowed` cause code is not supported for the MME.

**Important:** The `roaming-not-allowed-in-this-tracking-area` and `tracking-area-not-allowed` cause codes are not applicable for use with the `imsi-attach-fail` or `voice-unsupported` keywords.

`imsi-attach-fail`

Directs the MME to restrict EPS attach when IMSI attach fails. If the policy is configured, all IMSI failures will result in an EPS restriction.

The default cause code for calls rejected for imsi-attach-fail is `no-suitable-cell-in-tracking-area`.

`voice-unsupported`

Directs the MME to restrict EPS attach when voice is not supported, such as when Voice over IMS is not supported and the UE does not support Circuit Switched Fall Back (CSFB).

This setting is applicable when all of the following conditions apply:

- The UE is voice-centric as determined in the UE usage setting of the Voice Domain and UE Settings IE sent in the request.
- The UE does not support CSFB as determined in the EMM Combined procedures Capability bit of the MS Network Capability IE sent in the request, OR if CSFB is not supported on the MME as determined by the SGs service not being associated with the MME service.
- Voice over IMS is not supported in the network as defined by the `network-feature-support-ims-voice-over-ps` command.

The default cause code for calls rejected for voice-unsupported is `no-suitable-cell-in-tracking-area`.

`all`

Instructs the system to apply the command action to all location area lists. Location area lists should already have been created with the `location-area-list` command. The location area list consists of one or more LACs, location area codes, where the MS is when placing the call.

`location-area-list instance list_id`

Instructs the SGSN to apply the command action to a specific location area list. Location area lists should already have been created with the `location-area-list` command. The location area list consists of one or more LACs, location area codes, where the MS is when placing the call.

Using this keyword with either the `allow` or `restrict` keywords enables you to configure with more granularity.

`list_id`: Enter an integer between 1 and 5.

**Important:** This keyword only applies to the SGSN.
### Usage

Once the IMSI of an incoming call is known and matched with a specific operator policy, according to the filter definition of the `mcc` command, then the associated call control profile is selected to determine how the incoming call is handled.

By default, all attaches are allowed. If no access limitations are needed, then do not use the `attach` command.

**Important:** Before using this command, ensure that the appropriate LAC information has been defined with the `location-area-list` command.

Use this command to restrict attaches for the call control profile.

Use this command to fine-tune the attach configuration specifying which calls/subscribers can attach and which calls are restricted from attaching and what failure code is included in the Reject message.

Attachment restrictions can be based on any one or combination of the options, such as location area code or access type. It is even possible to restrict all attaches.

The command can be repeated using different keyword values to further fine-tune the attachment configuration.

**Related Commands**

- Use the `attach access-type` command to define the type of access to restrict or allow. The command `attach restrict access-type gprs all` has to be enabled, if the command `attach access-type gprs all failure-code < code >` is used to define a failure code. The failure code is saved after a re-boot only when the command `attach restrict access-type gprs all` is enabled.

- Use the `attach allow` command to re-enable restrictions after an `attach restrict` command has been used.

**Example**

For calls under the purview of this call control profile, the following command restricts the attaches of all subscribers using the GPRS access type.

```bash
attach restrict access-type gprs all
```

To change the attach restriction to only restrict attaches of GPRS subscribers from specified LACs included in location area list #2 and include failure-code 45 as the reject cause. This configuration requires two CLI commands:

```bash
attach restrict access-type gprs location-area-list instance 2
attach access-type gprs location-area-list instance 2 failure-code 45
```

In the case of a dual-access SGSN, it is possible to also add a second definition to restrict attaches of UMTS subscribers within the LACs included in location area list #3.

```bash
attach restrict access-type UMTS location-area-list instance 3
```

Change the configuration to allow attaches for GPRS access for all previously restricted LACs - note that GPRS attaches would still be limited:

```bash
no attach restrict access-type gprs all
```

Restrict (deny) all GPRS attach requests (coming from any location area) and assign a single failure code for the reject messages. This is a two command process:
attach restrict access-type gprs all
attach access-type grps all failure-code 22
authenticate all-events

Allows the operator to quickly define authentication procedures, based on limited parameters, for all types of events.

Product

MME
SGSN

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > Call Control Profile Configuration
configure > call-control-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-call-control-profile-profile_name)#

Syntax

authenticate all-events [ access-type { gprs | umts } | frequency frequency [ access-type { gprs | umts } ] ]

[ no | remove ] authenticate all-events [ access-type { gprs | umts } ]

---

no
Disables the specified authentication configuration in the call control profile.

---

remove
Removes the specified authentication configuration from the call control profile configuration file.

---

access-type type
One of the following must be selected to identify the type of network access if the access-type keyword is included in the command:

• gprs
• umts

The access-type keyword can be included with any of the other three keywords available with the authenticate all-events command.

---

frequency frequency
This keyword defines 1-in-N selective authentication for all types of subscriber events. If the frequency is set for 12, then the service skips authentication for the first 11 events and authenticates on the 12th event. frequency must be an integer from 1 to 16.
Usage

By default, authentication is not performed for any subscriber events. Use this command to enable authentication for all types of events at one time, such as but not limited to: Activate Requests, Attach Requests, Detach Requests, Service-Requests.

**Important:** For the SGSN, in releases 15.0 and forward, the authentication on activation functionality has been removed so the SGSN will not authenticate on Activate Requests.

Example

The following command configures all authentication for all subscribers to occur every tenth time a specific type of event occurs (for example every tenth time an Attach Request is received):

```
authenticate all-events frequency 10
```

The following command configures authentication for all Detach Requests and RAUs to occur if the UE access-type is UMTS:

```
authenticate all-events access-type umts
```
authenticate attach

Allows the operator to define authentication for Attach procedures.

Product

MME
SGSN

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > Call Control Profile Configuration
configure > call-control-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-call-control-profile-profile_name)#

Syntax

authenticate attach access-type { gprs | umts }
authenticate attach attach-type { combined | gprs-only } [ access-type { gprs | umts } ]
frequency frequency
authenticate attach frequency frequency [ access-type { gprs | umts } ]
authenticate attach inter-rat [ access-type { gprs | umts } ]
attach-type { combined | gprs-only } [ access-type { gprs | umts } ]
frequency frequency
[ access-type { gprs | umts } ]
[ no | remove ] authenticate attach [ access-type { gprs | umts } ]
attach-type { combined | gprs-only } [ access-type { gprs | umts } ]
inter-rat | attach-type { combined | gprs-only } ] [ access-type { gprs | umts } ]

no
Disables the defined authentication procedures configured for Attach Requests from the call control profile.

remove
Deletes the defined authentication procedures for Attach Requests from the call control profile configuration file.

access-type type

One of the following must be selected to identify the type of network access if the access-type keyword is included in the command:

• gprs
• umts
**attach-type**

This keyword configures the Attach authentication based on the type of attach requested. The `attach-type` must be one of the following options:

- `combined`: Authenticates combined GPRS/IMSI Attaches.
- `gprs-only`: Authenticates GRPS Attaches only.

**frequency frequency**

This keyword defines 1-in-N selective authentication for this type of subscriber event - Attach Request. If the frequency is set for 12, then the service skips authentication for the first 11 events and authenticates on the twelfth event.

`frequency` must be an integer from 1 to 16.

**inter-rat**

Enables/disables authentication for Inter-RAT Attaches.

**Usage**

Authentication for Attach is disabled by default. This command enables/disables authentication for an Attach with a local P-TMSI or Attaches with an IMSI, which will be authenticated to acquire the CK (cipher key) and the IK (integrity key).

**Example**

The following command configures authentication to occur after every tenth attach event for GPRS access.

```
authenticate attach frequency 10 access-type gprs
```

The following command disables authentication for Inter-RAT Attaches, use:

```
no authenticate attach inter-rat
```
authenticate detach

Allows the operator to enable and define authentication for Detach procedures.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Call Control Profile Configuration
configure > call-control-profile profile_name

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

**Syntax**

```
authenticate detach [ access-type umts ]
[ no | remove ] authenticate detach [ access-type umts ]
```

- **no**
  Disables the defined authentication procedures configured for Detach Requests from the call control profile.

- **remove**
  Deletes the defined authentication procedures for Detach Requests from the call control profile configuration file.

- **access-type umts**
  Optionally, identifies the type of network access if the `access-type umts` keywords are included in the command. By default, access-type UMTS is assumed.

**Usage**

Authentication for Detach procedures is disabled by default. This command enables/disables authentication for a Detach Request and allows the operator to limit authentication based on the MS/UE access-type.

**Example**

The following command configures detach authentication to occur only for UMTS attached subscribers:

```
authenticate detach access-type umts
```

The following command disables authentication for all Detach Requests, use:

```
no authenticate detach
```
**authenticate on-first-vector**

Allows the operator to enable the SGSN to begin MS authentication immediately after receiving the first vector from the HLR.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Call Control Profile Configuration  
```bash
configure > call-control-profile profile_name
```

Entering the above command sequence results in the following prompt:
```
[local]host_name(config-call-control-profile-profile_name)#
```

**Syntax**

```bash
authenticate on-first-vector
```

```bash
remove authenticate on-first-vector
```

**Usage**

After an initial attach request, some end devices restart themselves after waiting for the PDP to be established. In such cases, the SGSN restarts and a large number of end devices repeat their attempts to attach. The attach requests flood the radio network, and if the devices timeout before the PDP is established then they continue to retry, thus even more traffic is generated.

To avoid the high traffic levels during PDP establishment, the SGSN has been modified to reduce the attach time, as much as possible, so that the devices can attach and discontinue sending requests. The current enhancement is intended to reduce the time needed to retrieve vectors over the GR interface by allowing the operator to configure the SGSN to start authentication towards the MS as soon as it receives the first vector from the AuC/HLR. With the new command included in the configuration, the SGSN begins the MS authentication process immediately after receiving the first vector from the HLR while the SAI continues in parallel.

**Example**

Use the following command to configure the SGSN to begin MS authentication immediately after receiving the first vector from the AuC/HLR:

```bash
authenticate on-first-vector
```

Use the following command to reset the default behavior, so that the SGSN waits to receive all vectors requested in the SAI from the AuC/HLR before beginning authentication towards the MS:

```bash
remove authenticate on-first-vector
```
authenticate rau

Enables or disables and fine tunes authentication procedures for routing area updates (RAUs)

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Call Control Profile Configuration

**Syntax**

```bash
authenticate rau [ access-type { gprs | umts } | frequency frequency [ access { gprs | umts } ] | periodicity duration [ access { gprs | umts } ] | update-type { combined-update | imsi-combined-update | periodic | ra-update } [ access-type { gprs | umts } | frequency frequency | periodicity duration | with { foreign-ptmsi | inter-rat-local-ptmsi | local-ptmsi } [ access-type { gprs | umts } | frequency frequency | periodicity duration ]
```

```bash
no authenticate rau [ access-type { gprs | umts } | update-type { combined-update | imsi-combined-update | periodic | ra-update } [ access-type { gprs | umts } | with { foreign-ptmsi | inter-rat-local-ptmsi | local-ptmsi } [ access-type { gprs | umts } ]
```

```bash
remove authenticate rau [ access-type { gprs | umts } | periodicity [ access { gprs | umts } | update-type { combined-update | imsi-combined-update | periodic | ra-update } [ access-type { gprs | umts } | periodicity | with { foreign-ptmsi | inter-rat-local-ptmsi | local-ptmsi } [ access-type { gprs | umts } | periodicity ] ]
```

```bash
no
```

Disables authentication for the RAUs specified in the configuration for the call control profile.

```bash
remove
```

Deletes the authentication configuration for the RAUs from the call control profile in the configuration file.

**access-type type**

One of the following must be selected to identify the type of network access if the `access-type` keyword is included in the command:

```bash
* gprs
* umts
```

The `access-type` keyword can be included with any of the other keywords available with the `authenticate rau` command.
**frequency** *frequency*

Defines 1-in-N selective authentication for RAU events. If the frequency is set for 12, then the SGSN skips authentication for the first 11 events and authenticates on the twelfth event. *frequency* must be an integer from 1 to 16.

**periodicity** *duration*

Defines the length of time (number of minutes) that authentication can be skipped. *duration*: Must be an integer from 1 to 10800.

**update-type**

Defines the type of RAU Request. Select one of the following:

- `combined-update [ access-type | with inter-rat-local-ptmsi ]`
- `imsi-combined-update [ access-type | with inter-rat-local-ptmsi ]`
- `periodic [ access-type | frequency | periodicity ]`
- `ra-update [ access-type | with inter-rat-local-ptmsi ]`

**Usage**

By default, authentication is not performed for routing area updates (RAUs). Use this command to enable/disable authentication and to fine tune the authentication procedure based on frequency, periods for skipping authentication and the various types of routing area updates.

**Example**

The following command configures RAU authentication to occur after every tenth event for GPRS access.

```
authenticate rau frequency 10 access-type gprs
```

The following command disables authentication for RAUs based on the combined IMSI with foreign P-TMSIs, use:

```
no authenticate rau imsi-combined-update with foreign-ptmsi
```

The following command deletes all authentication configuration from the call control profile for all RAUs using GPRS access-type:

```
remove authenticate rau access-type gprs
```
authenticate service-request

Enables or disables and fine-tunes authentication procedures for Service Requests.

Product
MME
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Call Control Profile Configuration
configure > call-control-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-call-control-profile-profile_name)#

Syntax

authenticate service-request [ frequency frequency | periodicity duration | service-type { data | page-response | signaling } [ frequency frequency | periodicity duration ] ]

no authenticate service-request [ service-type { data | page-response | signaling } ]

remove authenticate service-request [ periodicity | service-type { data | page-response | signaling } [ periodicity ] ]

no
Disables authentication for the Service Requests specified in the configuration for the call control profile.

remove
Deletes the authentication configuration for Service Requests from the call control profile in the configuration file.

frequency frequency
Defines 1-in-N selective authentication for this type of subscriber event - Service Request. If the frequency is set for 12, then the service skips authentication for the first 11 events and authenticates on the twelfth event. frequency must be an integer from 1 to 16.

periodicity duration
Defines the length of time (number of minutes) that authentication can be skipped. duration: Must be an integer from 1 to 10800.

signaling-type
Defines the type of service being requested by the Service Request. Select one of the following:

• data
• page-response
By default, authentication is not performed for Service Requests. Use this command to enable/disable authentication and to fine-tune the authentication procedure based on frequency and periods for skipping authentication and the various types of service. Repeat the commands as needed to configure criteria for all service types.

Example

The following command configures authentication Service Requests for data service to only occur every 5 minutes:

```
authenticate service-request service-type data periodicity 5
```
authenticate sms

Enables or disables and fine tunes authentication procedures for Short Message Service (SMS).

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Call Control Profile Configuration

`configure > call-control-profile profile_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax

```
authenticate sms [ access-type { gprs | umts } ] | frequency frequency [ access-type { gprs | umts } ] | sms-type { mo-sms | mt-sms } [ access-type { gprs | umts } ] | frequency frequency ] ]
```

```
[ no | remove ] authenticate sms [ access-type { gprs | umts } ] | sms-type { mo-sms | mt-sms } | access-type { gprs umts } ] ]
```

- **no**
  Disables authentication for the SMS Requests specified in the configuration for the call control profile.

- **remove**
  Deletes the authentication configuration for SMS Requests from the call control profile in the configuration file.

- **access-type type**
  One of the following must be selected to identify the type of network access if the `access-type` keyword is included in the command:
  ```
  *gprs
  *umts
  ```
  The `access-type` keyword can be included with any of the other keywords available with the `authenticate sms` command.

- **frequency frequency**
  Defines 1-in-N selective authentication for SMS Requests. If the frequency is set for 12, then the SGSN skips authentication for the first 11 events and authenticates on the twelfth event.
  `frequency` must be an integer from 1 to 16.

- **sms-type**
  Enables authentication for the following SMS types:
**authenticate sms**

- **mo-sms**: mobile-originated SMS
- **mt-sms**: mobile-terminated SMS

**Usage**

By default, authentication is not performed for short message service (SMS). Use this command to enable/disable authentication and to fine-tune the authentication procedure based on MS/UE access type and the frequency for the selected SMS type. Repeat the commands as needed to configure criteria for all service types.

**Example**

The following command configures MO-SMS authentication to occur every fifth request:

```
authenticate sms sms-type mo-sms frequency 5
```
authenticate tau

Allows the operator to enable/disable and fine-tune authentication for the tracking area update (TAU) procedures.

Product
MME

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Call Control Profile Configuration
configure > call-control-profile profile_name
Entering the above command sequence results in the following prompt:

[local]host_name(config-call-control-profile-profile_name)#

Syntax

authenticate tau [ frequency frequency | inter-rat | periodicity interval ]

no authenticate tau inter-rat

no

Disables the TAU authentication procedures specified in the call control profile configuration.

frequency frequency

Defines 1-in-N selective authentication for this type of subscriber event - a tracking area update for an inter-RAT Attach. If the frequency is set for 12, the MME skips authentication for the first 11 events and authenticates on the twelfth event.
frequency must be an integer from 1 to 16.

inter-rat

Enables authentication for TAU procedures for inter-RAT Attaches.

periodicity duration

Defines the length of time (number of minutes) that authentication can be skipped.
duration: Must be an integer from 1 to 10800.

Usage

Authentication for TAU procedures is disabled by default. This command enables/disables authentication for a inter-RAT TAU procedures and allows the operator to limit authentication based on the frequency of the events or elapsed intervals between the events.

Example

The following command configures TAU authentication to occur when there is 15 minutes between inter-RAT Attaches:

authenticate tau periodicity 15
The following command disables authentication for all TAU Inter-RAT Attaches, use:

```
no authenticate tau
```
CC

Defines the charging characteristics to be applied for CDR generation when the handling rules are applied via the Operator Policy feature.

Product

MME
SAEGW
S-GW
SGSN

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > Call Control Profile Configuration
configure > call-control-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-call-control-profile-profile_name)#

Syntax

cc { behavior-bit no-records bit_value | local-value behavior bit_value profile index_bit | prefer { hlr-hss-value | local-value } }

no cc behavior-bit no-records

remove cc { behavior-bit no-records | local-value | prefer }

no

Disables the no records generation behavior-bit configuration for this call control profile.

remove

Removes the specified charging characteristic configuration from this profile.

behavior-bit no-records bit_value

Default: disabled
Specifies the charging characteristic behavior bit. no-records instructs the system not to generate any accounting records regardless of what may be configured elsewhere.

local-value behavior bit_value profile index_bit

Defaults: bit_value = 0x0, index_bit = 8
Sets the local value of the behavior bits and profile index for the charging characteristics when the HLR/HSS does not provide values for these parameters.

bit_value is a hexadecimal value between 0x0 and 0xFFF.

index_bit is an integer value from 1 through 15.
Setting the profile index bis selects different charging trigger profiles to be used with the call control profile. Some of the index values are predefined according to 3GPP standard:

- **1** for hot billing
- **2** for flat billing
- **4** for prepaid billing
- **8** for normal billing

If the HLR/HSS provides the charging characteristics with behavior bits and profile index and the operator prefers to ignore the HLR/HSS values, then also configure the `prefer local-value` keyword.

```
prefer { hlr-hss-value | local-value }
```

Default: `hlr-hss-value`

Specifies a preference for using charging characteristics settings received from HLR or HSS, or those set by the SGSN or MME locally with the `local-value behavior` command.

- **hlr-hss-value** sets the call control profile to use charging characteristics settings received from HLR or HSS. This is the default preference.
- **local-value** sets the call control profile to use charging characteristics settings from the SGSN or MME only. If no charging characteristics are received from the HLR/HSS then local values will be applied.

**Usage**

Use this command to set the behavior for charging characteristic comings from either an HLR/HSS or locally from an MME/SGSN.

These charging characteristics parameters can also be set within an APN profile with the commands of the APN Profile configuration mode. For generation of M-CDRs, the parameters configured in this mode, Call Control Profile configuration mode, will prevail but for generation of S-CDRs the parameters configured in the APN Profile configuration mode will prevail.

The 12 behavior bits (of the `local-value behavior` keyword) can be used to enable or disable CDR generation.

**Example**

The following command specifies a rule not to generate charging records (CDRs) and sets the charging characteristics behavior bit to 2:

```
cc behavior-bit no-records 2
```
check-zone-code

Enables or disables the zone code checking mechanism.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-call-control-profile-profile_name)#

Syntax

[ no | remove ] check-zone-code

*no*
 Included with the command, this keyword disables the mechanism.

*remove*
 Included with the command, this keyword causes the removal of the current check-zone-code configuration and returns to the SGSN to the default where zone-code checking is enabled.

Usage
Use this command to enable/disable the zone-code checking function.

Example
Disable checking of the zone code:

*no check-zone-code*
ciphering-algorithm-gprs

Defines the order of preference of the ciphering algorithms.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Call Control Profile Configuration
configure > call-control-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-call-control-profile-profile_name)#

Syntax

ciphering-algorithm-gprs priority priority algorithm

remove ciphering-algorithm-gprs priority priority

remove
Delete the priority definition.

priority priority
Sets the order in which the algorithm will be selected for use.
priority is an integer from 1 to 4.

algorithm
Identifies the ciphering algorithm to be used.
algorithm is one of the following: gea0, gea1, gea2, gea3.

Usage
Define the order in which the ciphering algorithms are chosen for use. The command can be repeated to provide multiple definitions -- multiple priorities.

Example
Define gea1 as the third priority algorithm:

ciphering-algorithm-gprs priority 3 gea1
csfb

Configures circuit-switched fallback options. CSFB is the mechanism to move a subscriber from LTE to a legacy technology to obtain circuit switched voice or short message.

Product
MME

Privilege
Administrator

Mode
Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-call-control-profile-profile_name)#

Syntax

csfb { policy { not-allowed | not-preferred | sms-only | suppress-call-reject } | sms-only }

remove csfb { policy | sms-only }

remove csfb { policy | sms-only }

sms-only: Removes the SMS-only restriction allowing the UE to request voice and short message service (SMS) support for circuit-switched fallback (CSFB).

policy: Removes the configured policy.

policy { not-allowed | not-preferred | sms-only | suppress-call-reject }

not-allowed: Specifies that the CSFB function is not allowed for both voice and SMS.

not-preferred: Specifies that the MME returns a “not-preferred” response for CSFB services. The MME does not enforce this and a voice centric is allowed to make CSFB calls on a not-preferred case if it chooses to do so.

sms-only: Specifies that the CSFB function only supports SMS.

suppress-call-reject: Configures the MME to ignore a paging request for an SMS-only CS call for an attached UE and suppress the paging reject. This allows the MME to process SGs CS call SMS-only paging requests for Ultra Card users where the same MSISDN is allocated to different IMSIs. By default the MME will reject the paging request with a cause: SGSAP_SGS_CAUSE_MOBILE_TERMINATING_CSFB_REJECTED_BY_USER

sms-only

Specifies that the circuit-switched fallback function only supports SMS.

Important: This is a legacy keyword that remains to support earlier versions of the code. It operates identically to the policy sms-only keyword.
Usage

Use this command to restrict the circuit-switched fallback function to SMS only or no support for either voice or SMS.

Example

The following command enforces the SMS-only functionality for UEs requesting circuit-switched fallback:

   csfb policy sms-only
description

Allows you to enter a relevant descriptive string.

Product

MME
SAEGW
S-GW
SGSN

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-call-control-profile-profile_name)#

Syntax

description description

no description

description

Enter an alphanumeric string of 1 to 100 characters. The string may include spaces, punctuation, and case-sensitive letters if the string is enclosed in double quotation marks (" )..

no

Removes the description from the call control profile.

Usage

Define information that identifies this particularly call control profile.

Example

description “call-control-profile handling incoming from CallTell”
diameter-result-code-mapping

Maps an EMM (EPS Mobility Management) NAS (Network Access Server) cause code to a Diameter result code.

Product
MME

Privilege
Administrator

Mode
Exec > Global Configuration > Call Control Profile Configuration
configure > call-control-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-call-control-profile-profile_name)#

Syntax

diameter-result-code-mapping s6a diameter_result_code mme-emm-cause mme_emm_error_code

remove diameter-result-code-mapping s6a diameter_result_code

Removes the mapping for the specified Diameter result code.

s6a diameter_result_code

Specifies the Diameter result code to which the EMM NAS cause code is mapped.

diameter_result_code: Specify one of the supported Diameter result codes:

* diameter-authorization-rejected - s6a result code 5003. Default mapped EMM code: “No suitable cells in tracking area.”
* diameter-error-other - miscellaneous s6a error result code. Default mapped EMM code: “Network failure.”
* diameter-error-rat-not-allowed - s6a result code 5421. Default mapped EMM code: “No suitable cells in tracking area.”
* diameter-error-roaming-not-allowed - s6a result code 5004. Default mapped EMM code: “PLMN not allowed.”
* diameter-error-user-unknown - s6a result code 5001/5030. Default mapped EMM code: “EPS Service and non-EPS services not allowed.”
* diameter-invalid-avp-value - s6a result code 5004. Default mapped EMM code: “Network failure.”
* diameter-unable-to-comply - s6a result code 5012. Default mapped EMM code: “Network failure.”
* diameter-unknown-eps-subscription - s6a result code 5420. Default mapped EMM code: “No suitable cells in tracking area.”
Call Control Profile Configuration Mode

• **diameter-unsupported-feature** - s6a result code 5011. Default mapped EMM code: “Network failure.”

----

**mme-emm-cause mme_emm_error_code**

Specifies the EMM NAS cause code to be mapped to the Diameter result code.

*mme_emm_error_code:* Specify one of the supported EMM NAS error codes:

- **eps-non-eps-not-allowed:** Specifies that the EMM NAS cause code #8 “EPS services and non-EPS services not allowed” is to be mapped to the specified Diameter result code.
- **network-failure:** Specifies that the EMM NAS cause code #17 “Network failure” is to be mapped to the specified Diameter result code.
- **no-suitable-cell-in-tracking-area:** Specifies that the EMM NAS cause code #15 “No suitable cells in tracking area” is to be mapped to the specified Diameter result code.
- **plmn-not-allowed:** Specifies that the EMM NAS cause code #11 “PLMN not allowed” is to be mapped to the specified Diameter result code.
- **roaming-not-allowed-in-this-tracking-area:** Specifies that the EMM NAS cause code #13 “Roaming not allowed in this tracking area” is to be mapped to the specified Diameter result code.
- **tracking-area-not-allowed:** Specifies that the EMM NAS cause code #12 “Tracking area not allowed” is to be mapped to the specified Diameter result code.

----

**Usage**

Use this command to map a selected EMM NAS cause code to a specific Diameter result code.

**Example**

The following command maps the EMM NAS cause code “Roaming not allowed in this tracking area” to the Diameter result code “S6a Diameter error RAT not allowed”:

```
diameter-result-code-mapping s6a diameter-error-rat-not-allowed mme-emm-cause roaming-not-allowed-in-this-tracking-area
```
**direct-tunnel**

Allows direct tunneling if direct tunneling is supported by the destination node.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Call Control Profile Configuration

`configure > call-control-profile profile_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

**Syntax**

```plaintext
direct-tunnel attempt-when-permitted
remove direct-tunnel
```

**Usage**

Use this command to enable the Direct-Tunnel feature. To ensure that direct tunnel is fully configured for support by the SGSN, check the settings for `direct-tunnel` in

- the APN profile -- from the Exec mode, use command: `show apn-profile <profile_name> all`
- the RNC (radio network controller) configuration -- from the Exec mode, use command: `iups-service <service_name> all`

**Important:** Direct tunneling must be enabled at both of these two points to allow direct tunneling for the MS/UE.

**Example**

The following command sets the configuration to instruct the SGSN to attempt to setup a direct tunnel if permitted at the destination node:

```plaintext
direct-tunnel attempt-when-permitted
```
**dns-ggsn**

Defines the context to be used to do DNS lookup for GGSNs.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Call Control Profile Configuration

```
configure > call-control-profile profile_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

**Syntax**

```
dns-ggsn context ctxt_name

no dns-ggsn context ctxt_name
```

*no*

Removes the dns-ggsn configuration from this call control profile.

```
context ctxt_name
```

Specifies the context to be used to do DNS lookup for GGSNs as an alphanumeric string of 1 through 64 characters.

**Usage**

Use this command to define the context to be used to do DNS lookup to find the GGSN address.

**Example**

```
dns-ggsn context sgsn1
```
dns-sgsn

Identifies the context to be used to do DNS to find an SGSN address.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Call Control Profile Configuration

```bash
configure > call-control-profile profile_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

**Syntax**

```
[ no ] dns-sgsn context ctxt_name
```

- **no**
  - Removes the dns-sgsn configuration from this call control profile.

- **context ctxt_name**
  - Identify the context where the DNS client is configured to send the DNS query to get the peer SGSN address.
  - **context_name**: Enter a string of 1 to 79 alphanumeric characters to identify the context.
  - This configuration would override any similar configuration for `dns-sgsn context` in the SGTP service configuration.

**Usage**

Use this command to configure the context ID for the SGSN address that will be used to do the DNS lookup.

**Example**

Configure context `sgsn1` for DNS lookup:

```
dns-sgsn context sgsn1
```
**dns-pgw**

Defines the context to be used to do DNS lookup for P-GWs.

**Product**

MME
SGSN

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Call Control Profile Configuration  
*configure > call-control-profile profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

**Syntax**

```
[ remove ] dns-pgw context ctxt_name
```

- **remove**
  
  Deletes this definition from the call control profile.

- **context ctxt_name**
  
  Specifies the context to be used to do DNS lookup for P-GWs as an alphanumeric string of 1 through 64 characters.

  On the S4-SGSN, if the interface selected for a UE is S4 and if there is no DNS-PGW context configured under a call control profile, then by default the system will look for the DNS client in the context where the eGTP service is defined. If the interface selected for a UE is Gn-Gp and if there is no **dns-pgw context** configured in a call control profile, then by default the S4-SGSN will look for the DNS client in the context where the SGTP service is configured for selecting a co-located PGW/GGSN if:

  - the UE is EPC capable and,

    - **apn-resolve-dns-query snaptr** is configured in an APN profile using **APN Profile Configuration Mode**.

  If the **dns-pgw context** is deleted with the **remove** option, the S4-SGSN chooses the DNS client from the context where the eGTP service is configured.

**Usage**

Use this command to configure the context ID for the DNS lookup.

**Example**

```
dns-pgw context pgw1
```
**dns-sgw**

Defines the context to be used to do DNS lookup for S-GWs.

**Product**
MME  
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Call Control Profile Configuration  
configure > call-control-profile profile_name

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

**Syntax**

```
[ remove ] dns-sgw context ctxt_name
```

- **remove**
  Deletes this definition from the call control profile.

- **context ctxt_name**
  Specifies the context to be used to do DNS lookup for S-GWs as an alphanumeric string of 1 through 64 characters.
  This command must be used to configure DNS client settings when using dynamic S-GW selection where the tai-mgmt-db has been associated with a call-control-profile.
  On the S4-SGSN, this specifies the name of the context where the DNS client is configured that will be used for DNS resolution of S-GWs. If **dns-sgw context** is not specified, the S4-SGSN uses the DNS client configured in the context where the eGTP service is configured to query the S-GW DNS address.

**Usage**

Use this command to configure the context ID for the DNS lookup.

**Example**

```
dns-sgw context sgw1
```
**encryption-algorithm-lte**

Defines the priorities for using the encryption algorithms.

**Product**

MME

**Privilege**

Administrator

**Mode**

Exec > Global Configuration > Call Control Profile Configuration

```plaintext
configure > call-control-profile profile_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

**Syntax**

```plaintext
encryption-algorithm-lte priority1 128-eea { 0 | 1 | 2 } priority2 128-eea { 0 | 1 | 2 } priority3 128-eea { 0 | 1 | 2 }
```

```plaintext
remove encryption-algorithm-lte
```

**Usage**

Set the order or priority in which the MME will select a 128-EEA algorithm for use. All three priorities must be set or the definition is invalid. The command can be re-entered to change the priorities without removing the configuration.

**Example**

Configure 128-EEA2 as first priority encryption algorithm:

```plaintext
encryption-algorithm-lte priority1 128-eea 2 priority2 128-eea 0 priority3 128-eea 1
```
encryption-algorithm-umts

Defines the priorities for using the encryption algorithms.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Call Control Profile Configuration

`configure > call-control-profile profile_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

**Syntax**

```
encryption-algorithm-umts { uea0 | uea1 | uea2 } [ then-uea# | then-uea# ]
```

```
no encryption-algorithm-lte
```

**Usage**

Set the order or priority in which the SGSN will select a UEA algorithm for use. It is not necessary to define priorities for all three priority levels. The command can be re-entered to change the priorities without removing the configuration.

**Example**

Configure algorithm UEA2 as the first priority encryption algorithm with no others to be considered:

```
encryption-algorithm-umts uea2
```
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
equivalent-plmn

Configures the definition for an equivalent public land mobile network identifier (PLMN ID) and the preferred radio access technology (RAT). This is a list of PLMNs which should be considered by the mobile as equivalent to the visited PLMN for cell reselection and network selection. When configured, the equivalent PLMN list will be sent to the UE in NAS ATTACH ACCEPT / TAU ACCEPT messages (up to 15 PLMNs in each message).

Product
MME
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Call Control Profile Configuration
configure > call-control-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-call-control-profile-profile_name)#

Syntax

equivalent-plmn radio-access-technology { 2G | 3g | 4g | any } plmnid mcc mcc_number mnc mnc_number priority priority

no equivalent-plmn radio-access-technology { 2G | 3g | any } plmnid mcc mcc_number mnc mnc_number

no

Removes the equivalent-PLMN configuration from this call control profile.

radio-access-technology { 2G | 3g | 4g | any }

Identify the RAT type of the equivalent PLMN:
- 2G: 2nd generation
- 3G: 3rd generation
- 4G: 4th generation
- any: Any RAT

plmnid mcc mcc_number mnc mnc_number

- mcc: Specifies the mobile country code (MCC) portion of the PLMN ID. The number can be any integer between 100 and 999.
- mnc: Specifies the mobile network code (MNC) portion of the PLMN ID. The number can be any 2- or 3-digit integer between 00 and 999.
priority priority
Enter an integer between 1 and 15 with the highest priority assigned to the integer of the lowest numeric value.

Usage
Use the command to identify an ‘equivalent PLMN’ and assign it a priority to define the preferred equivalent PLMN to be used. This command can be entered multiple times to set priorities of usage.

Example
The following command sets up a secondary equivalent PLMN definition that allows for any RAT with a PLMN ID of MCC121.MNC767:

    equivalent-plmn radio_access_technology any plmnid mcc 121 mnc 767
    priority 2
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Use this command to return to the parent configuration mode.
gmm information-in-messages

Provides the configuration to include the information in messages for the GPRS mobility management (GMM) parameters.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-call-control-profile-profile_name)#

Syntax

gmm information-in-messages access-type { { gprs | umts } [ network-name { full-text name | short-text name } ] [ send-after { attach | rau } ] }

[ default | no ] gmm { information-in-messages access-type { gprs | umts }

no
Disables the GMM configuration from this call control profile.

default
Sets up a GMM configuration with system default values.

access-type

Must select one of the following options:
• gprs - General Packet Radio Service network
• umts - Universal Mobile Telecommunications System network

After selecting the access-type, an additional parameter can be configured:
• network-name: identifies the network name in either short text or full text.
• send-after: configures the information in message to send after attachment or Routing Area Update (RAU).

network-name { full-text name | short-text name }

This keyword provides the option to add the network name to the message. The network name will in full text or short text. Possible options are:
• full-text name: Indicate the network name in full text
• short-text name: Indicate the network name in short text
send-after{ attach | rau }

This keyword configures the information in message to send after attachment or RAU message. Possible options are:

- **attach**: Information sent after attachment
- **rau**: Information sent after routing area update

**Usage**

Use this command to configure identifying information about the network that will be included in GMM messages.

**Example**

Set default settings for calls coming from 2.5G networks:

```
default gmm information-in-messages access-type gprs
```
gmm retrieve-equipment-identity

Configures the International Mobile Equipment Identity (IMEI) or software version (SV) retrieval and validation procedure.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile profile_name

Entering the above command sequence results in the following prompt:

[local] host_name(config-call-control-profile-profile_name)#

Syntax

```
gmm retrieve-equipment-identity { imei | imeisv [ unciphered ] [ thenimei ] } [ verify-equipment-identity [ deny-greylisted ] ]

[ no | default ] gmm retrieve-equipment-identity
```

no

Disables the equipment identity retrieval procedure configured for this call control profile.

default

Sets the default action for equipment identity retrieval (EIR) procedure:

- **retrieve-equipment-identity**: Default action is disabled - no retrieval of IMEI/IMEI-SV
- **verify-equipment-identity**: Default action is disabled - no verification with Equipment Identity Register (EIR)

**equipment-identity-type**

Default: disabled

Indicates the type of equipment identification, with the possible values:

- **imei**: International Mobile Equipment Identity
- **imeisv**: International Mobile Equipment Identity - Software Version

**imei**

Indicates the equipment identity retrieval type to International Mobile Equipment Identity (IMEI). IMEI is a unique 15-digit number consisting of a TAC (Technical Approval Code), a FAC (Final Assembly Code), an SNR (Serial Number), and a check digit.
Call Control Profile Configuration Mode

**gmm retrieve equipment identity**

<table>
<thead>
<tr>
<th>imeisv [ unciphered ] [ thenimei ]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Indicates the equipment identity retrieval type to IMEI with software version (SV). IMEI with SV is a unique 16-digit number consisting of a TAC (Technical Approval Code), a FAC (Final Assembly Code), an SNR (Serial Number), and a 2-digit software version number.</td>
</tr>
<tr>
<td><strong>unciphered</strong>: This optional keyword enables the unciphered retrieval of IMEI-SV. If this option is enabled the retrieval procedure will get IMEISV (if auth is still pending, get as part of Authentication and Ciphering Response otherwise, via explicit Identification Request after Security Mode Complete).</td>
</tr>
<tr>
<td><strong>thenimei</strong>: This optional keyword enables the retrieval of software version number before the IMEI. If this option is enabled the equipment identity retrieval procedure will get IMEISV on secured link (after Security mode procedure via explicit GMM Identification Request), and if MS is not having IMEISV (responded with NO Identity), SGSN will try to get IMEI.</td>
</tr>
<tr>
<td>If no other keyword is provided, imeisv will get IMEISV on a secured link (after a Security mode procedure via explicit GMM Identification Request).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>verify-equipment-identity [ deny-greylisted ]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default: disabled</td>
</tr>
<tr>
<td>This keyword enables the equipment identity validation and validates the equipment identity against the EIR.</td>
</tr>
<tr>
<td><strong>deny-greylisted</strong>: This keyword fine-tunes the configuration and enables the restriction to the user having mobile equipment with an IMEI in the EIR grey list.</td>
</tr>
</tbody>
</table>

**Usage**

Use this command to enable and configure the procedures for mobile equipment identity retrieval and validation from the EIR identified in the MAP Service Configuration mode.

**Example**

The following command enables the SGSN to send "check IMEI" messages to the EIR:

```
gmm retrieve-equipment-identity imei verify-equipment-identity
```
gs-service

Associates the context of a Gs service interface with this call control profile.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Call Control Profile Configuration
configure > call-control-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-call-control-profile-profile_name)#

Syntax

gs-service gs_srvc_name context ctx_name

no gs-service svc_name

no
Removes/disassociates the named Gs service from the call control profile.

gs-service gs_srvc_name

Specifies the name of a specific Gs service for which to display information. gs_srvc_name is the name of a configured Gs service expressed as an alphanumeric string of 1 through 63 characters that is case sensitive.

context ctx_name

Specifies the specific context name where Gs service is configured. If this keyword is omitted, the named Gs service must exist in the same context as the GPRS/SGSN service. ctx_name is name of the configured context of Gs service expressed as an alphanumeric string from 1 through 63 characters that is case sensitive.

Usage
Use this command to associate a specific Gs service interface with this GPRS service instance.

Important: A Gs service can be used with multiple SGSN and/or GPRS service.

Example

The following command associates a Gs service instance named stargs1, which is configured in context named star_ctx, with a call control profile:

    gs-service stargs1 context star_ctx
gtp send

Configures which information elements (IE) the SGSN sends in GTP messages. These are required by the GGSN.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Call Control Profile Configuration
    configure > call-control-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-call-control-profile-profile_name)#

Syntax

```
```

```
remove gtp send { imeisv | ms-timezone | rai | rat | uli }
```

```
no gtp send
```

---

remove

Removes the specified GTP send definition from the system configuration.

---

no

Disables the specified GTP send configuration.

---

imeisv

Instructs the SGSN to include the IMEISV (International Mobile Equipment Identity with Software Version) of the mobile when sending GTP messages of the type Create PDP Context Request.
By default, this function is disabled.

---

derive-imeisv-from-imei

This is a filter for the imeisv keyword. It allows the operator to configure the SGSN to send IMEI to the GGSN as IMEI-SV.
This filter instructs the SGSN to add four 1s (1111) to the final semi-octet of the CPCQ (Create PDP Context Request) message which enables the SGSN to deduce the IMEI-SV value from the IMEI. If this filter is used, then IMEI is also sent as IMEI-SV when the gmm retrieve-equipment-identity command is configured.
**ms-timezone**

Instructs the SGSN to include this IE in GTP messages of the type Create PDP Request and Update PDP Context Request. This IE specifies the offset between universal time and local time, where the MS currently resides, in 15-minute steps.

This IE is sent by default.

---

**rai**

Configures the SGSN to include the Routing Area Identity (RAI) of the SGSN in the following situations:

- 2G new SGSN RAU
- 3G new SGSN SRNS
- 2G -> 3G HO (only if PLMN Id has changed)
- 3G -> 2G HO (only if PLMN Id has changed)
- multiple IUPS service RAU (only if PLMN Id has changed)
- multiple GPRS service RAU (only if PLMN Id has changed)
- 3G new SGSN RAU (change in behavior)
- 3G primary and secondary PDP activation (change in behavior)
- 2G primary and secondary PDP activation (change in behavior)

Optionally, this keyword can be followed with the keyword selection for the PLMN - `use-local-plmn`.

---

**rat**

Specifies which radio access technology (RAT) is being used by the MS (GERAN, UTRAN, or GAN). Including this keyword instructs the SGSN to include this IE when sending GTP messages of the type Create PDP Request and Update PDP Context Request.

This IE is sent by default.

---

**uli**

Specifies the CGI (MCC, MNC, etc.) and SAI of the MS where it is registered. Including this keyword instructs the SGSN to include the IE when sending GTP messages of the type Create PDP Request and Update PDP Context Request.

This IE is not sent by default.

Optionally, this keyword can be followed with the keyword selection for the PLMN - `use-local-plmn`.

---

**Important:** Currently, the next 5 (five) keywords, are only used with parameters `rai` or `uli`.

---

**use-local-plmn**

This keyword selects the local PLMN when network is not shared.

---

**network-sharing**

This keyword is used to configure network-sharing.

---

**use-selected-plmn**

This keyword selects the Selected PLMN when network is shared.
**use-ue-plmn**

This keyword selects Selected PLMN for supporting UE and Common PLMN for non-supporting UE when network is shared.

**use-common-plmn**

This keyword selects the Common PLMN when network is shared.

**Usage**

Use this command to define a preferred set of information to include when GTP messages are sent. Repeat this command multiple times to enable or disable multiple options. This instruction will be implemented when the specific operator policy and call control profile are applied.

The PLMN value in RAI/ULI can be selected if 3G network-sharing is enabled.

**Example**

The following command series instructs the SGSN (1) not to send MS’ timezone IE, and (2) to identify the MS’ radio access technology info in the GTP messages:

```
no gtp send ms-timezone

gtp send rat
```

On executing the following command, ULI is sent and PLMN will be “use-selected-plmn” if network-sharing is enabled. If network-sharing is not enabled, PLMN will be “use-local-plmn”.

```
gtp send uli
```

On executing the following command, ULI is sent and PLMN will be “use-selected-plmn” if network-sharing is enabled. If network-sharing is not enabled, PLMN will be “use-local-plmn”.

```
gtp send uli use-local-plmn
```

On executing the following command, ULI is sent and PLMN will be “use-selected-plmn” if network-sharing is enabled. If network-sharing is not enabled PLMN will be “use-local-plmn”.

```
gtp send uli use-local-plmn network-sharing use-selected-plmn
```

On executing the following command, ULI is sent and PLMN will be “use-common-plmn” if network-sharing is enabled. If network-sharing is not enabled PLMN will be “use-local-plmn”.

```
gtp send uli use-local-plmn network-sharing use-common-plmn
```
gtpp

Enables secondary GTPP accounting for an S-GW call control profile. By default, secondary GTPP accounting is disabled.

Product
S-GW
SAEGW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Call Control Profile Configuration
configure > call-control-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-call-control-profile-profile_name)#

Syntax

gtpp secondary-group group_name [ accounting context ctx_name ]

no gtpp secondary-group

no

Disables secondary GTPP accounting.

secondary-group group_name

Enables secondary GTPP accounting and specifies a GTPP group name.

group_name must be an alphanumeric string of 1 through 63 characters.

accounting context ctx_name

Specifies the specific accounting context to be used for secondary GTPP accounting. If this keyword is omitted, source context will be used for secondary GTPP accounting.

ctx_name must be an alphanumeric string of 1 through 79 characters.

Usage

Use this command to enable or disable secondary GTPP accounting for an S-GW call control profile.

Example

The following command enables secondary GTPP accounting for an S-GW call control profile and specifies a GTPP group named gtpp-grp1:

    gtpp secondary-group gtpp-grp1
gtpu fast-path

Enables or disables the network processing unit (NPU) Fast Path support for NPU processing of GTP-U packets of user sessions at the NPU.

Product
SAEGW
SGSN
S-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Call Control Profile Configuration
configure > call-control-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-call-control-profile-profile_name)#

Syntax

[ remove ] gtpu fast-path

```
remove
Removes the NPU fast path functionality configuration from the call control profile.
```

Usage
Use this command to enable/disable the NPU processed fast-path feature for processing of GTP-U data packets received from GGSN/RNC or P-GW/eNodeB. This feature enhances the GTP-U packet processing by adding the ability to fully process and forward the packets through the NPU itself.

**Important:** When enabled/disabled, fast-path processing will be applicable only to new subscriber who establishes a PDP context after issuing this command (enabling GTP-U fast path). No existing subscriber session will be affected by this command.

Example

The following command enables the NPU fast path processing for all new subscribers’ session established with this call control profile:

```
gtpu fast-path
```
**gw-selection**

Configures the parameters controlling the gateway selection process.

**Product**
MME

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Call Control Profile Configuration

`configure > call-control-profile profile_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

**Syntax**

```
```

---

**remove gw-selection**

Deletes the gw-selection definition from the call control profile.

---

**co-location [ weight [ prefer { sgw | pgw } ] ]**

Selects "co-location" as the determining factor for gateway selection. Collocation should be configured for both P-GW and S-GW selection for collocation to function. If a collocated PGW/SGW node cannot be found, then topologically closest nodes are chosen next. Host names with both “topon” and “topoff” labels will be considered in collocation.

- **weight**: Enables weighted selection if there are multiple co-located pairs.
- **prefer { pgw | sgw }**: Configures which weight to be used for weighted selection.

---

**pgw weight**

Selects PDN-Gateway as the determining factor for gateway selection.

---

**sgw weight**

Selects Serving Gateway as the determining factor for gateway selection.

---

**topology [ weight [ prefer { sgw | pgw } ] ]**

Selects topology as the determining factor for gateway selection. Topological selection is done only during initial attach, and not used during S-GW relocation or additional-pdn-connection.

- **weight**: Enables weighted selection if there are multiple pairs with the same degree of topological closeness.
- **prefer { pgw | sgw }**: Configures which weight to be used for weighted selection.

---

**Usage**

Use this command to define the criteria for gateway selection.
Selection of a co-located gateway (GW) node or a topologically closer GW node is based on string comparison of canonical node names included in two or more sets of records received in DNS S-NAPTR query result. For comparison, the canonical node names are derived from the hostnames received in the DNS records. The hostnames must adhere to the following format:

```
<topon|topoff>.<single-label-interface-name>.<canonical-node-name>;
```

Where “topon” or “topoff” is a prefix of the hostname and indicates whether or not the canonical node name can be used for topology matching.

The table below lists the behaviors with various CLI options:

**Table 20. CLI Behavior Options**

<table>
<thead>
<tr>
<th>Option</th>
<th>Keyword Selected</th>
<th>Prefix in Hostname</th>
<th>Topological Match Nodes Selected</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>co-location</td>
<td>topon</td>
<td>Yes</td>
<td>Co-located nodes are selected if available as they are listed before topologically closer nodes in the DNS records.</td>
</tr>
<tr>
<td>2</td>
<td>co-location</td>
<td>topoff</td>
<td>Yes</td>
<td>Co-located nodes are selected if available as they are listed before topologically closer nodes in the DNS records.</td>
</tr>
<tr>
<td>3</td>
<td>topology</td>
<td>topon</td>
<td>Yes</td>
<td>Co-located nodes are selected if available as they are listed before topologically closer nodes in the DNS records.</td>
</tr>
<tr>
<td>4</td>
<td>topology</td>
<td>topoff</td>
<td>No</td>
<td>Nodes with prefix 'topoff' are ignored for topological matching purposes. If no nodes are present with 'topon' as prefix then nodes are selected independently based on Order/Priority mentioned in DNS Records.</td>
</tr>
<tr>
<td>5</td>
<td>co-location</td>
<td>neither</td>
<td>Yes</td>
<td>Will strip only the first label from hostname to fetch canonical node name for topology matching. Co-located nodes are selected if available as they are listed before topologically closer nodes in the DNS records.</td>
</tr>
<tr>
<td>6</td>
<td>topology</td>
<td>neither</td>
<td>No</td>
<td>No co-located node pair listing; topologically closer node listing used if available (Same behavior as defined for 4).</td>
</tr>
</tbody>
</table>

**Example**

The following command instructs the MME to determine gateway selection on the basis of topology:

```
gw-selection topology
```
idle-mode-signaling-reduction

Enables or disables the Idle-Mode-Signaling-Reduction (ISR) feature on the S4-SGSN.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Call Control Profile Configuration
configure > call-control-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-call-control-profile-profile_name)#

Syntax

[ remove ] idle-mode-signaling-reduction access-type [ gprs | umts ]

remove
Disables the ISR feature configuration from this call control profile.

idle-mode-signaling-reduction
Configures ISR for this call control profile.

access-type
Specifies the network access type for the ISR feature. Select one of the following options:
• gprs - General Packet Radio Service network. Specifies 2G network access support for the ISR feature. This option is only supported for Release 15.0 and beyond.
• umts - Universal Mobile Telecommunications System network. Specifies 3G network access support for the ISR feature.

Usage
Use this command to enable or disable the ISR feature on the S4-SGSN. Note that ISR is supported on the S4-SGSN only.
This command is available only if the Idle Mode Signaling Reduction license is enabled on the SGSN.
When 3G ISR is enabled, operators should set the ISR deactivation timer value sent by the S4-SGSN to the UE in Attach Accept and Routing Area Update Accept messages. Use the gmm T3323-timeout command in SGSN Service Configuration Mode to set the ISR deactivation timer value.
When 2G ISR is enabled, operators should set the implicit detach timeout value to use for 2G ISR. Use the gmm implicit_detach_timeout command in GPRS Service Configuration Mode.

Example

idle-mode-signaling-reduction access-type umts
**integrity-algorithm-lte**

 Specifies the order of preference for using an Integrity Algorithm.

**Product**
MME

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Call Control Profile Configuration  
`configure > call-control-profile profile_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

**Syntax**

```
integrity-algorithm-lte priority1 { 128-eia0 | 128-eia1 | 128-eia2 } priority2 128-eia { 0 | 1 | 2 } priority3 128-eia { 0 | 1 | 2 }
```

**Usage**
Set the order or priority in which the MME will select an integrity algorithm for use. All three priorities must be set or the definition is invalid. The command can be re-entered to change the priorities without removing the configuration.

**Example**
Configure 128-EIA0 as first priority integrity algorithm:

```
integrity-algorithm-lte priority1 128-eia 0 priority2 128-eia 2 priority3 128-eia 1
```
integrity-algorithm-umts

Configures the order of preference for the Integrity Algorithm used for 3G.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-call-control-profile-profile_name)#

Syntax

integrity-algorithm-umts type then_type

default integrity-algorithm-umts

<table>
<thead>
<tr>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the default preference based on system defaults.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creates a configuration defining an order of preference. Enter one or more of the following options in the order of preference:</td>
</tr>
<tr>
<td>• uia1 - uia1 Algorithm</td>
</tr>
<tr>
<td>• uia2 - uia2 Algorithm</td>
</tr>
</tbody>
</table>

Usage
Use this command to determine which integrity algorithm is preferred 3G. This command is configured in tandem with the algorithm type for encryption-algorithm-umts command.

Example

default integrity-algorithm-umts
**Ics-mo**

This command enables/disables mobile-originating Location Requests by access-type when Location Services functionality is enabled.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Call Control Profile Configuration
configure > call-control-profile profile_name

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

**Syntax**

```
lcs-mo { allow | restrict } access-type { gprs | umts }
```

**Example**
Use the following command to disable or disallow mobile-originating Location Requests within a GPRS network:

```
lcs-mo restrict access-type GPRS
```
**lcs-mt**

This command enables/disables mobile-terminating Location Requests by access-type when Location Services functionality is enabled.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Call Control Profile Configuration

`configure > call-control-profile profile_name`

Entering the above command sequence results in the following prompt:

```bash
[local] host_name(config-call-control-profile-profile_name)#
```

**Syntax**

```
lcs-mt { allow | restrict } access-type { gprs | umts }
```

- **allow**
  
  Enables mobile-terminating Location Requests. This is the default state when Location Services are enabled.

**Usage**

This command ties Location Service functionality to a call-control profile by IMSI so that Location Services can optionally be determined by an operator policy for incoming calls.

**Example**

Use the following command to disable or disallow mobile-terminating Location Requests within a UMTS network:

```
lcs-mt restrict access-type umts
```
### lcs-ni

This command enables/disables network-initiated Location Requests by access-type when Location Services functionality is enabled.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Call ControlProfile Configuration

```plaintext
configure > call-control-profile profile_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

**Syntax**

```plaintext
lcs-ni { allow | restrict } access-type { gprs | umts }
```

- **allow**
  Enables network-initiated Location Requests. This is the default state when Location Services are enabled.

**Usage**

This command ties Location Service functionality to a call-control profile by IMSI so that Location Services can optionally be determined by an operator policy for incoming calls.

**Example**

Use the following command to enable or allow network-initiated Location Requests within a UMTS network if this function has been restricted previously:

```plaintext
lcs-ni allow access-type umts
```
local-cause-code-mapping apn-mismatch

Configures the reject cause code to send to a UE when an APN mismatch occurs.

Product
MME

Privilege
Administrator

Mode
Exec > Global Configuration > Call Control Profile Configuration
configure > call-control-profile profile_name

Entering the above command sequence results in the following prompt:
[local]host_name(config-call-control-profile-profile_name)#

Syntax


remove local-cause-code-mapping apn-mismatch

remove local-cause-code-mapping apn-mismatch

Removes the configured cause code mapping.


Specifies the EPS Mobility Management (EMM) cause code to return when an APN mismatch occurs.

• eps-service-not-allowed-in-this-plmn
• esm-failure esm-cause-code unknown-apn - Default.
  For the esm-failure cause code only, the unknown-apn ESM code is also reported to the UE.
  • no-suitable-cell-in-tracking-area
  • plmn-not-allowed
  • roaming-not-allowed-in-this-tracking-area
  • tracking-area-not-allowed

Usage

Use this command to configure the cause code returned to a UE when an APN mismatch occurs, such as when an APN is present in the HSS subscription but the HSS subscription for this IMSI has other APNs present in the subscription.
Related Commands:
If a condition is specified in both the call-control-profile associated with a call, and also the mme-service, the cause configured for the call-control-profile will be signalled to the UE. See also the `local-cause-code-mapping` command in the mme-service configuration mode. This command is described in the MME Service Configuration Mode Commands chapter.

Example
The following command maps the “PLMN not allowed” cause code to the APN mismatch condition:

```
local-cause-code-mapping apn-mismatch emm-cause-code plmn-not-allowed
```
local-cause-code-mapping apn-not-subscribed

Gives the operator the option to specify the local cause-code mapping when the UE-requested APN is not subscribed.

Product
MME

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Call Control Profile Configuration
configure > call-control-profile profile_name
Entering the above command sequence results in the following prompt:

[local]host_name(config-call-control-profile-profile_name)#

Syntax

local-cause-code-mapping apn-not-subscribed esm-cause-code requested-service-option-not-subscribed

remove local-cause-code-mapping apn-not-subscribed

remove

Deletes the local cause code mapping from the configuration.

Usage
The operator can specify "Requested-Option-Not-Subscribed" cause code value #33 will be sent in the Reject message when the PDN Connectivity Request is rejected because no subscription is found. If the command option is not configured, then by default the MME uses the cause code value #27 (Unknown or Missing APN) in standalone PDN Connectivity Reject message when the UE-requested APN is not subscribed. The new keyword apn-not-subscribed is added to specify the local cause-code mapping when the UE-requested APN is not subscribed for that subscriber. If cause code mapping for apn-not-subscribed is explicitly configured with requested-service-option-not-subscribed in either the Call-Control-Profile or MME-Service configuration mode, then the new code "Requested-Option-Not-Subscribed" (cause-code #33) will be sent in the Reject message when the PDN Connectivity Request is rejected because no subscription is found.

Example
The following instructs the MME to use cause code #33 ("Requested-Option-Not-Subscribed") in place of the default #27 (Unknown or Missing APN):

    local-cause-code-mapping apn-not-subscribed esm-cause-code requested-service-option-not-subscribed
local-cause-code-mapping auth-failure

Configures the reject cause code to send to a UE when an authentication failure occurs.

Product
MME

Privilege
Administrator

Mode
Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-call-control-profile-profile_name)#

Syntax


remove local-cause-code-mapping auth-failure

remove local-cause-code-mapping auth-failure

Removes the configured cause code mapping.


Specifies the EPS Mobility Management (EMM) cause code to return when an authentication failure occurs.

*eps-service-not-allowed-in-this-plmn
*network-failure
*no-suitable-cell-in-tracking-area
*plmn-not-allowed
*roaming-not-allowed-in-this-tracking-area
*tracking-area-not-allowed

Usage

Use this command to configure the cause code returned to a UE when an authentication failure occurs. By default, the MME sends the UE the #3 - Illegal MS cause code when encountering an authentication failure. This condition occurs for TAU and ATTACH procedures in the following cases:

* The Authentication response from the UE does not match the expected value in the MME.
* Security Mode Reject is sent by the UE.
• The UE responds to any identity request with a different type of identity (for example, the MME could query for IMSI and the UE responds with IMEI).

The following are not considered for the authentication failure condition:

• HSS returning a result code other than SUCCESS.
• HSS not available.
• EIR failures.
• UE not responding to requests.

Related Commands:
If a cause code mapping is specified in both the call-control-profile associated with a call, and also the mme-service, the cause configured for the call-control-profile will be signalled to the UE. See also the `local-cause-code-mapping` command in the mme-service configuration mode. This command is described in the MME Service Configuration Mode Commands chapter.

Example

The following command maps the “network-failure” cause code to the authentication failure condition:

```
local-cause-code-mapping auth-failure emm-cause-code network-failure
```
local-cause-code-mapping congestion

Configures the reject cause code to send to a UE when a procedure fails due to a congestion condition.

Product
MME

Privilege
Administrator

Mode
Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-call-control-profile-profile_name)#

Syntax


remove local-cause-code-mapping congestion

remove local-cause-code-mapping congestion

Removes the configured cause code mapping.


Specifies the EPS Mobility Management (EMM) cause code to return when a UE requests access when the system is exceeding any of its congestion control thresholds.

• congestion - Default
  • eps-service-not-allowed-in-this-plmn
  • network-failure
  • no-suitable-cell-in-tracking-area
  • plmn-not-allowed
  • roaming-not-allowed-in-this-tracking-area
  • tracking-area-not-allowed
esm-cause-code { congestion | insufficient-resources | service-option-temporarily-out-of-order }

Specifies the EPS Session Management (ESM) cause code to return when a UE requests access when the system is exceeding any of its congestion control thresholds.

- congestion - Default
- insufficient-resources
- service-option-temporarily-out-of-order

Usage

Use this command to configure the cause code returned to a UE when a UE procedure fails due to a congestion condition on the MME.

Related Commands:

To set the cause codes for situations where a call control profile cannot be attached to a call (for example new-call restrictions, congestion during new call attempt, etc.), use the local-cause-code-mapping command in the mme-service configuration mode. This command is described in the MME Service Configuration Mode Commands chapter.

Example

The following command maps the “network failure” cause code to the congestion event:

   local-cause-code-mapping congestion emm-cause-code network-failure
local-cause-code-mapping ctxt-xfer-fail-mme

Configures the reject cause code to send to a UE when a UE context transfer failure from a peer MME occurs.

Product
MME

Privilege
Administrator

Mode
Exec > Global Configuration > Call Control Profile Configuration
configure > call-control-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-call-control-profile-profile_name)#

Syntax


remove local-cause-code-mapping ctxt-xfer-fail-mme

Removes the configured cause code mapping.


Specifies the EPS Mobility Management (EMM) cause code to return when a UE context transfer failure from a peer MME occurs.

• eps-service-not-allowed-in-this-plmn
• network-failure
• no-suitable-cell-in-tracking-area
• plmn-not-allowed
• roaming-not-allowed-in-this-tracking-area
• tracking-area-not-allowed

Usage

Use this command to configure the cause code returned to a UE when a UE context transfer failure from a peer MME occurs. By default, the MME sends the UE the #9 - MS identity cannot be derived by the network cause code for this condition.

After the peer node has been identified, the MME sends a Context Request to the peer node. If the peer node is an MME, and if the context transfer procedure fails, this condition is detected.
Related Commands:
If a cause code mapping is specified in both the call-control-profile associated with a call, and also the mme-service, the cause configured for the call-control-profile will be signalled to the UE. See also the `local-cause-code-mapping` command in the mme-service configuration mode. This command is described in the MME Service Configuration Mode Commands chapter.

Example
The following command maps the “network-failure” cause code to the context transfer failure from MME condition:

```plaintext
local-cause-code-mapping ctxt-xfer-fail-mme emm-cause-code network-failure
```
local-cause-code-mapping ctxt-xfer-fail-sgsn

Configures the reject cause code to send to a UE when a UE context transfer failure from a peer SGSN occurs.

Product
MME

Privilege
Administrator

Mode
Exec > Global Configuration > Call Control Profile Configuration
configure > call-control-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-call-control-profile-profile_name)#

Syntax


remove local-cause-code-mapping ctxt-xfer-fail-sgsn

remove local-cause-code-mapping ctxt-xfer-fail-sgsn

Removes the configured cause code mapping.


Specifies the EPS Mobility Management (EMM) cause code to return when a UE context transfer failure from a peer SGSN occurs.

*eps-service-not-allowed-in-this-plmn
*network-failure
*no-suitable-cell-in-tracking-area
*plmn-not-allowed
*roaming-not-allowed-in-this-tracking-area
*tracking-area-not-allowed

Usage

Use this command to configure the cause code returned to a UE when a UE context transfer failure from a peer SGSN occurs. By default, the MME sends the UE the #9 - MS identity cannot be derived by the network cause code when encountering this condition.

After the peer node has been identified, the MME sends a Context Request to the peer node. If the peer node is an SGSN, and if the context transfer procedure fails, this condition is detected.
Related Commands:

If a cause code mapping is specified in both the call-control-profile associated with a call, and also the mme-service, the cause configured for the call-control-profile will be signalled to the UE. See also the `local-cause-code-mapping` command in the mme-service configuration mode. This command is described in the MME Service Configuration Mode Commands chapter.

Example

The following command maps the “network-failure” cause code to the context transfer failure from SGSN condition:

```
local-cause-code-mapping ctxt-xfer-fail-sgsn emm-cause-code network-failure
```
**local-cause-code-mapping gw-unreachable**

Configures the reject cause code to send to a UE when a gateway (S-GW or P-GW) does not respond during an EMM procedure.

**Product**
MME

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Call Control Profile Configuration

```bash
configure > call-control-profile profile_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

**Syntax**

```bash
```

```bash
remove local-cause-code-mapping gw-unreachable [ attach | tau ]
```

Remove the configured cause code mapping.

```bash
```

Specifies the EPS Mobility Management (EMM) cause code to return when a gateway does not respond.

- `eps-service-not-allowed-in-this-plmn`
- `network-failure`
- `no-bearers-active`
- `no-suitable-cell-in-tracking-area`
- `plmn-not-allowed`
- `roaming-not-allowed-in-this-tracking-area`
- `tracking-area-not-allowed`

```bash
[ attach | tau ]
```

Optionally, the MME can return separate cause codes for Attach procedures and TAU procedures. This capability is available for any of the above EMM cause codes except `no-bearers-active`, which can only be defined for TAU procedures.
**Usage**

Use this command to configure the cause code returned to a UE when a gateway (S-GW or P-GW) does not respond during an EMM procedure.

**Defaults:**
Prior to StarOS 15.0 MR5, the MME sends the UE the #19 - **ESM Failure** cause code when encountering this condition.
In StarOS 15.0 MR5 and higher releases, the MME sends the UE the #19 - **ESM Failure** cause code for Attach procedures, and #40 - **NO-EPS-BEARER-CONTEXT-ACTIVATED** for TAU procedures.

**Related Commands:**
If a cause code mapping is specified in both the call-control-profile associated with a call, and also the mme-service, the cause configured for the call-control-profile will be signalled to the UE. See also the **local-cause-code-mapping** command in the mme-service configuration mode. This command is described in the *MME Service Configuration Mode Commands* chapter.

**Example**

The following command maps the “network-failure” cause code to the gateway unreachable condition:

```
local-cause-code-mapping gw-unreachable emm-cause-code network-failure
```
local-cause-code-mapping hss-unavailable

Configures the reject cause code to send to a UE when the HSS does not respond.

Product
MME

Privilege
Administrator

Mode
Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-call-control-profile-profile_name)#

Syntax


remove local-cause-code-mapping hss-unavailable

Removes the configured cause code mapping.


Specifies the EPS Mobility Management (EMM) cause code to return when the HSS does not respond.

*eps-service-not-allowed-in-this-plmn
*network-failure
*no-suitable-cell-in-tracking-area
*plmn-not-allowed
*roaming-not-allowed-in-this-tracking-area
*tracking-area-not-allowed

Usage

Use this command to configure the cause code returned to a UE when the HSS is unavailable. By default, the MME sends the UE the #17 - Network failure cause code when encountering this condition. This condition is detected in the following cases:

*HSS resolution fails in the MME.
*HSS does not respond in time.
The cause code configured for this condition will be signaled in TAU and ATTACH REJECT messages.

**Related Commands:**
If a cause code mapping is specified in both the call-control-profile associated with a call, and also the mme-service, the cause configured for the call-control-profile will be signalled to the UE. See also the `local-cause-code-mapping` command in the mme-service configuration mode. This command is described in the *MME Service Configuration Mode Commands* chapter.

**Example**
The following command maps the “tracking-area-not-allowed” cause code to the HSS unavailable condition:
```
local-cause-code-mapping hss-unavailable emm-cause-code tracking-area-not-allowed
```
local-cause-code-mapping map-cause-code

Configures the operator-preferred GMM reject cause code to send to a UE in response to some failures.

**Product**
SGSN

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Call Control Profile Configuration

```plaintext
configure > call-control-profile profile_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

**Syntax**

```plaintext
local-cause-code-mapping map-cause-code roaming-not-allowed gmm-cause-code gmm-cause
remove local-cause-code-mapping map-cause-code roaming-not-allowed
```

---

**remove**

Removes the specified, previously configured cause code mapping.

---

**roaming-not-allowed**

Instructs the SGSN to send a different GPRS mobility management (GMM) cause code to a UE when the UE’s access request is rejected due to map cause ‘roaming not allowed’. Specify one of the GMM cause codes listed below.

---

**gmm-cause-code**

Specifies the GPRS mobility management (GMM) cause code to return to a UE in access request Reject messages. Replacement cause code options include:

- `gprs-serv-and-non-gprs-serv-not-allowed`
- `gprs-serv-not-allowed`
- `gprs-serv-not-in-this-plmn`
- `location-area-not-allowed`
- `network-failure`
- `no-suitable-cell-in-this-la`
- `plmn-not-allowed`
- `roaming-not-allowed-in-this-la`
Usage

This command enables the operator to configure a preferred GMM cause code to return to the UE when a UE access request is rejected due to map-cause ‘roaming-not-allowed’.

Example

The following command maps network-failure as the GMM cause code to be included in an Access Reject sent to the UE when the UE is denied due to map-cause ‘roaming-not-allowed’:

```
local-cause-code-mapping map-cause-code roaming-not-allowed gmm-cause-code network-failure
```
local-cause-code-mapping no-active-bearers

Configures the reject cause code to send to a UE when the context received from a peer SGSN (during a TAU procedure) does not contain any active PDP contexts.

Product
MME

Privilege
Administrator

Mode
Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-call-control-profile-profile_name)#

Syntax


remove local-cause-code-mapping no-active-bearers

remove local-cause-code-mapping no-active-bearers

Removes the configured cause code mapping.


Specifies the EPS Mobility Management (EMM) cause code to return when no active PDP context exists.

• eps-service-not-allowed-in-this-plmn
• network-failure
• no-bearers-active
• no-suitable-cell-in-tracking-area
• plmn-not-allowed
• roaming-not-allowed-in-this-tracking-area
• tracking-area-not-allowed
Usage
Use this command to configure the cause code returned to a UE when the context received from a peer SGSN (during a TAU procedure) does not contain any active PDP contexts. By default, the MME sends the UE the #40 - No PDP context activated cause code when encountering this condition.

Related Commands:
If a cause code mapping is specified in both the call-control-profile associated with a call, and also the mme-service, the cause configured for the call-control-profile will be signalled to the UE. See also the local-cause-code-mapping command in the mme-service configuration mode. This command is described in the MME Service Configuration Mode Commands chapter.

Example
The following command maps the “plmn-not-allowed” cause code to the no active bearer condition:

    local-cause-code-mapping no-active-bearers emm-cause-code plmn-not-allowed
local-cause-code-mapping peer-node-unknown

Configures the reject cause code to send to a UE when peer node resolution is not successful.

**Product**
MME

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Call Control Profile Configuration

`configure > call-control-profile profile_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

**Syntax**

```
```

```
remove local-cause-code-mapping peer-node-unknown
```

Removes the configured cause code mapping.

```
```

Specifies the EPS Mobility Management (EMM) cause code to return when the peer node resolution is not successful.

- `eps-service-not-allowed-in-this-plmn`
- `network-failure`
- `no-suitable-cell-in-tracking-area`
- `plmn-not-allowed`
- `roaming-not-allowed-in-this-tracking-area`
- `tracking-area-not-allowed`

**Usage**

Use this command to configure the cause code returned to a UE when peer node resolution is not successful.

By default, the MME sends the UE the #9 - MS identity cannot be derived by the network cause code when encountering this condition.

During processing of a TAU REQUEST, the resolution of a peer MME that had allocated the temporary identity that is signaled to the UE takes several steps in the MME. This resolution can be done based on DNS...
or based on local configuration. This condition occurs when all mechanisms for peer node resolution are done with no success.

**Related Commands:**
If a cause code mapping is specified in both the call-control-profile associated with a call, and also the mme-service, the cause configured for the call-control-profile will be signalled to the UE. See also the `local-cause-code-mapping` command in the mme-service configuration mode. This command is described in the `MME Service Configuration Mode Commands` chapter.

**Example**
The following command maps the “plmn-not-allowed” cause code to the peer node unknown condition:

```
local-cause-code-mapping peer-node-unknown emm-cause-code plmn-not-allowed
```
local-cause-code-mapping pgw-selection-failure

Configures the reject cause code to send to a UE when a failure occurs during P-GW selection.

Product
MME

Privilege
Administrator

Mode
Exec > Global Configuration > Call Control Profile Configuration
configure > call-control-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-call-control-profile-profile_name)#

Syntax


remove local-cause-code-mapping pgw-selection-failure

Removes the configured cause code mapping.


Specifies the EPS Mobility Management (EMM) cause code to return when a failure occurs during P-GW selection.

• eps-service-not-allowed-in-this-plmn
• network-failure
• no-suitable-cell-in-tracking-area
• plmn-not-allowed
• roaming-not-allowed-in-this-tracking-area
• tracking-area-not-allowed

Usage

Use this command to configure the cause code returned to a UE when a failure occurs during P-GW selection. By default, the MME sends the UE the #17 - Network failure cause code when encountering this condition.
Related Commands:

If a cause code mapping is specified in both the call-control-profile associated with a call, and also the mme-service, the cause configured for the call-control-profile will be signalled to the UE. See also the `local-cause-code-mapping` command in the mme-service configuration mode. This command is described in the MME Service Configuration Mode Commands chapter.

Example

The following command maps the “plmn-not-allowed” cause code to the P-GW selection failure condition:

```
local-cause-code-mapping pgw-selection-failure emm-cause-code plmn-not-allowed
```
local-cause-code-mapping restricted-zone-code

Configures the reject cause code to send to a UE when a UE requests access to a restricted zone.

**Product**  
MME

**Privilege**  
Administrator

**Mode**  
Exec > Global Configuration > Call Control Profile Configuration  
`configure > call-control-profile profile_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

**Syntax**

```plaintext
local-cause-code-mapping restricted-zone-code emm-cause-code { eps-service-not-allowed-in-this-plmn | no-suitable-cell-in-tracking-area | plmn-not-allowed | roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed }
remove local-cause-code-mapping restricted-zone-code
```

**Usage**

Use this command to configure the cause code returned to a UE when a UE requests access to a restricted zone.

**Related Commands:**

To set the cause codes for situations where a call control profile cannot be attached to a call (for example new-call restrictions, congestion during new call attempt, etc.), use the `local-cause-code-mapping`
command in the mme-service configuration mode. This command is described in the *MME Service Configuration Mode Commands* chapter.

**Example**

The following command maps the “PLMN not allowed” cause code to the restricted zone code event:

```
local-cause-code-mapping restricted-zone-code emm-cause-code plmn-not-allowed
```
local-cause-code-mapping sgw-selection-failure

Configures the reject cause code to send to a UE when a failure occurs during S-GW selection.

Product
MME

Privilege
Administrator

Mode
Exec > Global Configuration > Call Control Profile Configuration

```
configure > call-control-profile profile_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

Syntax

```
```

```
remove local-cause-code-mapping sgw-selection-failure
```

Removes the configured cause code mapping.

```
```

Specifies the EPS Mobility Management (EMM) cause code to return when a failure occurs during S-GW selection.

- `eps-service-not-allowed-in-this-plmn`
- `network-failure`
- `no-suitable-cell-in-tracking-area`
- `plmn-not-allowed`
- `roaming-not-allowed-in-this-tracking-area`
- `tracking-area-not-allowed`

Usage

Use this command to configure the cause code returned to a UE when a failure occurs during S-GW selection. By default, the MME sends the UE the #17 - Network failure cause code when encountering this condition.
**Related Commands:**

If a cause code mapping is specified in both the call-control-profile associated with a call, and also the mme-service, the cause configured for the call-control-profile will be signalled to the UE. See also the `local-cause-code-mapping` command in the mme-service configuration mode. This command is described in the *MME Service Configuration Mode Commands* chapter.

**Example**

The following command maps the “plmn-not-allowed” cause code to the S-GW selection failure condition:

```
local-cause-code-mapping sgw-selection-failure emm-cause-code plmn-not-allowed
```
local-cause-code-mapping vlr-down

Configures the cause code to send in a ATTACH ACCEPT or TAU ACCEPT to a UE that attachment to the VLR has failed because a VLR down condition is present.

**Product**
MME

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Call Control Profile Configuration
configure > call-control-profile profile_name

Entering the above command sequence results in the following prompt:

[local] host_name(config-call-control-profile-profile_name)#

**Syntax**

```plaintext
local-cause-code-mapping vlr-down emm-cause-code { congestion | cs-domain-unavailable | imsi-unknown-in-hlr | msc-temp-unreachable | network-failure }
```

```plaintext
remove local-cause-code-mapping vlr-down
```

Removes the configured cause code mapping.

```plaintext
vlr-down emm-cause-code  emm_cause_code
```

Specifies the EPS Mobility Management (EMM) cause code to return when a VLR down condition is present.

*emm_cause_code* must be one of the following options:

- congestion
- cs-domain-unavailable
- imsi-unknown-in-hlr
- msc-temp-unreachable- Default.
- network-failure

**Usage**

Use this command to configure the cause code returned to a UE when a VLR down condition is present.

**Related Commands:**

To set the cause codes for situations where a call control profile cannot be attached to a call (for example new-call restrictions, congestion during new call attempt, etc.), use the **local-cause-code-mapping**
command in the mme-service configuration mode. This command is described in the *MME Service Configuration Mode* Commands chapter.

**Example**

The following command maps the “network failure” EMM cause code to the VLR down condition:

```
local-cause-code-mapping vlr-down emm-cause-code network-failure
```
local-cause-code-mapping vlr-unreachable

Configures the cause code to send in a ATTACH ACCEPT or TAU ACCEPT to a UE that attachment to the VLR has failed because a VLR unreachable condition is present.

**Product**
MME

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Call Control Profile Configuration
configure > call-control-profile profile_name

Entering the above command sequence results in the following prompt:

`[local]host_name(config-call-control-profile-profile_name)#`

**Syntax**

```
local-cause-code-mapping vlr-unreachable emm-cause-code { congestion | cs-domain-unavailable | imsi-unknown-in-hlr | msc-temp-unreachable | network-failure }
```

```
remove local-cause-code-mapping vlr-unreachable
```

**Usage**
Use this command to configure the cause code returned to a UE when a VLR unreachable condition is present.

**Related Commands:**
To set the cause codes for situations where a call control profile cannot be attached to a call (for example new-call restrictions, congestion during new call attempt, etc.), use the `local-cause-code-mapping`
command in the mme-service configuration mode. This command is described in the *MME Service Configuration Mode* Commands chapter.

**Example**

The following command maps the “network failure” EMM cause code to the VLR unreachable condition:

```
local-cause-code-mapping vlr-unreachable emm-cause-code network-failure
```
location-area-list

Defines the location area list to allow or restrict services in the specified location areas identified by location area code (LAC).

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Call Control Profile Configuration

`configure > call-control-profile profile_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

**Syntax**

```
location-area-list instance instance area-code area_code [ area_code * ]
```

```
no location-area-list instance instance[ area-code area_code ]
```

**Usage**

Use the command multiple times to configure multiple LAC lists or to modify the list.

**Example**

The following command creates a location area list for a single area code:

```
location-area-list instance 1 area-code 514
```

This command creates a second location area list for with multiple area codes - all separated by a single blank space:

```
location-area-list instance 2 area-code 514 62552 32 1513
```
The next command corrects an area code mistake (327 not 32) made in the previous configuration:

```
location-area-list instance 1 area-code 514 62552 327 1513
```
location-reporting

Enable 3G/2G Location Change Reporting feature on the SGSN.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Call Control Profile Configuration
 configuring > call-control-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-call-control-profile-profile_name)#

Syntax

[ remove ] location-reporting access-type { gprs | umts }

remove

If the remove keyword is included in the command, then the location change reporting feature is disabled.

access-type type

Defines the type of subscriber access which is to reported for location changes.

* gprs - 2G
* umts - 3G

Usage

Use the command multiple times to configure both types of access types.

This command enables the 3G/2G Location Change Reporting feature which notifies the GGSN whenever one of the following changes for a UE:

* the serving cell global identity (CGI), or
* the service area identity (SAI), or
* the routing area identity (RAI).

Example

The following command enables location change reporting to a GGSN for 3G subscribers:

   location-reporting access-type umts

This command disables location change reporting that has been enabled for 2G subscribers:

   remove location-reporting access-type gprs
**lte-zone-code**

Configures the enforcement of allowed or restricted zone code lists and associates an EPS Mobility Management (EMM) cause code to rejected attach attempts.

**Product**
MME

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Call Control Profile Configuration

```
configure > call-control-profile profile_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

**Syntax**

```
lte-zone-code [ allow | restrict ] { emm-cause-code { eps-service-not-allowed-in-this-plmn | no-suitable-cell-in-tracking-area | plmn-not-allowed | roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed } zone-code-list zc_id +
remove lte-zone-code zone-code-list
```

remove

Removes the zone code list from the call control profile.

```
[ allow | restrict ]
```

Specifies whether the zone code list is allowed or restricted.

**Important:** You can only create an allowed or restricted list, not both.

```
emm-cause-code { eps-service-not-allowed-in-this-plmn | no-suitable-cell-in-tracking-area | plmn-not-allowed | roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed }
```

Optionally, specify one of the following EMM cause codes to apply when a UE request is rejected:

- `eps-service-not-allowed-in-this-plmn`
- `no-suitable-cell-in-tracking-area`
- `plmn-not-allowed`
- `roaming-not-allowed-in-this-tracking-area`
- `tracking-area-not-allowed`

```
zone-code-list zc_id +
```

Specifies the zone code in the allowed or restricted list of zone codes. `zone_code` must be an integer value from 0 to 65535.
**Usage**

Use this command to create zone code lists that allow or restrict access to UEs managed by this call control profile.

**Example**

The following command restricts access to zone codes 234 and 456 and returns an EMM cause code of “tracking area not allowed”:

```
lte-zone-code restrict emm-cause-code tracking-area-not-allowed zone-code-list 234 456
```
map

Configures the optional extensions to Mobile Application Part (MAP) messages.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Call Control Profile Configuration

`configure > call-control-profile profile_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

**Syntax**

```
[ remove ] map message { mo-fwd-sm imsi | update-gprs-location { imeisv | private-extension access-type } }
```

**remove**

IMEI-SV is not included in the GLU request -- this is the default behavior.

**message mo-fwd-sm imsi**

Configures the SGSN to include the IMSI of the originating subscriber in the mobile-originated SM transfer. This parameter shall be included when the sending entity (MSC or SGSN) supports mobile number portability (MNP). This IMSI IE is required in the in MAP-MO-FORWARD-SHORT-MESSAGE in countries where MNP is deployed. This keyword-set is required. The default is disabled.

**update-gprs-location**

Includes a GLU message.

**imeisv**

Specifies the International Mobile equipment Identity-Software Version (IMEI-SV) information to include in the GPRS Location Update (GLU) request message. SGSN will include IMEI-SV in the message, if available. Default: disabled

**private-extension access-type**

Includes a specific access-type private extension in the message.

**Usage**

This command configures optional extensions to MAP messages. The HLR should ignore these extensions if not supported by the HLR.

**Example**

Use the following command to have the SGSN add GLU extension information to the MAP messages sent to the HLR.
map message update-gprs-location private-extension access-type
map-service

Identifies a Mobile Application Part (MAP) service and the context which contains it and associates both with the call control profile.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Call Control Profile Configuration

```
configure > call-control-profile profile_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-call-control-profile-profile_name) #
```

**Syntax**

```
map-service context  ctxt_name  service  map_srvc_name

no map-service context
```

**Usage**

Use this command to enable or disable MAP service with this call control profile.

**Example**

```
no map-service context
```
max-bearers-per-subscriber

Defines the maximum number of bearers allowed per subscriber.

**Product**
MME

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Call Control Profile Configuration

```
configure > call-control-profile profile_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

**Syntax**

```
max-bearers-per-subscriber number

remove max-bearers-per-subscriber

remove

Deletes the definition from the call control profile.

number

Identifies the maximum number of bearers allowed per subscriber as an integer from 1 to 11.

**Usage**

Use this command to set the maximum number of bearers allowed per subscriber.

**Example**

Set the maximum to 3:

```
max-bearers-per-subscriber 3
```
max-pdns-per-subscriber

Defines the maximum number of PDNs allowed per subscriber.

**Product**
MME

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Call Control Profile Configuration

```
configure > call-control-profile profile_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

**Syntax**

```
max-pdns-per-subscriber number
```

```
remove max-pdns-per-subscriber
```

**remove**

Deletes the definition from the call control profile.

```
number
```

Identifies the maximum number of PDNs allowed per subscriber as an integer from 1 to 11.

**Usage**

Use this command to set the maximum number of PDNs allowed per subscriber.

**Example**

Set the maximum to 4:

```
max-pdns-per-subscriber 4
```
**min-unused-auth-vectors**

Configures a specific minimum number of unused vectors to be maintained by the SGSN.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Call Control Profile Configuration

```bash
configure > call-control-profile profile_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

**Syntax**

```
min-unused-auth-vectors min #__vectors

remove min-unused-auth-vectors
```

---

**Syntax**

```
remove
```

Removes the definition from the configuration file and restores the default behavior, which does not use the threshold.

```
min #__vectors
```

Enables and defines a threshold for the minimum number of unused vectors that the SGSN retains to trigger the initiation of a service area identity request (SAI).

**min #__vectors**: Enter a digit between 1 and 4.

---

**Usage**

Vectors are used by the SGSN for authentication. Use this command to enable a minimum threshold for unused vector for this call control profile. When the unused vector count falls below this configured threshold, then an SAI is initiated to fill the buffer back to 5 or to the most appropriate number based on the MAP service configuration.

---

**Example**

Enter a command similar to the following to set a threshold of 3:

```
min-unused-auth-vectors 3
```

Use the following command to disable this function and restore the default behavior, which does not use a threshold to trigger an SAI:

```
remove min-unused-auth-vectors
```
network-feature-support-ie

Configures support for the IMS Voice over Packet-Switched indication.

Product
MME

Privilege
Administrator

Mode
Exec > Global Configuration > Call Control Profile Configuration

call-control-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-call-control-profile-profile_name)#

Syntax

network-feature-support-ie ims-voice-over-ps

remove network-feature-support-ie

remove
Disables support for Voice over PS.

ims-voice-over-ps
Enables support for Voice over PS in all Tracking Areas.

Usage

Use this command to include the “IMS Voice over PS” indication, thereby indicating support for IMS Voice over PS sessions for all Tracking Areas.

Example

The following command enables support for IMS Voice over PS on the MME:

network-feature-support-ie ims-voice-over-ps
network-initiated-pdp-activation

Configures the call control profile to perform two functions: (1) to enable or disable network-requested PDP context activation (NRPCA) for 3G attachments and (2) to define a failure cause code for inclusion in NRPCA-related reject messages.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-call-control-profile-profile_name)#

Syntax

[ remove ] network-initiated-pdp-activation { allow primary | restrict primary | secondary } access type { gprs | umts } { all | location-area-list instance <instance> } network-initiated-pdp-activation primary access type { gprs | umts } { all | location-area-list instance <instance> } failure-code code

network-initiated-pdp-activation secondary access type { gprs | umts } { all | location-area-list instance <instance> } failure-code code

remove
Including this keyword with the command, removes all configured values for the specified configuration.

allow
Allows network-initiated PDP context activation. This keyword must be followed by other parameters to indicate the limitations for allowing the NRPCA.
Allow is the default for NRPCA.

restrict
Restricts network-initiated PDP context activation. This keyword must be followed by other command parameters to indicate the limitations for restricting the NRPCA.

primary
Specifies that only network-initiated primary PDP context activations are to be allowed.

secondary
Specifies that only network-initiated secondary PDP context activations (NRSPCAs) are to be allowed.
**Important:** The secondary keyword is visible and can be selected. However, NRSPCA functionality is only supported for Release 15.0 onwards.

```all
```
Configures the SGSN to allow or to restrict NRPCA for calls within all location areas.

```location-area-list instance instance
```
Selects a pre-defined list of location area codes (LACs) and allows/restricts the NRPCA procedure for calls within the listed area codes.

*instance:* Enter a list ID; an integer between 1 and 5.

**Important:** Before using this keyword, ensure that the appropriate LAC information has been defined with the ```location-area-list``` command, also in this configuration mode.

```failure-codes code
```
Enter an integer from 192 to 226 to identify the GTPP failure cause code (from 3GPP TS29.060, list below) to be included in the reject messages when NRPCA is restricted. If a failure cause code is not defined, the default value is 200 (service not supported).

- 192 - Non-existent
- 193 - Invalid message format
- 194 - IMSI not known
- 195 - MS is GPRS Detached
- 196 - MS is not GPRS Responding
- 197 - MS Refuses
- 198 - Version not supported
- 199 - No resources available
- 200 - Service not supported
- 201 - Mandatory IE incorrect
- 202 - Mandatory IE missing
- 203 - Optional IE incorrect
- 204 - System failure
- 205 - Roaming restriction
- 206 - P-TMSI Signature mismatch
- 207 - GPRS connection suspended
- 208 - Authentication failure
- 209 - User authentication failed
- 210 - Context not found
- 211 - All dynamic PDP addresses are occupied
- 212 - No memory is available
Call Control Profile Configuration Mode

Usage

Use this command to allow or restrict network-requested PDP context activation (NRPCA) based on access-type and location areas. NRPCA is used when there is downlink data at the GGSN for a subscriber, but there is no valid context for the already-established PDP address so the GGSN initiates an NRPCA procedure towards the SGSN.

This command can also be used to define the failure cause code that will be included in activation reject messages.

These commands can be repeated to define a unique set of NRPCA parameters for each access-type and each location area list.

The T3385-timeout and the max-actv-retransmission timers configure the retransmission timer and the number of retries for PDP context activation requests. Both of these timers are set in the SGSN service configuration mode.

The configuration for NRPCA can be viewed via the `show call-control-profile full name profile_name`. Statistics associated with NRPCA can be seen via the `show gmm-sm statistics` output and via the `show sgtpc statistics verbose` output.

Example

The following command changes the failure code for Reject messages from 200 (service not supported) to 205 (roaming restriction) for primary NRPCA for all GRPS access and all LACs:

```
network-initiated-pdp-activation primary access-type gprs all failure-code 205
```

The following command enables network-initiated primary PDP context activation for UMTS calls from the LACs in location-area-list 1:

```
network-initiated-pdp-activation allow primary access-type umts location-area-list instance 1
```

The following command restricts network-initiated primary PDP context activation for UMTS calls from the LACs in location-area-list 2:

```
network-initiated-pdp-activation deny primary access-type umts location-area-list instance 1
```
network-initiated-pdp-activation restrict primary access-type umts
location-area-list instance 2
override-arp-with-ggsn-arp

Enables or disables the ability of the SGSN to override an Allocation/Retention Priority (ARP) value with one received from a GGSN. If there is no authorized Evolved ARP received from the GGSN, by default the SGSN continues to use the legacy ARP included in the Quality of Service (QoS) Profile IE.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-call-control-profile-profile_name)#

Syntax

[ remove ] override-arp-with-ggsn-arp

   remove

   Adding the remove keyword to the command disables the override feature.

Usage

Enabling this function on the SGSN will allow the ARP sent by the GGSN, in CPCR / UPCR / UPCQ, to be applicable as an overriding value.

Example

Use this command to configure the SGSN to negotiate the ARP to be used as an overriding value:

   override-arp-with-ggsn-arp
pdp-activate access-type

Configures the PDP context activation option based the type of access technology.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-call-control-profile-profile_name)#

Syntax

pdp-activate access-type { grps | umts } { all | location-area-list instance instance } failure-code failure_code

default pdp-activate access-type { grps | umts } { all | location-area-list instance instance } failure-code code

default
Resets the configuration to system default values for PDP context activation request.

{ grps | umts }

Specifies the access technology type for PDP context activation.
  • grps: Enables access type as GPRS.
  • umts: Enables access type as UMTS.

all
Default: allow
Configures the system to allow the creation of all PDP context activation requests received from MS.

location-area-list instance instance

Specifies the location area instance for which to create a PDP context as an integer from 1 through 5. The value must be an already defined instance of a location area code (LAC) list created via the location-area-list command.

failure-code code

Specifies the failure code for PDP context activation as an integer from 8 through 112. Default: 8

Usage

Use this command to configure this call control profile to allow GPRS/UMTS access through PDP context activation request from MS.
Example

The following command configures the system to create the PDP context for requests from MS for GPRS access with location area list instance 2 and failure-code 5:

```
pdp-activate access-type gprs location-area-list 2 failure-code 5
```
pdp-activate allow

Configures the system to allow the PDP context activation based on the type of access technology.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Call Control Profile Configuration
configure > call-control-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-call-control-profile-profile_name)#

Syntax

[ no ] pdp-activate allow access-type { gprs | umts } location-area-list instance

_instance

no

Removes the configured permission to create PDP context on request of PDP context activation from MS for an access type.

access-type { gprs | umts }

Specifies the access technology type for PDP context activation.

• gprs: Enables access type as GPRS.
• umts: Enables access type as UMTS.

location-area-list instance instance

Specifies the location area instance to create PDP context.

_instance must be an integer from 1 through 5. The value must be an already defined instance of a location area code (LAC) list created via the location-area-list command.

Usage

Use this command to configure this call control profile to allow GPRS/UMTS access through PDP context activation request from MS.

Example

The following command configures the system to allow the PDP context activation for GPRS access type with location area list instance 2:

pdp-activate allow access-type gprs location-area-list instance 2
pdp-activate restrict

Configures the system to restrict the PDP context activation based on the type of access technology.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-call-control-profile-profile_name)#

**Syntax**

```
[ no | remove ] { { access-type { gprs | umts } { all | location-area-list instance instance } } | { pdp-type { all | dual-ipv4v6 | ipv4 | ipv6 | ppp } { access-type { gprs | umts } { all | location-area-list instance instance } } } | { secondary-activation access-type { gprs | umts } { all | location-area-list instance instance } } }
```

- **no | remove**
  Either of these prefixes removes the previously configured restriction on PDP context activation and returns the ‘allow’ default.

- **access-type { gprs | umts }**
  Specifies the access technology type for which to restrict PDP context activation.
  - **gprs**: Enables access type as GPRS.
  - **umts**: Enables access type as UMTS.
  - **all**: Configures the system to restrict all PDP context activation requests from the MS.
  - **location-area-list instance instance**: Specifies the location area instance to restrict PDP context activation, where list_id must be an integer from 1 through 5. The value must be an already defined instance of a location area code (LAC) list created with the location-area-list command.

- **pdp-type**
  Sets the configuration to restrict PDP activation based on the requested PDP type.
  To restrict more than one type of PDP, the command must be reissued for each PDP type.
  - **all**: restricts activation of all types PDP.
  - **dual-ipv4v6**: restricts activation when dual-IPv4v6 PDP contexts are requested.
  - **ipv4**: restricts activation when IPv4 PDP contexts are requested.
  - **ipv6**: restricts activation when IPv6 PDP contexts are requested.
  - **ppp**: restricts activation when PPP PDP contexts are requested.
secondary-activation

Restricts the SGSN, based on the access-type, so that secondary PDP contexts are not created when receiving the PDP Context Activation Request from the MS.

Usage

Use this command to configure this call control profile to restrict PDP context activation requests from MS.

Example

The following command configures the system to restrict the PDP context activation for request from 2G MS with location area list instance 2:

```
pdp-activate restrict access-type gprs location-area-list instance 2
```

The following command configures the SGSN to restrict PDP context activation for requests from 3G MS if their PDP-type is IPv4. The second command restricts based on PDP-type IPv6.

```
pdp-activate restrict pdp-type ipv4 access-type umts all
pdp-activate restrict pdp-type ipv6 access-type umts location-area-list instance 1
```
pdn-type-override

Configures the MME or the SGSN to override the requested packet data network (PDN) type based on the inbound roamer PLMN, and re-assigns the UE to an IPv4-only or IPv6-only PDN. This override can be applied based on the type of access technology.

Product
MME
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Call Control Profile Configuration
configure > call-control-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-call-control-profile-profile_name)#

Syntax

```
pdn-type-override ipv4v6 { ipv4 | ipv6 } [ access-type { eps | grps | umts } ]
remove pdn-type-override [ access-type { eps | grps | umts } ]
```

- `remove`
  Removes the configured PDN type override.
- `ipv4v6 { ipv4 | ipv6 }`
  Defines the PDN type (IPv4 or IPv6) to which UEs should be restricted.
- `access-type { eps | grps | umts }`
  Specifies the access technology type to which the override is applied.
  * `eps` - enables PDN override for EPS access type.
  * `grps` - enables PDN override for GPRS access type.
  * `umts` - enables PDN override for UMTS access type.
  If this keyword is not included, then all three access types can have the PDN type overridden.

Usage

Use this command to configure the call control profile to override the requested packet data network (PDN) type and re-assign the UE to a different PDN type. Optionally, it is possible to filter the override based on access technology.

**Important:** This call control profile becomes valid only when it is associated with an operator policy using the `associate` command in the Operator Policy configuration mode.
Example

The following command configures the system to override the requested PDN type and assign a UE to an IPv4-only PDN if the UE’s access technology is GPRS:

```
pdn-type-override ipv4v6 ipv4 access-type gprs
```
**peer-mme**

Configures a peer MME address. S4-SGSN operators can use this command if they wish to bypass DNS resolution to obtain the MME address.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Call Control Profile Configuration
configure > call-control-profile profile_name

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

**Syntax**

```
peer-mme { mme-groupid <lac val> mme-code <rac value> | tac tac } prefer { fallback-for-dns | local } address { <ipv4_address> | <ipv6_address> } interface { gn [ s3 ] | s3 [ gn ] }

remove peer-mme { mme-groupid <lac val> mme-code <rac value> | tac tac } address { <ipv4_address> | <ipv6_address> } interface { gn [ s3 ] | s3 [ gn ] }
```

**remove**
Removes a specified peer MME from the call control profile. The `interface` keyword is optional. If it is not used, the entire interface will be deleted.

**mme-groupid <lac val>**
Specifies the location area code value of the peer MME. The MME group ID of the peer MME maps to the LAC value when GUTI is converted to P-TMSI.

<lac val> must be an integer from 1 to 65535.

**mme-code <rac value>**
Specifies the routing area code value of the peer MME. The MME code of the peer MME maps to the RAC value when GUTI is converted to P-TMSI.

<rac value> must be an integer from 0 to 255.

**tac tac**
Optional. Specifies the Tracking Area Code (TAC) of the target eNodeB that is used for UTRAN to E-UTRAN (SGSN to MME) SRNS relocation across the S3 interface. Valid entries are 1 to 65535. This setting applies only if SRNS relocation first has been configured via the `srns-inter` and/or `srns-intra` commands in Call Control Profile Configuration Mode.
prefer { fallback-for-dns | local }

Indicates whether to use a DNS query to obtain the address or to use a locally configured peer MME address:

- **fallback-for-dns** - Instructs the SGSN to perform a DNS query to get the IP address of the peer MME. If the DNS query fails, then the IP address configured with this command is used.
- **local** - Use the locally configured address for the MME address.

**Important:** If the `prefer` command is used to change an existing peer-mme configuration (with the same LAC and RAC) from **fallback-for-dns** to **local** or from **local** to **fallback-for-dns**, the new setting overwrites the previously configured setting for all interfaces.

address { ipv4_address | ipv6_address }

Specifies the IP address of the peer MME. Currently, the IPv6 address option is not supported on the S4-SGSN.

*ipv4* must be in standard dotted-decimal notation.

interface { gn [ s3 ] | s3 [ gn ] }

Specifies the interface to use for communication between the SGSN and the peer MME:

- **gn**: Use the Gn interface between the S4-SGSN and the MME in the LTE network.
- **s3**: Use the S3 interface between the S4-SGSN and the MME in the LTE network. This is the default setting.

**Usage**

Use this command to instruct the S4-SGSN how to determine a peer MME address, via DNS or local configuration. For a local address, use this command to configure the peer MME address. This command also sets the interface type to be used between the peer MME and the SGSN.

**Example**

The following command configures LAC/RAC 111/22 for the peer MME and instructs the SGSN to use the MME’s locally configured IPv4 address of 1.1.1.1 and an S3 interface between the MME and the SGSN.

```
peer-mme mme-groupid 111 mme-code 22 prefer local address 1.1.1.1
interface s3
```
peer-nri-length

Enables the SGSN to use NRI-FQDN-based DNS resolution for non-local RAIs when selection of the call control profile is based on the old-RAI and the PLMN Id of the RNC where the subscriber originally attached. The SGSN also supports RAI based query when NRI based query fails.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-call-control-profile-profile_name)#

Syntax

peer-nri-length length [rai-fqdn-fallback]
remove peer-nri-length [rai-fqdn-fallback]

remove

Deletes the NRI length configuration for the non-local RAIs and the SGSN sends RAI-FQDN-based DNS resolution.

length

This defines the NRI length for the peer SGSN and enables use of NRI-FQDN-based DNS resolution for non-local RAIs. This variable allows for an integer from 1 to 10.

Usage

Important:

- This feature is supported only for 3G subscribers until Release 15.0.

The command enables the SGSN to perform DNS query with an NRI when RAU comes from an SGSN outside the pool. The SGSN uses NRI-FQDN-based DNS resolution for the non-local RAIs for 3G subscribers in place of RAI-FQDN-based DNS resolution. This functionality is applicable in situations for either inter- or intra-PLMN when the SGSN has not chosen a local NRI value (configured with SGSN Service commands) other than local-pool-rai or nb-rai. This means the RAI (outside pool but intra-PLMN) NRI length configured here will be applicable even for intra-PLMN with differently configured NRI lengths (different from the local pool). This functionality is not applicable to call control profiles with an associated MSIN range as ccprofile selection is not IMSI-based. When this feature is enabled, the selection of the ccprofile is based on the old-RAI and the PLMN Id (if configured) of the RNC where the subscriber originally attached.
Example

The following command is used to configure a peer-nri-length of 3, with support for RAI based query when NRI based query fails:

```
peer-nri-length 3 rai-fqdn-fallback
```
plmn-protocol

Configures the protocol supported by the PLMN (Public Land Mobile Network).

**Product**
MME

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-call-control-profile-profile_name)#

**Syntax**

```
plmn-protocol plmnid mcc mcc_num mnc mnc_num { s5-protocol | s8-protocol } { gtp | pmip }
remove plmn-protocol plmnid mcc mcc_num mnc mnc_num
```

**remove**
Deletes the definition from the call control profile configuration.

```plaintext
plmn-id mcc mcc_num mnc mnc_num
```

Identifies the PLMN by MCC (mobile country code) and MNC (mobile network code).

- **mcc_num**: Enter a 3-digit integer from 100-999.
- **mnc_num**: Enter a 2- or 3-digit integer from 00 to 999.

```plaintext
s5-protocol | s8-protocol
```

Select which protocol – S5 or S8 – that controls the identified PLMN.

```plaintext
gtp | pmip
```

Select the protocol variant - GTP or PMIP - that controls functionality for the identified PLMN.

**Usage**
Use this command to identify a particular PLMN and, at a higher level, its operational characteristics.

**Example**

The following command instructs the MME to use PLMN MCC423.MNC40.GPRS with PMIP under S8 Protocol:

```
plmn-protocol plmnid mcc 423 mnc 40 s8-protocol pmip
```
prefer subscription-interface

Selects the specified subscription interface (Gr or S6d) if both interface types are associated with a call-control-profile. Use of this command requires an S6d license.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Call Control Profile Configuration

```
configure > call-control-profile profile_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

**Syntax**

```
prefer subscription-interface { hlr | hss }
```

```
remove prefer subscription-interface
```

- **hlr**
  Selects the HLR Gr interface.

- **hss**
  Selects the HSS S6d interface.

**Usage**

Use of this command requires an S6d license.

The SGSN provides a mechanism to associate a MAP service with call control profile. It is possible that both MAP service and HSS peer service are associated with the call control profile. If the interface preference selected is “hlr”, the MAP protocol is used to exchange messages with the HLR. If the interface preference selected is “hss”, the Diameter-protocol is used to exchange messages with the HSS.

**Example**

The following command specifies that “hss” for S6d is selected as the subscription-interface:

```
prefer subscription-interface hss
```
ptmsi-reallocate

Defines P-TMSI reallocation for Attach Requests, RAU Request, and Service Requests.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Call Control Profile Configuration
configure > call-control-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-call-control-profile-profile_name)#

Syntax

```
ptmsi-reallocate { attach | frequency frequency | interval interval | routing-area-update [ update-type ] | service-request [ service-type ] } [ access-type { gprs | umts } ]
```

```
ptmsi-reallocate routing-area-update { access-type { gprs | umts } | frequency frequency | update-type { combined-update | imsi-combined-update | periodic | ra-update } [ access-type { gprs | umts } | frequency frequency ] }
```

```
ptmsi-reallocate service-request { frequency frequency | service-type { data | page-response | signaling } [ frequency frequency ] } [ access-type { gprs | umts } ]
```

[ no | remove | ptmsi-reallocate { attach | frequency | interval | routing-area-update { update-type { combined-update | imsi-combined-update | periodic | ra-update } [ access-type { gprs | umts } ] | service-request { service-type { data | page-response | signaling } [ frequency frequency ] } [ access-type { gprs | umts } ] }
```

**no**

Disables the authentication procedures configured for the specified P-TMSI reallocation configuration in the call control profile.

**remove**

Deletes the defined authentication procedures for the specified P-TMSI reallocation configuration from the call control profile configuration file.

**attach**

Enables/disables P-TMSI reallocation for Attach with local P-TMSI.

**Important:** IMSI or inter-SGSN Attach is not configurable and will always be reallocated.
access-type type

One of the following must be selected to reallocate on the basis of the type of network access:

- gprs
- umts

This keyword can be used in combination with other keywords to refine the reallocation configuration.

frequency frequency

Defines frequency of the reallocation based on the number of messages skipped. If the frequency is set for 1, then the SGSN skips 1 message and then reallocates on receipt of the 2nd (alternate) request message, essentially reallocating the P-TMSI every time. If the frequency is set for 12, then the SGSN skips reallocation for 12 messages and reallocates on receipt of the 13th request message. This keyword can be used in combination with other keywords to refine the reallocation configuration.

frequency must be an integer from 1 to 50.

By default, frequency is not defined and, therefore, reallocation is done for every request message and none are skipped.

interval minutes

Enter an integer between 1 and 1440 to define the time interval (in minutes) for skipping the service/RAU/attach request message procedure.

routing-area-update [ update-type ]

Enables/disables P-TMSI reallocation for RAU (routing area update) with local P-TMSI. To refine the reallocation configuration, include one of the optional types of updates to limit reallocation:

- combined-update
- imsi-combined-update
- periodic
- ra-update

**Important:** Inter-SGSN RAU will always be reallocated.

service-request [ service-type ]

Enables/disables P-TMSI reallocation for Service Requests. To refine the Service-Request reallocation configuration, include one of the optional service-types to limit the reallocation:

- data
- page-response
- signaling

**Usage**

By default, reallocation is not enabled. Use this command to enable P-TMSI reallocation for Attach Requests, RAU Request, and Service Requests. Fine-tune the reallocation configuration according to frequency, interval, or access-type.

**Example**

The following command configures the SGSN to perform P-TMSI reallocation upon receiving 2G Attach Requests.
ptmsi-reallocate attach access-type gprs

The following command configures the SGSN to disable all previously defined P-TMSI reallocations based on the combined criteria of interval and 3G requests:

no ptmsi-reallocate interval access-type umts
ptmsi-signature-reallocate

Enables P-TMSI signature reallocation during Attach/RAU procedures.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Call Control Profile Configuration

```command
configure > call-control-profile profile_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

**Syntax**

```command
ptmsi-signature-reallocate { attach | frequency frequency | interval interval | ptmsi-reallocation-command | routing-area-update [ update-type ] } [ access-type { gprs | umts } | frequency frequency ]
```

```command
ptmsi-signature-reallocate routing-area-update [ access-type { gprs | umts } | frequency frequency | update-type { combined-update | imsi-combined-update | periodic | ra-update } ] [ access-type { gprs | umts } | frequency frequency ]
```

```command
[ no | remove ] ptmsi-signature-reallocate { attach | frequency | interval | routing-area-update [ update-type { combined-update | imsi-combined-update | periodic | ra-update } ] } [ access-type { gprs | umts } ]
```

---

**no**

Disables the authentication procedures configured for the specified P-TMSI signature reallocation configuration in the call control profile.

---

**remove**

Deletes the defined authentication procedures for the specified P-TMSI signature reallocation configuration from the call control profile configuration file.

---

**attach**

Enables/disables P-TMSI signature reallocation for Attach with local P-TMSI.

---

**access-type type**

One of the following must be selected to reallocate on the basis of the type of network access:

- **gprs**
- **umts**

This keyword can be used in combination with other keywords to refine the reallocation configuration.
**Call Control Profile Configuration Mode**

**ptmsi-signature-reallocate**

---

**frequency frequency**

Defines 1-in-N selective reallocation. If the frequency is set for 12, then the SGSN skips reallocation for the first 11 messages and reallocates on receipt of the twelfth request message.

*frequency* must be an integer from 1 to 50.

This keyword can be used in combination with other keywords to refine the reallocation configuration.

---

**interval minutes**

Enter an integer between 1 and 1440 to define the time interval (in minutes) for skipping the service/RAU/attach request message procedure before performing a P-TMSI signature reallocation.

---

**ptmsi-reallocation-command**

Includes P-TMSI signature reallocation as a part of the P-TMSI reallocation configuration.

---

**routing-area-update [ update-type ]**

Enables/disables P-TMSI signature reallocation for RAU (routing area update) with local P-TMSI. To refine the reallocation configuration, include one of the optional types of updates to limit reallocation:

- combined-update
- imsi-combined-update
- periodic
- ra-update

---

**Usage**

By default, P-TMSI signature reallocation is disabled. This command allows the operator to configure when the P-TMSI signature is reallocated.

---

**Example**

The following command configures the SGSN to reallocate the P-TMSI signature for every third UMTS attach procedure:

```
ptmsi-signature-reallocate attach frequency 3 access-type umts
```

The following command configures the SGSN to reallocate the P-TMSI signature for every seventh GPRS periodic RAU procedure:

```
ptmsi-signature-reallocate routing-area-update update-type periodic frequency 7 access-type gprs
```

The following command removes all configuration instances for reallocating the P-TMSI signature based on intervals and UMTS access:

```
remove ptmsi-signature-reallocate interval access-type umts
```
**qos**

Configures the quality of service (QoS) parameters to be applied.

**Product**
- MME
- SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Call Control Profile Configuration

```
configure > call-control-profile profile_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

**Syntax**
```
qos { gn-gp  }
qos gn-gp { arp high-priority priority medium-priority priority | pre-emption { capability { may-trigger-pre-emption | shall-not-trigger-pre-emption } | vulnerability { not-pre-emptable | pre-emptable } }
qos ue-ambr { max-ul mbr_up max-dl mbr_dl | prefer-as-cap { both-hss-and-local minimum | local } }
remove qos { gn-gp | ue-ambr }
```

**remove**
Deletes the configuration from the call control profile.

**gn-gp**
Configures Gn-Gp pre-release 8 ARP and pre-emption parameters.

**arp**
Maps usage of ARP (allocation/retention policy) high-priority (H) and medium-priority (M):
- **high-priority** *priority*: Enter an integer from 1 to 13.
- **medium-priority** *priority*: Enter an integer from 2 to 14.

**pre-emption**
Defines the pre-emption/vulnerability criteria for PDP Contexts imported from SGSN on Gn/Gp:
- **capability**
  - **may-trigger-pre-emption**: PDP Contexts imported from Gn/Gp SGSN may preempt existing bearers.
• **shall-not-trigger-pre-emption**: PDP Contexts imported from Gn/Gp SGSN shall not preempt existing bearers.

**vulnerability**

• **not-pre-emptable**: PDP Contexts imported from Gn/Gp SGSN are not vulnerable to pre-emption.

• **pre-emptable**: PDP Contexts imported from Gn/Gp SGSN are vulnerable to pre-emption.

---

**ue-ambr**

This keyword enables the operator to configure either the aggregate maximum bit rate stored on the UE (UE AMBR) or select the preferred uplink and downlink QoS cap values.

---

**Important**: The SGSN only supports the `ue-ambr` keyword beginning in Release 16.

---

Configures the aggregate maximum bit rate that will be stored on the UE (user equipment).

• **max-ul mbr-up**: Defines the maximum bit rate for uplink traffic.
  
  `mbr-up`: Enter a value from 1 to 1410065408 (Release 16.1 and higher), or 0 to 1410065408.

• **max-dl mbr-down**: Defines the maximum bit rate for downlink traffic.
  
  `mbr-down`: Enter a value from 1 to 1410065408 (Release 16.1 and higher), or 0 to 1410065408.

---


This set of options is only available on the MME.

Specifies the QoS cap value to use.

• **local-when-subscription-not-available**: Use the locally configured values if the Home Subscriber Server (HSS) does not provide QoS bit rate values.

• **minimum**: Use the lower of either the locally configured QoS bit rate or the HSS-provided QoS bit rate. This will override the HSS provided values if it is greater than the locally configured values, or if the HSS does not provide any values.

• **subscription-exceed-reject**: If the requested QoS bit rate exceeds the locally configured value, reject the PDN connection.

• **emm-cause-code**: Specifies the EPS Mobility Management (EMM) cause code to return when the PDN connection is rejected.

  • **eps-service-disallowed**: Default
  • **eps-service-not-allowed-in-this-plmn**
  • **no-suitable-cell-in-tracking-area**
  • **plmn-not-allowed**
  • **roaming-not-allowed-in-this-tracking-area**
  • **tracking-area-not-allowed**
Usage

Use this command to configure the QoS parameters for the call control profile for either the MME or the SGSN.

On an S4-SGSN, this command ensures proper QoS parameter mapping between the S4-SGSN and EPC UEs, SGWs and PGWs:

- Map EPC ARP parameters to pre-release 8 ARP (Gn/Gp ARP) used during S4-SGSN-to-Gn SGSN call handovers.

- Map ARP parameters received in a GPRS subscription from the HLR to EPC ARP parameters if:
  - The S4 interface is selected for an EPC capable UE, and
  - The UE has only a GPRS subscription (but no EPS subscription) in the HLR / HSS.

Example

Configure the Gn/Gp interface ARP priority values:

```
qos gn-gp arp high-priority 2 medium-priority 3
```
**rau-inter**

Defines acceptable parameters for inter-SGSN routing area updates.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Call Control Profile Configuration

`configure > call-control-profile profile_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

**Syntax**

```
rau-inter { accept use-auth-vector | access-type gprs { all | location-area-list instance instance } { failure-code fail_code | user-device-release { before-r99 | r99-or-later } failure-code fail_code } } | allow accept access-type gprs location-area-list instance instance | avoid-s12-direct-tunnel | ignore-peer-context-id | peer-sgsn-addr-resolution-failure failure-fail-code fail_code | restrict access-type { { gprs | umts } { all | location-area-list instance instance } }

default rau-inter { accept use-auth-vector | access-type { { gprs | umts } { all | location-area-list instance instance } user-device-release { before-r99 | r99-or-later } failure-code fail_code } } | avoid-s12-direct-tunnel | failure-fail-code fail_code | ignore-peer-context-id | peer-sgsn-addr-resolution-failure failure-fail-code fail_code

no rau-inter { accept use-auth-vector | allow access-type { gprs | umts } location-area-list instance instance | ignore-peer-context-id | restrict access-type { gprs | umts } { all | location-area-list instance instance } }

remove rau-interavoid-s12-direct-tunnel

no

Including no as part of the command structure disables the values already configured for parameters specified in the command.

**default**

Resets the configuration of specified parameters to system default values.

**remove**

remove can only be used with the avoid-s12-direct-tunnel keyword to erase a configuration instructing the SGSN to avoid establishment of a direct tunnel for S12 interfaces.

**accept use-auth-vector**

Sets the SGSN to accept using the authorization vector.
allow access-type
Including this keyword with one of the following options, configures the SGSN to allow MS/UE with the identified access-type extension to be part of the intra-RAU procedure.
- gprs - General Packet Radio Service
- umts - Universal Mobile Telecommunications System

avoid-s12-direct-tunnel
Enables the operator to modify the Call-Control profile default configuration and instructs the SGSN to avoid establishment of a direct tunnel for S12 interfaces. This keyword is only supported for configuration of S12 interfaces.

ignore-peer-context-id
Sets the SGSN to ignore the peer’s context-ID and replace with PDP context-ID information based on the HLR subscription.

restrict access-type
Including this keyword-set with one of the following options, configures the SGSN to restrict MS/UE with the identified access-type extension from the inter-RAU procedure.
- gprs - General Packet Radio Service
- umts - Universal Mobile Telecommunications System

all
all - adding this option to the keyword determines that the failure cause code will be applicable to all location areas.

location-area-list instance instance
list_id must be an integer between 1 and 5. The value must be an already defined instance of a location area code (LAC) list created with the location-area-list command.

failure-code fail-code
Specify a GSM Mobility Management (GMM) failure cause code to identify the reason an inter SGSN RAU does not occur. This GMM cause code will be sent in the reject message to the MS. fail-code must be an integer from 2 to 111. Refer to the GMM failure cause codes listed below (from section 10.5.5.14 of the 3GPP TS 124.008 v7.2.0 R7):
- 2 - IMSI unknown in HLR
- 3 - Illegal MS
- 6 - Illegal ME
- 7 - GPRS services not allowed
- 8 - GPRS services and non-GPRS services not allowed
- 9 - MSID cannot be derived by the network
- 10 - Implicitly detached
- 11 - PLMN not allowed
- 12 - Location Area not allowed
- 13 - Roaming not allowed in this location area
- 14 - GPRS services not allowed in this PLMN
- 15 - No Suitable Cells In Location Area
- 16 - MSC temporarily not reachable
- 17 - Network failure
- 20 - MAC failure
- 21 - Synch failure
- 22 - Congestion
- 23 - GSM authentication unacceptable
- 40 - No PDP context activated
- 48 to 63 - retry upon entry into a new cell
- 95 - Semantically incorrect message
- 96 - Invalid mandatory information
- 97 - Message type non-existent or not implemented
- 98 - Message type not compatible with state
- 99 - Information element non-existent or not implemented
- 100 - Conditional IE error
- 101 - Message not compatible with the protocol state
- 111 - Protocol error, unspecified

```
user-device-release { before-r99 | r99-or-later } failure-code code
```

Default: Disabled

Enables the SGSN to reject an Inter-RAU procedure based on the detected 3GPP release version of the MS equipment and selectively send a failure cause code in the reject message. The SGSN uses the following procedure to implement this configuration:

1. When Attach Request is received, the SGSN checks the subscriber’s IMSI and current location information.
2. Based on the IMSI, an operator policy and call control profile is found that relates to this Attach Request.
3. Call control profile is checked for access limitations.
4. Attach Request is checked to see if the revision indicator bit is set
   - if not, then the configured common failure code for reject is sent;
   - if set, then the 3GPP release level is verified and action is taken based on the configuration of this parameter

One of the following options must be selected and completed:

- **before-r99**: Indicates the MS would be a 3GPP release prior to R99 and an appropriate failure code should be defined.
  
  `failure-code code`: Enter an integer from 2 to 111.

- **r99-or-later**: Indicates the MS would be a 3GPP Release 99 or later and an appropriate failure code should be defined.
  
  `failure-code code`: Enter an integer from 2 to 111.
Usage
Use this command to configure the restrictions and function of the inter-RAU procedure.

Example
Configure default inter-RAU settings for Edge calls from subscribers on location-area-list no. 1:

    default rau-inter allow access-type gprs location-area-list instance 1
rau-inter-plmn

Enables or disables restriction of all Routing Area Updates (RAUs) occurring between different PLMNs.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Call Control Profile Configuration

```bash
configure > call-control-profile profile_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

**Syntax**

```bash
rau-inter-plmn access-type { all | location-area-list instance instance } { failure-code fail_code | user-device-release { before-r99 } failure-code fail_code | r99-or-later } { failure-code fail_code }
```

```
default rau-inter-plmn access-type { all | location-area-list instance instance } user-device-release { before-r99 failure-code | r99-or-later failure-code }
```

```
[ no ] rau-inter-plmn { restrict | allow } access-type { gprs | umts } { all | location-area-list instance instance }
```

```
[ no ] rau-inter-plmn { allow access-type | restrict access-type } { [ all ] failure-code fail_code | location-area-list instance instance }
```

```
default rau-inter { allow access-type | restrict access-type } { [ all ] failure-code fail_code | location-area-list instance instance }
```

---

**no**

Including “no” as part of the command structure disables the values already configured for parameters specified in the command.

---

**default**

Resets the configuration of specified parameters to system default values.

---

**allow access-type**

Including this keyword-set with one of the following options, configures the SGSN to allow MS/UE with the identified access-type extension to be part of the intra-RAU procedure.

- **gprs** - General Packet Radio Service
- **umts** - Universal Mobile Telecommunications System
restrict access-type

Including this keyword-set with one of the following options, configures the SGSN to restrict MS/UE with the identified access-type extension from the inter-RAU procedure.

- gprs - General Packet Radio Service
- umts - Universal Mobile Telecommunications System

all

all - adding this option to the keyword determines that the failure cause code will be applicable to all location areas.

location-area-list instance instance

list_id must be an integer between 1 and 5. The value must be an already defined instance of a LAC list created with the location-area-list command.

failure-code fail-code

Specify a GSM Mobility Management (GMM) failure cause code to identify the reason an inter SGSN RAU does not occur. This GMM cause code will be sent in the reject message to the MS.

fail-code must be an integer from 2 to 111. Refer to the GMM failure cause codes listed below (from section 10.5.5.14 of the 3GPP TS 124.008 v7.2.0 R7):

- 2 - IMSI unknown in HLR
- 3 - Illegal MS
- 6 - Illegal ME
- 7 - GPRS services not allowed
- 8 - GPRS services and non-GPRS services not allowed
- 9 - MSID cannot be derived by the network
- 10 - Implicitly detached
- 11 - PLMN not allowed
- 12 - Location Area not allowed
- 13 - Roaming not allowed in this location area
- 14 - GPRS services not allowed in this PLMN
- 15 - No Suitable Cells In Location Area
- 16 - MSC temporarily not reachable
- 17 - Network failure
- 20 - MAC failure
- 21 - Synch failure
- 22 - Congestion
- 23 - GSM authentication unacceptable
- 40 - No PDP context activated
- 48 to 63 - retry upon entry into a new cell
- 95 - Semantically incorrect message
- 96 - Invalid mandatory information
• 97 - Message type non-existent or not implemented
• 98 - Message type not compatible with state
• 99 - Information element non-existent or not implemented
• 100 - Conditional IE error
• 101 - Message not compatible with the protocol state
• 111 - Protocol error, unspecified

user-device-release { before-r99 | r99-or-later } failure-code code

Default: Disabled

Enables the SGSN to reject an Inter-RAU procedure based on the detected 3GPP release version of the MS equipment and selectively send a failure cause code in the reject message. The SGSN uses the following procedure to implement this configuration:

1. When Attach Request is received, the SGSN checks the subscriber’s IMSI and current location information.
2. Based on the IMSI, an operator policy and call control profile are found that relate to this Attach Request.
3. The call control profile is checked for access limitations.
4. Attach Request is checked to see if the revision indicator bit is set
   • if not, then the configured common failure code for reject is sent;
   • if set, then the 3GPP release level is verified and action is taken based on the configuration of this parameter

One of the following options must be selected and completed:

• before-r99: Indicates the MS would be a 3GPP release prior to R99 and an appropriate failure code should be defined.
  
  failure-code code: Enter an integer from 2 to 111.

• r99-or-later: Indicates the MS would be a 3GPP Release 99 or later and an appropriate failure code should be defined.
  
  failure-code code: Enter an integer from 2 to 111.

Usage

Use this command to configure the restrictions and function of the inter-RAU procedure occurring across RNCs or BSSs where the PLMN changes. For example:

• inter-IuPS RAU, where the two IuPSs have different PLMNs
• inter-GPRS RAU, where the two GPRSs have different PLMNs
• inter-RAT RAU (2G > 3G), where the IuPS/GPRS services have different PLMNs
• inter-RAT-RAU (3G > 2G), where the IuPS/GPRS services have different PLMNs

Example

default rau-inter allow access-type gprs location-area-list instance 1
**rau-intra**

Defines an acceptable procedure for intra-SGSN Routing Area Updates (RAUs).

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Call Control Profile Configuration

```configure > call-control-profile profile_name```

Entering the above command sequence results in the following prompt:

```[local]host_name(config-call-control-profile-profile_name)#```

**Syntax**

```rau-intra access-type { all | location-area-list instance instance } { failure-code fail_code | user-device-release { before-r99 } { failure-code fail_code | r99-or-later } { failure-code fail_code } }

default rau-intra access-type { all | location-area-list instance instance } user-device-release { before-r99 failure-code | r99-or-later failure-code }

default rau-intra { allow access-type | restrict access-type } { [ all ] failure-code fail_code | location-area-list instance instance } }

```

**no rau-intra { allow access-type | restrict access-type } { [ all ] failure-code fail_code | location-area-list instance instance } }

```default rau-intra { allow access-type | restrict access-type } { [ all ] failure-code fail_code | location-area-list instance instance } }

```

**no**
Including “no” as part of the command structure disables the values already configured for parameters specified in the command.

**default**
Resets the configuration of specified parameters to system default values.

**allow access-type**
Including this keyword-set with one of the following options, configures the SGSN to allow an MS/UE with the identified access-type extension to be part of the intra-RAU procedure.

- **gprs** - General Packet Radio Service
- **umts** - Universal Mobile Telecommunications System
restrict access-type

Including this keyword-set with one of the following options, configures the SGSN to restrict an MS/UE with the identified access-type extension from the intra-RAU procedure.

- gprs - General Packet Radio Service
- umts - Universal Mobile Telecommunications System

all

all - adding this option to the keyword determines that the failure cause code will be applicable to all location areas.

location-area-list instance instance

list_id must be an integer between 1 and 5. The value must be an already defined instance of a location area code (LAC) list created via the location-area-list command.

failure-code fail-code

Specify a GSM Mobility Management (GMM) failure cause code to identify the reason an inter SGSN RAU does not occur. This GMM cause code will be sent in the reject message to the MS.

fail-code must be an integer from 2 to 111. Refer to the GMM failure cause codes listed below (from section 10.5.5.14 of the 3GPP TS 124.008 v7.2.0 R7):

- 2 - IMSI unknown in HLR
- 3 - Illegal MS
- 6 - Illegal ME
- 7 - GPRS services not allowed
- 8 - GPRS services and non-GPRS services not allowed
- 9 - MSID cannot be derived by the network
- 10 - Implicitly detached
- 11 - PLMN not allowed
- 12 - Location Area not allowed
- 13 - Roaming not allowed in this location area
- 14 - GPRS services not allowed in this PLMN
- 15 - No Suitable Cells In Location Area
- 16 -MSC temporarily not reachable
- 17 - Network failure
- 20 - MAC failure
- 21 - Synch failure
- 22 - Congestion
- 23 - GSM authentication unacceptable
- 40 - No PDP context activated
- 48 to 63 - retry upon entry into a new cell
- 95 - Semantically incorrect message
- 96 - Invalid mandatory information
user-device-release { before-r99 | r99-or-later } failure-code code

Default: Disabled

Enables the SGSN to reject an Intra-RAU procedure based on the detected 3GPP release version of the MS equipment and selectively send a failure cause code in the reject message. The SGSN uses the following procedure to implement this configuration:

1. When Attach Request is received, the SGSN checks the subscriber’s IMSI and current location information.
2. Based on the IMSI, an operator policy and call control profile are found that relate to this Attach Request.
3. Call control profile is checked for access limitations.
4. Attach Request is checked to see if the revision indicator bit is set
   - if not, then the configured common failure code for reject is sent;
   - if set, then the 3GPP release level is verified and action is taken based on the configuration of this parameter

One of the following options must be selected and completed:

- **before-r99**: Indicates the MS would be a 3GPP release prior to R99 and an appropriate failure code should be defined.

  `failure-code code`: Enter an integer from 2 to 111.

- **r99-or-later**: Indicates the MS would be a 3GPP Release 99 or later and an appropriate failure code should be defined.

  `failure-code code`: Enter an integer from 2 to 111.

Usage

Use this command to configure the restrictions and function of the intra-RAU procedure.

Example

```
default rau-intra allow access-type gprs location-area-list instance 1
```
re-authenticate

Enables or disables the re-authentication feature. This command is available in releases 8.1 and higher.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Call Control Profile Configuration

`configure > call-control-profile profile_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

**Syntax**

```
re-authenticate [ access-type { gprs | umts } ]
remove re-authenticate
```

**Syntax**

**remove**
Including this keyword with the command disables the feature. The feature is disabled by default.

**access-type**
Defines the type of access to be allowed or restricted.

- `gprs`
- `umts`

If this keyword is not included, then both access types are allowed by default.

**Usage**
Use this command to enable or disable the re-authentication feature, which instructs the SGSN to retry authentication with another RAND in situations where failure of the first authentication has occurred. To address the introduction of new SIM cards, for security reasons a systematic "last chance" authentication retry with a fresh Authentication Vector is needed, particularly in cases where there is an SRES mismatch at authentication.

**Example**

```
re-authenticate
```
regional-subscription-restriction

Allows the operator to define the cause code for subscriber rejection when it is due to regional subscription information failure.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Call Control Profile Configuration
configure > call-control-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-call-control-profile-profile_name)#

Syntax

[ remove ] regional-subscription-restriction [ failure-code code | user-device-release { before-r99 failure-code code | r99-or-later failure-code code } ]

---

remove
This keyword causes the configuration to be deleted from the call control profile configuration.

---

failure-code cause_code

cause_code: Enter an integer from 2 to 111; default code is 13 (roaming not allowed in this location area [LA]). Refer to the GMM failure cause codes listed below (from section 10.5.5.14 of the 3GPP TS 124.008 v7.2.0 R7):

- 2 - IMSI unknown in HLR
- 3 - Illegal MS
- 6 - Illegal ME
- 7 - GPRS services not allowed
- 8 - GPRS services and non-GPRS services not allowed
- 9 - MSID cannot be derived by the network
- 10 - Implicitly detached
- 11 - PLMN not allowed
- 12 - Location Area not allowed
- 13 - Roaming not allowed in this location area
- 14 - GPRS services not allowed in this PLMN
- 15 - No Suitable Cells In Location Area
- 16 - MSC temporarily not reachable
- 17 - Network failure
• 20 - MAC failure
• 21 - Synch failure
• 22 - Congestion
• 23 - GSM authentication unacceptable
• 40 - No PDP context activated
• 48 to 63 - retry upon entry into a new cell
• 95 - Semantically incorrect message
• 96 - Invalid mandatory information
• 97 - Message type non-existent or not implemented
• 98 - Message type not compatible with state
• 99 - Information element non-existent or not implemented
• 100 - Conditional IE error
• 101 - Message not compatible with the protocol state
• 111 - Protocol error, unspecified

**user-device-release { before-r99 | r99-or-later } failure-code code**

Enables the SGSN to assign a reject cause code based on the detected 3GPP release version of the MS equipment.

One of the following options must be selected and completed:

• **before-r99**: Indicates the MS would be a 3GPP release prior to R99 and an appropriate failure code should be defined.

  **failure-code code**: Enter an integer from 2 to 111. Refer to the list above.

• **r99-or-later**: Indicates the MS would be a 3GPP Release 99 or later and an appropriate failure code should be defined.

  **failure-code code**: Enter an integer from 2 to 111. Refer to the list above.

**Usage**

Use this command to define GMM reject cause codes when rejection is due to regional subscription information failure.

**Example**

The following command sets a location area rejection message, code 12 for regional restriction rejections:

```
regional-subscription-restriction failure-code 12
```
reuse-authentication-triplets

Creates a configuration entry to enable or disable the reuse of authentication triplets in the event of a failure.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Call Control Profile Configuration

```bash
configure > call-control-profile profile_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

**Syntax**

```
[ no | remove ] reuse-authentication-triplets no-limit
```

- **no**
  - Disables this configuration entry and disables reuse of authentication triplets.

- **remove**
  - This keyword causes the reuse configuration to be deleted from the call control profile configuration. This is the default behavior. Triplets are reused.

- **no-limit**
  - This keyword enables reuse triplets as needed.

**Usage**

Use this command to enable reuse of authentication triplets.

**Example**

```
reuse-authentication-triplets no limit
```
rfsp-override

Configures RAT frequency selection priority override parameters for this call control profile.

Product
MME
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Call Control Profile Configuration
configure > call-control-profile profile_name

Entering the above command sequence results in the following prompt:
[local]host_name(config-call-control-profile-profile_name)#

Syntax

rfsp-override { default value | ue-val value new-val value + }
remove rfsp-override { default | ue-val value }

remove
Deletes the rfsp-override configuration from the call control profile.

default
Restores the default value assigned.

ue-val value
Assign the UE value for the RAT frequency selection priority.
value: Enter an integer from 1 to 256.

new-val value
Assign a new RFSP Index value.
value: Enter an integer from 1 to 256.
Multiple UE value/new value combinations can be configured in a single command.

Usage
Use this command to configure the RAT frequency selection priority override parameter. 
Multiple UE value/new value combinations can be configured.

Example
The following command resets the specified RFSP Index value (1) to its default value, thereby removing the RFSP Index override value previously configured:

rfsp-override default 1
rfsp-override ue-settings

Configures the override of the RAT Frequency Selection Priority (RFSP) of matching subscribers.

Product
MME

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Call Control Profile Configuration
configure > call-control-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-call-control-profile-profile_name)#

Syntax


remove

Deletes the rfsp-override configuration from the call control profile.

ue-settings value

Assign the UE value for the RAT frequency selection priority.

data-centric ue-voice-domain-preference

Assign the UE value for the RAT frequency selection priority for data-centric calls.

• cs-voice-only: Circuit switched voice only.
• cs-voice-preferred-ims-ps-voice-secondary: Circuit switched voice preferred.
• ims-ps-voice-only: IMS Packet switched voice only.

voice-centric ue-voice-domain-preference

Assign the UE value for the RAT frequency selection priority for voice-centric calls.

• cs-voice-only: Circuit switched voice only.
• cs-voice-preferred-ims-ps-voice-secondary: Circuit switched voice preferred.
• ims-ps-voice-only: IMS Packet switched voice only.
new-val value

Assign a new RFSP Index value.

value: Enter an integer from 1 to 256.

Multiple UE value/new value combinations can be configured in a single command.

Usage

Use this command to assign an RFSP Index for a UE based on the following factors:

- Operator policy (where IMSI range or PLMN can influence the selected RFSP)
- UE usage setting (voice centric, data centric)
- Voice domain preference (CS voice only, CS voice preferred, IMS PS voice preferred, IMS PS voice only).

To support Radio Resource Management (RRM) in E-UTRAN, the MME provides the parameter RFSP Index to an eNodeB across S1. The RFSP Index is used by the eNodeB to apply specific RRM strategies. The MME receives the subscribed RFSP Index from the HSS, then overrides the RFSP Index for the UE based on the settings defined in this command.

Multiple UE value/new value combinations can be configured.

Example

The following command overrides the RFSP Index value for voice-centric circuit switched calls to an RFSP Index of 10:

```
rfsp-override ue-setting voice-centric voice-domain-pref cs-voice_only
new-val 10
```
s1-reset

Configures the behavior of user equipment (UE) on S1-reset.

**Product**
MME

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Call Control Profile Configuration
configure > call-control-profile *profile_name*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

**Syntax**

```
s1-reset { detach-ue | idle-mode-entry }
```

**default s1-reset**

```
default
Reset the profile configuration to the system default of **idle-mode-entry**.
```

```
detach-ue
Upon S1-reset the MME will detach the UE.
```

```
idle-mode-entry
Upon S1-reset the MME will move the UE to idle-mode. This is the default setting for this command.
```

**Usage**
Use this command to set the MME’s reactions to an S1-reset.

**Example**
Configure the MME to put the UE into idle-mode upon receipt of S1-reset:

```
s1-reset idle-mode-entry
```
sctp-down

Configures the behavior towards UE (user equipment) when Stream Control Transmission Protocol (SCTP) goes down.

Product
MME

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Call Control Profile Configuration
configure > call-control-profile profile_name

Entering the above command sequence results in the following prompt:
[local]host_name(config-call-control-profile-profile_name)#

Syntax
sctp-down { detach-ue | idle-mode-entry }

default sctp-down

default
Reset the profile configuration to the system default when SCTP layer goes down. The default for this command is idle-mode-entry.

detach-ue
When SCTP goes down, the MME will detach the UE.

idle-mode-entry
When the SCTP goes down, the MME will move the UE to idle-mode. This is the default for this command.

Usage
Use this command to set the MME’s reactions when the SCTP goes down.

Example
Configure the MME to put the UE into idle-mode when the SCTP layer goes down:

    sctp-down idle-mode-entry
sgs-cause-code-mapping

Configures the EMM reject cause code to send to a UE when an SGs cause code is received.

Product
MME

Privilege
Administrator

Mode
Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-call-control-profile-profile_name)#

Syntax

sgs-cause-code-mapping  sgs-cause  emm-cause-code  emm_cause_code

remove sgs-cause-code-mapping  sgs-cause

remove sgs-cause-code-mapping  sgs-cause

Removes the configured cause code mapping and returns it to its default value.

sgs-cause-code

Specifies the SGs cause code received on the SGs interface to which the new cause code should be mapped.

• congestion - Default mapped EMM cause code: #22 Congestion.
• illegal-me - Default mapped EMM cause code: #16 MSC temporarily unreachable.
• illegal-ms - Default mapped EMM cause code: #16 MSC temporarily unreachable.
• imei-not-accepted - Default mapped EMM cause code: #16 MSC temporarily unreachable.
• imsi-unknown-in-hlr - Default mapped EMM cause code: #2 IMSI unknown in HSS.
• imsi-unknown-in-vlr - Default mapped EMM cause code: #16 MSC temporarily unreachable.
• la-not-allowed - Default mapped EMM cause code: #16 MSC temporarily unreachable.
• network-failure - Default mapped EMM cause code: #17 Network failure.
• no-suitable-cells-in-la - Default mapped EMM cause code: #16 MSC temporarily unreachable.
• plmn-not-allowed - Default mapped EMM cause code: #16 MSC temporarily unreachable.
• protocol-error - Default mapped EMM cause code: #16 MSC temporarily unreachable.
• roaming-not-allowed-in-la - Default mapped EMM cause code: #16 MSC temporarily unreachable.
• service-not-subscribed - Default mapped EMM cause code: #16 MSC temporarily unreachable.
• service-not-supported - Default mapped EMM cause code: #16 MSC temporarily unreachable.
Call Control Profile Configuration Mode

**sgs-cause-code-mapping**

- **service-out-of-order** - Default mapped EMM cause code: #16 MSC temporarily unreachable.

```bash
display-cm
```

- **emm-cause-code emm_cause_code**

  Specifies the EPS Mobility Management (EMM) cause code to return to the UE for the given SGs cause code.

  - **congestion**
  - **cs-domain-unavailable**
  - **imsi-unknown-in-hlr**
  - **msc-temp-unreachable**
  - **network-failure**

**Usage**

Use this command to configure the EMM cause code returned to a UE when an error is reported via the SGs interface when attachment to the VLR has failed.

If a condition is specified in both the call control profile associated with a call and also the MME service, the cause configured on the call control profile is signalled to the UE.

**Important:** EMM cause code #18 “CS Domain not available” is not mapped to any SGs code but is returned when SGs service is disallowed by a policy or on unexpected behavior such as when the MME is unable to send an SGs message to a VLR.

**Related Commands**

To set the cause codes for situations where a call control profile cannot be attached to a call (for example new-call restrictions, congestion during new call attempt, etc.), use the `local-cause-code-mapping` command in the mme-service configuration mode. This command is described in the **MME Service Configuration Mode Commands** chapter.

**Example**

The following command maps the “congestion” EMM cause code to the “network-failure” SGs cause code:

```bash
sgs-cause-code-mapping network-failure emm-cause-code congestion
```
sgsn-address

Defines the IP addresses for peer SGSNs in a static SGSN address table. These configured addresses can be used if operators wish to bypass DNS.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-call-control-profile-profile_name)#

Syntax

sgsn-address { nri nri | rac rac_id lac lac_id | rnc_id rnc_id } [ nri nri ] prefer { fallback-for-dns | local } address { ipv4 ip_address | ipv6 ip_address } interface { gn | s16 }

no sgsn-address { ipv4 ip_address | ipv6 ip_address } { nri nri | rac rac_id lac lac_id [ nri nri | rnc_id rnc_id ] [ interface { gn | s16 } ]

no

Disables the specified peer-SGSN address configuration.

rac rac_id

Identifies the foreign routing area code (RAC) of the peer-SGSN address to be configured in the static peer-SGSN address table. rac_id must be an integer from 1 to 255.

lac lac_id

Identifies the foreign location area code (LAC) ID of the peer-SGSN address to be configured in the static peer-SGSN address table. lac_id must be an integer from 1 to 65535.

rnc_id rnc_id

Optional. Specifies the target RNC ID that maps to the address of the peer SGSN via the S16 interface. The RNC ID is used by the S4-SGSN for inter-SGSN SRNS relocations. Valid entries are 1 to 65535. This setting only applies if SRNS relocation has been configured via the srns-inter and/or srns-intra commands in Call Control Profile Configuration Mode.

nri nri

Identifies the network resource identifier stored in the P-TMSI (bit 17 to bit 23). nri must be an integer from 0 to 63.
**Important:** Typically, use of this keyword is optional. However, it must be included in the command when Flex (SGSN-Pooling) is implemented.

```
prefer { fallback-for-dns | local }
```

Indicates the preferred source of the address to be used.

- **fallback-for-dns** - Instructs the SGSN to perform a DNS query to get the IP address of the peer-SGSN. If the DNS query fails, then the IP address configured with this command is used.
- **local** - instructs the system to use the local IP address configured with this command.

**Important:** If the `prefer` command is used to change an existing `sgsn-address` configuration (with the same LAC and RAC) from `fallback-for-dns` to `local` or from `local` to `fallback-for-dns`, the new setting overwrites the previously configured setting for all interfaces.

```
address { ipv4 ip_address | ipv6 ip_address }
```

Specifies the IP address of the peer SGSN. Currently, the IPv6 address option is not supported on the S4-SGSN.

- **ipv4 ip_address** - specifies a valid address in IPv4 dotted-decimal notation.
- **ipv6 ip_address** -

**Important:** The `ipv6` option is under development for future use and is not supported in this release.

```
interface { gn | s16 }
```

*interface* - optional. Specifies the interface type used for communicating with the peer SGSN. Must be one of the following:

- **gn** specifies that communication will occur over the Gn interface with a peer SGSN configured for 2.5G, 3G, or dual access SGSN services.
- **s16** specifies that communication will occur over the S16 interface with a peer S4-SGSN.

**Usage**

Use this command to save time by avoiding DNS. This command enables a local mapping by setting the peer-SGSN IP address to be used for inter-SGSN Attach and inter-SGSN-RAU. When configured, if the SGSN receives a RAU or an Attach Request with a P-TMSI and an old-RAI that is not local, the SGSN consults this table and uses the configured IP address instead of resolving via DNS. If this table is not configured, then IP address resolution is done using DNS.

The MCC and MNC of the RAI are taken from the IMSI range configured in the operator policy and the LAC and RAC are configured here in the call control profile configuration mode.

The `sgsn-address` command differs from other Call Control Profile configuration mode commands in the following ways:

- Within the SGSN’s call logic, all other configuration elements defined with the other commands in this mode are used *after* the IMSI is learnt. The configuration defined with this command is part of the decision logic *prior* to the IMSI being known.
With the peer-SGSN address configured using this `sgsn-address` command, the peer-SGSN-RAI’s MCC/MNC is used as a 5 or 6-digit IMSI and the operator policy and call control profile selection are completed.

**Important:** Typically, use of this command is optional. However, it must be included in the configuration when Flex (SGSN-Pooling) is implemented if (1) the SGSN functions as a default SGSN, then configure the local-NRI of other SGSN with this command; or if (2) another SGSN is offloading, then configure the NB-RAI/null-NRI of the peer-SGSN with this command.

**Example**

Create a local peer-SGSN address mapping of an RAI with RAC of 123 and LAC of 4444 and an IPv4 address of 123.11.313.11 for the peer-SGSN:

```
sgsn-address rac 123 lac 4444 local address ipv4 123.11.313.11
```
sgsn-core-nw-interface

This command enables operators to select the Gn interface or the S4 interface for EPC capable UEs on the S4-SGSN.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-call-control-profile-profile_name)#

Syntax

sgsn-core-nw-interface { gn | s4 }

sgsn-core-nw-interface { gn | s4 }

Specifies the interface that EPC-capable UEs will use to communicate with packet core gateways (GGSN/SGW). Selection must be one of:

• gn: Forces the SGSN to forcefully select the Gn interface for EPC-capable UEs.

• s4: Specifies that the SGSN will use the S4 interface between the S4-SGSN and packet core gateways (GGSN/SGW). This is the default setting for EPC-capable UEs.

Usage
Use this command to forcefully select the interface that the SGSN will use for EPC-capable UEs. This command is available only if the SGSN S4 Interface license is enabled on the SGSN.

Example

sgsn-core-nw-interface gn
sgsn-number

Defines the SGSN’s E.164 number to be used for interactions via the Mobile Application Part (MAP) protocol. E.164 is an ITU-T recommendation that defines the international public telecommunication numbering plan used in public switched telephone networks (PSTN) and some other data networks.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Call Control Profile Configuration
configure > call-control-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-call-control-profile-profile_name)#

Syntax

sgsn-number E164_number
no sgsn-number

no

Disables the use of this configuration definition.

E164_number

Specifies a string of 1 to 16 digits that serve as the SGSN’s E.164 identification.

Usage

This command configures the current SGSN E164 contact number.
The SGSN number configured for a call control profile is related to the SGSN number configured in the SGSN service configuration and/or in the GPRS service configuration. If the SGSN number is not configured as part of the call control profile configuration, then the SGSN number defined as part of the SGSN service or GPRS service configuration is used.
When the 3G SGSN supports multiple PLMNs configured through different IuPS services or when network sharing is implemented, then it may be required to use different SGSN numbers for each PLMN. In such cases, configure the per-PLMN SGSN number in a call control profile. SGSN number definition for a call control profile allows emulation of a different SGSN to each HLR per PLMN. SGSN number definitions in the call control profile also enable the SGSN to use a different SGSN number per operator when network sharing is implemented.

Example

Map the E.164 number 198765432123456 for the SGSN to this call control profile configuration:

sgsn-number 198765432123456
### sgtp-service

Identifies the SGTP service configuration to be used according to this call control profile.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Call Control Profile Configuration  
configure > call-control-profile profile_name

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

**Syntax**

```
sgtp-service context ctxt_name service sgtp_service_name
no sgtp-service context
```

- **context ctxt_name**
  Specifies the SGTP context as an alphanumeric string of 1 through 64 characters.

- **service sgtp_service_name**
  Specifies the SGTP service name as an alphanumeric string of 1 through 64 characters.

- **no**
  Disables use of SGTP service.

**Usage**

Use this command to configure enabling or disabling of SGTP service for this call control profile.

**Example**

```
sgtp-service context sgtp1 service sgtp-srvcl
```
sms-mo

Configures how mobile-originated (MO) short message service (SMS) messages are handled.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-call-control-profile-profile_name)#

Syntax

[ remove ] sms-mo { { access-type { gprs | umts } { all-location-areas | location-area-list } | allow access-type { gprs | umts } | restrict access-type { gprs | umts } }

remove
Deletes the specified configuration.

access-type type
Access by SMS will be limited to SMS coming from this network type:

• gprs
• umts

allow
Allow either GPRS or UMTS type access for SMS.

restrict
Restrict either GPRS or UMTS type access for SMS.

location-area-list instance instance
instance must be an integer between 1 and 5. The value must identify an already defined location area code (LAC) list created with the location-area-list command.

failure-code code
code: Must be an integer from 2 to 111.

Usage
Configure filtering for SMS-MO messaging.

Example
sms-mo access-type gprs all-location-areas failure-code 100
**sms-mt**

This command configures how mobile-terminated (MT) short message service (SMS) messages are handled.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Call Control Profile Configuration

`configure > call-control-profile profile_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

**Syntax**

```
[ remove ] sms-mt { { access-type { gprs | umts } { all-location-areas | location-area-list } | allow access-type { gprs | umts } | restrict access-type { gprs | umts } }
```

- **remove**
  Deletes the specified configuration.

- **access-type**
  Access by SMS will be limited to SMS coming from this network type:
  - gprs
  - umts

- **allow**
  Allow either GPRS or UMTS type access for SMS.

- **restrict**
  Restrict either GPRS or UMTS type access for SMS.

- **location-area-list**
  `instance instance`
  `instance` must be an integer between 1 and 5. The value must identify an already defined LAC list created with the `location-area-list` command.

- **failure-code**
  `code`
  `code`: Must be an integer from 2 to 111.

**Usage**
Configure filtering for SMS-MT messaging.

**Example**

Configure filtering for SMS-MT messaging.
sms-mt access-type gprs all-location-areas failure-code 100
srns-inter

Defines handling parameters for Inter-SRNS (Serving Radio Network Subsystem) relocation.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Call Control Profile Configuration
configure > call-control-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-call-control-profile-profile_name)#

Syntax

srns-inter { all failure-code | allow location-area-list instance instance failure-code code | restrict location-area-list instance instance } } 

no srns-inter { allowlocation-area-list instance instance | restrictlocation-area-list instance instance } 

default srns-inter { all | location-area-list-instance instance } }

no
Deletes the inter-SRNS relocation configuration.

default
Resets the configuration to default values.

all failure-code code
Define the failure code that will apply to all inter-SRNS relocations.

code: Must be an integer from 2 to 111.

allow location-area-list instance instance
Identify the location area list Id (LAC Id) that will allow services in the defined location area.

location-area-list instance instance
instance: Must be an integer between 1 and 5 that identifies the previously defined location area list created with the location-area-list command.

restrict location-area-list instance instance
Identify the location area list Id (LAC Id) that indicates the location areas where services will be restricted.
Usage

This command defines the operational parameters for inter-SRNS relocation.

Example

The following command allows services in areas listed in LAC list #3:

```
srns-inter allow location-area-list instance 3
```
srns-intra

Defines handling parameters for intra-SRNS (Serving Radio Network Subsystem) relocation.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-call-control-profile-profile_name)#

Syntax

srns-intra ( all failure-code | allow location-area-list instance instance | location-area-list instance instance failure-code code | restrict location-area-list instance instance )

no srns-intra { allow location-area-list instance instance | restrictlocation-area-list instance instance }

default srns-intra { all | location-area-list-instance instance }

no

Deletes the intra-SRNS relocation configuration.

default

Resets the configuration to default values.

all failure-code code

Define the failure code that will apply to all intra-SRNS relocations.

code: Must be an integer from 2 to 111.

allow location-area-list instance instance

Identify the location area list Id (LAC Id) that will allow services in the defined location area.

location-area-list instance instance

instance: Must be an integer between 1 and 5 that identifies the previously defined location area list created with the location-area-list command.

restrict location-area-list instance instance

Identify the location area list Id (LAC Id) of the target RNC to determine the location areas where services will be restricted.
Usage

This command defines the operational parameters for intra-SRNS relocation.

Example

The following command restricts service in areas listed in the LAC list 1:

```
srns-intra restrict location-area-list instance 1
```
srvcc exclude-stnsr-nanpi

Configures the MME to **not** include the Nature of Address and Numbering Plan Indicator (NANPI) in the Session Transfer Number for Single Radio Voice Call Continuity (STN-SR) IE on Sv interface in PS to CS requests to the MSC server and Forward Relocation requests to the peer-SGSN/peer-MME.

**Product**
MME

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Call Control Profile Configuration
configure > call-control-profile profile_name

Entering the above command sequence results in the following prompt:

[local] host_name(config-call-control-profile-profile_name)#

**Syntax**

```
[ remove ] srvcc exclude-stnsr-nanpi
```

---

**remove**

Deletes this configuration from the call control profile. This returns the MME to its default configuration where the NANPI is not included in the STN-SR IE.

---

**Usage**

This command applies to Release 15.0 MR3 and higher.
In Release 15.0 MR3 and later releases, the encoding of the STN-SR IE on Sv interface now includes the NANPI from the HSS in PS to CS requests to the MSC server and Forward Relocation requests to the peer-SGSN/peer-MME. The value of NANPI sent by the MME is 0x11. This change in behavior is provided in support of TS 29.280 V10.1.0.
This command provides an option to maintain backward compatibility. When this command is issued, the MME excludes the NANPI from these requests, as was the default in releases prior to 15.0 MR3.
subscriber-control-inactivity

Configures the subscriber-control inactivity timer. The system detects inactivity when no PDP context is activated and starts the timer.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Call Control Profile Configuration
configure > call-control-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-call-control-profile-profile_name)#

**Syntax**

```
subscriber-control-inactivity timeout minutes time detach { immediate | next-connection | reattach-time-period }

{ no | default } subscriber-control-inactivity
```

- **no**
  Deletes the timer configuration.

- **default**
  Resets the timer configuration to the default value of 7 days (10080 minutes).

- **timeout minutes time detach**
  Sets the number of minutes the SGSN monitors the connection after inactivity has been detected. When the timer expires, the subscribe will be detached.
  
  **time**: Enter an integer from 1 to 20160 (two weeks).

- **detach**
  Instructs the SGSN to detach and can be configured to specify when the detach will occur after inactivity is detected. To fine-tune the detach instruction, include one of the following with the command:
  - **immediate** - Instructs the SGSN to detach immediately after inactivity is detected. May combine with **reattach-time-period**.
  - **next-connection** - instructs the SGSN to detach after the next Iu connection after inactivity is detected.

**Important**: Supported for 3G SGSNs only.
**reattach-time-period** period[ action ] - Specify the number of seconds the SGSN will monitor a new re-attach after the previous detach was due to inactivity. Also, you can define the action to be taken regarding new attaches.

- **period**: Enter an integer from 60 to 3600.
- **action** - Select an action:
  - **deny**
  - **permit-and-stop-monitoring**

**Usage**

Use this command to configure the timeout timer. After this timer times out the subscriber is detached from the SGSN.

**Example**

The following command instructs the SGSN to monitor the connection for up to 360 minutes after inactivity is detected, or detach immediately after inactivity is detected:

```
subscriber-control-inactivity timeout minutes 360 detach immediate
```
super-charger

Enables or disables the SGSN to work with a super-charged network.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Call Control Profile Configuration

```
configure > call-control-profile profile_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

**Syntax**

```
[ remove ] super-charger
```

```
remove
Disables the super-charger functionality.
```

**Usage**
By enabling the super charger functionality for 2G or 3G connections controlled by an operator policy, the SGSN changes the hand-off and location update procedures to reduce signalling traffic management.

**Example**
The following command enables the super charger feature:

```
super-charger
```
tau

Configure parameters for the tracking area update (TAU) procedure.

Product:
MME

Privilege:
Security Administrator, Administrator

Mode:
Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-call-control-profile-profile_name)#

Syntax:

tau { imei-query-type { imei | imei-sv | none } [ verify-equipment-identity [ allow-on-eca-timeout | deny-greystated | deny-unknown | verify-emergency ] ] | inter-rat security-ctxt { allow-mapped | native } } 

remove tau { imei-query-type | inter-rat security-ctxt }

remove

Deletes this TAU configuration from the call control profile.

imei-query-type { imei | imei-sv | none }

This keyword set is specific to the MME.
Sets the IMEI query-type if an IMEI (International Mobile Equipment Identity) is not already present.

- **imei**: Specifies that the MME is required to query the UE for its International Mobile Equipment Identity (IMEI).
- **imei-sv**: Specifies that the MME is required to query the UE for its International Mobile Equipment Identity - Software Version (IMEI-SV).
- **none**: Specifies that the MME does not need to query for IMEI or IMEI-SV.

verify-equipment-identity [ allow-on-eca-timeout | deny-greystated | deny-unknown | verify-emergency ] 

Specifies that the identification (IMEI or IMEI-SV) of the UE is to be performed by the Equipment Identity Register (EIR) over the S13 interface.

- **allow-on-eca-timeout**: Configures the MME to allow equipment that has timed-out on ECA during the attach procedure.
- **deny-greystated**: Configures the MME to deny grey-listed equipment during the attach procedure.
- **deny-unknown**: Configures the MME to deny unknown equipment during the attach procedure.
- **verify-emergency**: Configures the MME to ignore the IMEI validation of the equipment during the attach procedure in emergency cases. This keyword is only supported in release 12.2 and higher.
inter-rat security-ctxt { allow-mapped | native }

Configure inter-RAT parameters for TAU. This keyword provides the operator with the option of continuing with the mapped context or creating a new native context after an inter-RAT handover.

- **allow-mapped**: Configures inter-RAT security-context type as mapped. Mapped security context is allowed after inter-RAT handover. This is the default value.

- **native**: Configures inter-RAT security-context type as native only. Inter-RAT handover will always result in a native security context.

**Usage**

Use this command to define tracking area update procedures such as inter-RAT security context and IMEI query-type.

**Example**

The following command sets the IMEI query type to IMEI-SV:

```plaintext
tau imei-query-type imei-sv verify-equipment- identity
```
treat-as-hplmn

Enables or disables the SGSN to treat an IMSI series as coming from the home PLMN.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Call Control Profile Configuration

configure > call-control-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-call-control-profile-profile_name)#

Syntax

[ remove ] treat-as-hplmn

remove

Deletes this configuration from the profile. This would disable this function and is the default.

Usage

Use this command to enable or disable the SGSN to treat an IMSI series as coming from the home PLMN.

Example

The following command disables previously configured feature:

remove treat-as-hplmn
vplmn-address

Enables/disables the SGSN to override the VPLMN address-allowed flag.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Call Control Profile Configuration

Configure > call-control-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-call-control-profile-profile_name)#

Syntax

vplmn-address { allowed | not-allowed }

remove vplmn-address

remove
Using remove disables the override behavior and the VPLMN-Address-Allowed flag is interpreted as it is in the subscription data.

allowed
Using allowed instructs the SGSN to set the VPLMN-Address-Allowed flag during GGSN selection - even if the flag was not received in the subscription data from the HLR.

not-allowed
Using not-allowed instructs the SGSN not to set the VPLMN-Address-Allowed flag during GGSN selection - even if the flag is received in the subscription data from the HLR.

Usage
Use this command to override the VPLMN-Address-Allowed flag received in subscription data from HLR during GGSN selection. This flag is used to decide whether to use the VPLMN-OI received from a roaming subscriber to form the full-APN. The full-APN is then used in a DNS query to select a GGSN. This override enables the operator to control selection of a different GGSN for a roaming subscriber by using/not-using VPLMN-OI in full-APN.

Example
The following command instructs the SGSN to set the VPLMN-Address-Allowed flag during GGSN selection, even if the flag was not received in subscription data from the HLR:

vplmn-address allowed

The following command instructs the SGSN not to set the VPLMN-Address-Allowed flag during GGSN selection, even if the flag was received in subscription data from the HLR:
vplmn-address not-allowed

The following command instructs the SGSN not to override standard behavior regarding the VPLMN-Address-Allowed flag:

remove vplmn-address
**zone-code**

Configures a zone code listing of one or more location area code (LACs) included in the zone.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Call Control Profile Configuration

```
configure > call-control-profile profile_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-control-profile-profile_name)#
```

**Syntax**

```
zone-code zc_id location-area-code lac

no zone-code zc_id [ location-area-code lac ]
```

**no**
Removes either a specific LAC from the zone code list. If the `location-area-code` parameter is not included in the command, then the entire zone code list definition is removed from configuration.

**zc_id**
Identifies an instance of a zone code list as an integer from 1 to 65535. An unlimited number of zone code lists can be configured per call control profile as the zone code lists are allocated dynamically. A maximum of 10 zone code lists can be configured per Call Control Profile.

**location-area-code lac**
Prompts for the location area-code(s), where the subscribers can roam, that are part of the zone. `lac` is an integer from 1 to 65535. Repeat the command with this parameter to include up to 100 LACs in the zone code list.

**Usage**

![Important:]
While there is no limit to the number of zone codes that can be created, only 10 LACs per zone code can be defined.

Use this command to define zone code restrictions. Regional subscription data at the home location register (HLR) is used to determine the regional subscription area in which the subscriber is allowed to roam. The regional subscription data consists of a list of zone codes. A zone code is comprised of one or more location areas (identified by a LAC) into which the subscriber is allowed to roam. Regional subscription data, if present in the insert subscriber data (ISD) request from the HLR, defines the subscriber's subscription area for...
the addressed SGSN. It contains the complete list (up to 10 zone codes) that apply to a subscriber in the currently visited PLMN.
During the GPRS Location Update procedure, the zone code list is received in the ISD request from the HLR. The zone code list from the HLR is validated against the configured values in the operator policy. If matched, then the ISD is allowed to proceed. If not matched, then the ISD response is that the Network Node Area is Restricted and the GPRS Location Update procedure fails. If no zone codes are included in the ISD (whether or not the zone codes are defined in the SGSN configuration), then checking is not done.

Example

The following command defines multiple LACs for zone code 1:

```
zone-code 1 lac 413 212 113
```
Chapter 38
Call-Home Configuration Mode

The Call-Home Configuration Mode sets parameters for the Smart Call Home feature. Smart Call Home is a contracted service that sends real-time alerts, remediation, and personalized web-based reports to the Cisco Technical Assistance Center (TAC) and other configured receivers.

Mode

Exec > Global Configuration > Call-Home Configuration

cfg > call-home

Entering the above command sequence results in the following prompt:

[local]host_name(config-call-home)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
activate

Activates the Cisco Smart Call Home service.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Call-Home Configuration

```bash
configure > call-home
```
Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-home)#
```

**Syntax**

- `activate`
- `default activate`
- `no activate`

**Usage**

Use this command to enable the call-home services.

**Example**

The following command disables the call-home service:

```bash
no activate
```
alert-group

Enables or disables the Smart Call Home alert-group.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Call-Home Configuration
configure > call-home

Entering the above command sequence results in the following prompt:

[local]host_name(config-call-home)#

**Syntax**

```
[ default | no ] alert-group { all | configuration | crashinfo | diagnostic | environment | inventory | syslog }
```

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>default</strong></td>
<td>Configures the alert-group back to default settings. The default is enabled.</td>
</tr>
<tr>
<td><strong>no</strong></td>
<td>Disables the alert-groups.</td>
</tr>
<tr>
<td><strong>alert-group all</strong></td>
<td>Enables an alert group for all categories.</td>
</tr>
<tr>
<td><strong>alert-group configuration</strong></td>
<td>Enables an alert group related to configuration.</td>
</tr>
<tr>
<td><strong>alert-group crashinfo</strong></td>
<td>Enables an alert group related to crashes.</td>
</tr>
<tr>
<td><strong>alert-group diagnostics</strong></td>
<td>Enables an alert group related to diagnostics.</td>
</tr>
<tr>
<td><strong>alert-group environment</strong></td>
<td>Enables an alert group related to environment. These typically include events related to power, fan, and temperature alarms.</td>
</tr>
<tr>
<td><strong>alert-group inventory</strong></td>
<td>Enables an alert group related to inventory. This is a non-critical event that could include notifications when cards are inserted or removed, or when the system is cold-booted.</td>
</tr>
</tbody>
</table>
**alert-group syslog**

Enables an alert group related to syslog. This includes events generated by the syslog PORT facility.

**Usage**

An alert group is a predefined subset of Smart Call Home alerts that are supported on this device. Alert groups allow you to select the set of Smart Call Home alerts that you want to send to a predefined or custom destination profile.

**Example**

The following command enables alerts for all of the preconfigured Smart Call Home alerts:

```
alert-group all
```
**contact-email-addr**

Sets the e-mail address of the person identified as the prime contact for this system.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Call-Home Configuration

```
configure > call-home
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-home)#
```

**Syntax**

```
[ no ] contact-email-addr email_addr
```

---

**no**

Removes the contact e-mail address.

```
contact-email-addr email_addr
```

Specifies the information for prime contact as an alphanumeric string in the format `local-part@domain`, where domain can be made up of a number of labels, each separated by a period and between 1 and 63 characters in length. The local-part can be 1-64 characters. The domain-label can be 1-63 characters. The domain can be 1 through 135 characters. The entire alphanumeric string can be a no larger than 200 characters.

**Usage**

Use this command to set up the e-mail address for the person identified as the contact person for this device.

**Important:** You can enter any valid e-mail address. You cannot use spaces.

**Example**

The following command specifies e-mail address for the entity `notity.TAC@NOCservices.net`:

```
contact-email-addr notity.TAC@NOCservices.net
```
contract-id

Configures the system’s contract-identifier for Cisco AutoNotify.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Call-Home Configuration

configure > call-home

Entering the above command sequence results in the following prompt:

[local] host_name(config-call-home) #

Syntax

[ default | no ] contract-id contractID

default

Configures the call-home contract-id back to default settings.

no

Removes the call-home contract-id.

contract-id contractID

Specifies the call-home contract-id as an alphanumeric string of 1 through 64 characters that is case sensitive. If you include spaces in this string, you must enclose it in double quotation marks.

Usage

Use this command to enter this system’s AutoNotify contract ID.

Example

The following command specifies the contract-id as Contract1234_ID:

  contract-id Contract1234_ID
customer-id

Configures the system’s customer-identifier for Cisco AutoNotify.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Call-Home Configuration
configure > call-home

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-home)#
```

**Syntax**

```
[ default | no ] customer-id customerID
```

- **default**
  Configures the call-home customer-id back to default settings.

- **no**
  Removes the call-home customer-id.

- **customer-id**
  Specifies the call-home customer-id as an alphanumeric string of 1 through 64 characters that is case sensitive. If you include spaces in the string, you must enclose it in double quotation marks.

**Usage**

Use this command to set up the system’s customer ID for Cisco’s AutoNotify.

**Example**

The following command specifies the customer-id as `CustID_1234`:

```
customer-id CustID_1234
```
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

`exit`

Usage

Use this command to return to the parent configuration mode.
mail-server

Configures the Smart Call Home mail-server.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Call-Home Configuration

configure > call-home

Entering the above command sequence results in the following prompt:

[local]host_name(config-call-home)#

Syntax

[ no ] mail-server server_name priority priority_num

no
Removes the call-home mail-server.

mail-server server_name
Identifies the mail server as an alphanumeric string of 1 through 64 characters. The server ID can take the form of a host name (DNS) or an IPv4 address in dotted-decimal notation.

priority
Sets the mail server priority order as an integer from 1 (highest) to 100 (lowest).

Usage
Use this command to set up the mail server for Smart Call Home. This configuration is mandatory when the user profile is configured to only send out e-mail messages.

Example
The following command specifies the mail-server as 10.2.3.4 with a priority of 1:

    mail-server 10.2.3.4 priority 1
phone-number

Enables or disables the phone-number for the Smart Call Home contact person.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Call-Home Configuration
configure > call-home

Entering the above command sequence results in the following prompt:

[local]host_name(config-call-home)#

Syntax

[ no | default ] phone-number phone-number-string

default
Configures the phone number back to default settings. The default is enabled.

no
Removes the call-home phone number.

phone-number phone-number-string
Specifies the phone number for the contact person for this system as an alphanumeric string that can only contain: + (plus sign), - (dash) and numbers. The total length of the string is 12 to 16 characters. If you include spaces, you must enclose the string in double quotation marks.

Usage
Use this command to set up the phone number for Smart Call Home contact.

Example
The following command specifies the phone number as +866-111-2234:

phone-number 866-111-2234
profile

Creates the Smart Call Home profile.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Call-Home Configuration
configure > call-home

Entering the above command sequence results in the following prompt:

[local]host_name(config-call-home)#

Syntax

[ no ] profile profile_name

no
Removes the call-home profile.

profile profile_name
Creates or modifies the profile name for this system as an alphanumeric string of 1 through 31 characters.

Usage

Use this command to create a new profile or modify an existing profile. This command moves you to the Call-Home Profile Configuration mode.

Example

The following command creates a profile named Profile_1:

profile Profile_1
rate-limit

Enables or disables the message rate-limit for Smart Call Home features.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Call-Home Configuration
 configure > call-home
Entering the above command sequence results in the following prompt:

[local]host_name(config-call-home)#

Syntax

[ no | default ] rate-limit message_count

__default__
Sets the rate limit back to the default of 20 messages per minute.

__no__
Removes the call-home rate-limit.

rate-limit message_count
Sets the rate limit in messages per minute. message_count is an integer from 1 to 60. Default: 20

Usage
Use this command to configure the call-home message rate limit per minute. The default is 20 messages per minute.

Example
The following command sets the call-home rate limit to 10:

    rate-limit 10
sender

Specifies the Smart Call Home e-mail settings for the “from” address and “reply-to” address.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Call-Home Configuration

configure > call-home

Entering the above command sequence results in the following prompt:

[local]host_name(config-call-home)#

Syntax

[ no | default ] sender { from email_address | to email_address }

- **default**
  Sets the sender back to the default.

- **from email_address**
  Sets the sender’s reply from address.

- **no**
  Removes the call-home sender.

- **to email_address**
  Sets the sender’s reply-to address.

- **email_address**
  This is an alphanumeric string in the format `local-part@domain`, where domain can be made up of a number of labels, each separated by a period and between 1 and 63 characters in length. The local-part can be 1-64 characters. The domain-label can be 1-63 characters. The domain can be 1 through 135 characters. The entire alphanumeric string can be a no larger than 200 characters.

Usage

Use this command to specify the e-mail settings for the sender. This command sets the “to” and “from” fields in the e-mail.

Example

The following command sets the from address to `notity.TAC@NOCservices.net` and the reply-to address to `support@cisco.com`:

```
   semder from notity.TAC@NOCservices.net to support@cisco.com
```
site-id

Specifies the Smart Call Home site identifier for this system.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Call-Home Configuration

configure > call-home

Entering the above command sequence results in the following prompt:

[local]host_name(config-call-home)#

**Syntax**

```
[ default | no ] site-id siteID
```

- **default**
  
  Sets the site-id back to the default.

- **no**

  Removes the call-home site-id.

- **site-id siteID**

  Specifies the site ID as an alphanumeric string of 1 through 200 characters. If you include spaces, then you must enclose your entry in quotes.

**Usage**

Use this command to specify the Smart Call Home site identifier for this system.

**Example**

The following command sets the site-id to `NOC_Services_site_1011`:

```
site id NOC_Services_site_1011
```
street-address

Specifies the Smart Call Home street address for the system.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Call-Home Configuration

configure > call-home

Entering the above command sequence results in the following prompt:

[local]host_name(config-call-home)#

Syntax

[ default | no ] street-address streetADR

default
Sets the street-address back to the default.

no
Removes the call-home street-address.

street-address streetADR

Specifies the Smart Call Home street-address as an alphanumeric string of 1 through 200 characters. You can include the street address, City, State, and ZIP Code. If you include spaces, then you must enclose the string in double quotation marks.

Usage

Use this command to set up the street address for the system.

Example

The following command sets the street address to 123 Main St., Chicago, IL 60000:

street-address “123 Main St., Chicago, IL 60000”
The Call-Home Profile Configuration Mode is used to create groups of users that will receive alerts when events occur. The Smart Call Home service sends real-time alerts, remediation, and personalized web-based reports to the Cisco Technical Assistance Center (TAC) and other configured receivers.

Mode

Exec > Global Configuration > Call-Home Configuration > Call-Home Profile Configuration

configure > call-home > profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-call-home-profile)#

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
active

Activates this Smart Call Home profile.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Call-Home Configuration > Call-Home Profile Configuration
configure > call-home > profile profile_name
Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-home-profile)#
```

**Syntax**

```
active

default active

no active
```

**default**
Configures the call-home profile back to default settings. By default, the profile is enabled.

**no**
Deletes the call-home profile.

**activate**
Activates this Smart Call Home profile.

**Usage**

Use this command to activate or deactivate this call-home profile. By default, the profile is enabled.

**Example**

The following command disables the call-home profile:

```
no active
```
destination

Configures the message destinations for this Smart Call Home profile.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Call-Home Configuration > Call-Home Profile Configuration
configure > call-home > profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-call-home-profile) #

Syntax


default destination [ message-size-limit | preferred-msg-format | transport-method ]


destination

Configures an destination e-mail address or HTTP URL where short-text/long-text call-home message and XML-based call-home messages will be sent.

- **email**: Use this option to add an e-mail address to this profile. *email_addr* is an alphanumeric string of the form local-part@domain where domain can be made up of a number of labels, each separated by a period and between 1 and 63 characters in length. The local-part can be 1-64 characters. The domain-label can be 1-63 characters. The domain can be 1-135 characters. The entire alphanumeric string can be a no larger than 200 characters.

- **http**: Use this option to add an HTTP URL to this profile. *http_url* is an alphanumeric string of 1 through 200 characters.

default

Configures the call-home profile back to default settings. By default, the profile is enabled.

message-size-limit size

Specifies the message size (in bytes) for this profile as an integer from 50 to 3145728. The default is 3145728.

no

Deletes the call-home profile.
Call-Home Profile Configuration Mode

preferred-msg-format [ long-text | short-text | xml]

Specifies the message format for the profile. The default is xml.

- **long-text**: Use this option to set long-text messages as the preferred message format. The long message format has all the details related to the event, including information related to chassis, card, and outputs of show commands for the alert group.

- **short-text**: Use this option to set short-text messages as the preferred message format. The short message has information on the severity of event, a short description of the event, the event time, and the device ID.

- **xml**: Use this option to set XML as the preferred message format. (Default)

transport-method [ email email_address | http http_url ]

Specifies the transport-method for the messages. The default is e-mail. For the user profile, both e-mail and http can be enabled. If all are options are disabled, e-mail will be set for the profile.

For the Cisco TAC profile, only one transport method can be enabled. If the user enables a second transport method, the first one will be automatically disabled.

- **email**: Enables an e-mail address for this profile. This is the default.

- **http**: Enables an HTTP URL for this profile.

Usage

Use this command to activate the current call-home profile. By default, the profile is enabled.

Example

The following command disables the call-home profile:

```
no destination
```

The following command sets the preferred message format for the profile to the call-home profile to short text:

```
destination preferred-msg-format short-text
```
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Use this command to return to the parent configuration mode.
**subscribe-to-alert-group**

Subscribes this profile to the alert group for the call-home profile.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Call-Home Configuration > Call-Home Profile Configuration

`configure > call-home > profile profile_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-call-home-profile)#
```

**Syntax**

```
subscribe-to-alert-group [ all {severity [catastrophic | disaster | fatal | critical | major | minor | warning | notification | normal ] } | configuration { periodic [daily | monthly | weekly]} } | crashinfo | diagnostic {severity [catastrophic | disaster | fatal | critical | major | minor | warning | notification | normal ] } | environment {severity [catastrophic | disaster | fatal | critical | major | minor | warning | notification | normal ] } | inventory {periodic [daily | monthly | weekly]} } | syslog {severity [catastrophic | disaster | fatal | critical | major | minor | warning | notification | normal } ] ]

default subscribe-to-alert-group

no subscribe-to-alert-group [ all {severity [catastrophic | disaster | fatal | critical | major | minor | warning | notification | normal ] } | configuration { periodic [daily | monthly | weekly]} } | crashinfo | diagnostic {severity [catastrophic | disaster | fatal | critical | major | minor | warning | notification | normal ] } | environment {severity [catastrophic | disaster | fatal | critical | major | minor | warning | notification | normal ] } | inventory {periodic [daily | monthly | weekly]} } | syslog {severity [catastrophic | disaster | fatal | critical | major | minor | warning | notification | normal } ] [pattern pattern_to_match] ]
```

Enables call-home messages based for all group-types and severity for the profile. The following severities are supported:

- **catastrophic** – Level 1: catastrophic event, matches platform logging level critical.
- **disaster** – Level 2: disaster event, matches platform logging level critical.
- **fatal** – Level 3: fatal event, matches platform logging level critical.
- **critical** – Level 4: critical event, matches platform logging level critical.
- **major** – Level 5: major event, matches platform logging level error.
- **minor** – Level 6: minor event, matches platform logging level warning.
• **warning** – Level 7: warning event, matches platform logging level warning.
• **notification** – Level 8: notification event, matches platform logging level unusual.
• **normal** – Level 9: normal event, matches platform logging level info.

**configuration { periodic [ daily | monthly | weekly] }**

Enables call-home messages based for configuration alert groups. The messages are sent at periodic intervals such as:

• **daily**: Sends a daily call-home message.
• **monthly**: Sends a monthly call-home message.
• **weekly**: Sends a weekly call-home message.

**crashinfo**

Configures the call-home profile back to default settings. By default, the profile is enabled.

**default**

Restores the parameter back to the default value.

**diagnostic { severity [ catastrophic | disaster | fatal | critical | major | minor | warning | notification | normal ] }**

Enables call-home messages based for diagnostic group-types and severity for the profile. The following severities are supported:

• **catastrophic** – Level 1: catastrophic event, matches platform logging level critical.
• **disaster** – Level 2: disaster event, matches platform logging level critical.
• **fatal** – Level 3: fatal event, matches platform logging level critical.
• **critical** – Level 4: critical event, matches platform logging level critical.
• **major** – Level 5: major event, matches platform logging level error.
• **minor** – Level 6: minor event, matches platform logging level warning.
• **warning** – Level 7: warning event, matches platform logging level warning.
• **notification** – Level 8: notification event, matches platform logging level unusual.
• **normal** – Level 9: normal event, matches platform logging level info.

**environment { severity [ catastrophic | disaster | fatal | critical | major | minor | warning | notification | normal ] }**

Enables call-home messages based for environment group-types and severity for the profile. The following severities are supported:

• **catastrophic** – Level 1: catastrophic event, matches platform logging level critical.
• **disaster** – Level 2: disaster event, matches platform logging level critical.
• **fatal** – Level 3: fatal event, matches platform logging level critical.
• **critical** – Level 4: critical event, matches platform logging level critical.
• **major** – Level 5: major event, matches platform logging level error.
• **minor** – Level 6: minor event, matches platform logging level warning.
• **warning** – Level 7: warning event, matches platform logging level warning.
Call-Home Profile Configuration Mode

subscribe-to-alert-group

- **notification** – Level 8: notification event, matches platform logging level unusual.
- **normal** – Level 9: normal event, matches platform logging level info.

**inventory { periodic [ daily | monthly | weekly ] }**

Enables call-home messages based for inventory alert groups. The messages are sent at periodic intervals such as:

- **daily**: Sends a daily call-home message.
- **monthly**: Sends a monthly call-home message.
- **weekly**: Sends a weekly call-home message.

**no**

Deletes the alert groups.

**syslog { severity [catastrophic | disaster | fatal | critical | major | minor | warning | notification | normal ] [ pattern pattern_to_match ] }**

Enables and disables call-home messages based on severity and syslog string pattern match for the profile. The following severities are supported:

- **catastrophic** – Level 1: catastrophic event, matches platform logging level critical.
- **disaster** – Level 2: disaster event, matches platform logging level critical.
- **fatal** – Level 3: fatal event, matches platform logging level critical.
- **critical** – Level 4: critical event, matches platform logging level critical.
- **major** – Level 5: major event, matches platform logging level error.
- **minor** – Level 6: minor event, matches platform logging level warning.
- **warning** – Level 7: warning event, matches platform logging level warning.
- **notification** – Level 8: notification event, matches platform logging level unusual.
- **normal** – Level 9: normal event, matches platform logging level info.

*pattern_to_match* is an alphanumeric string of 1 through 80 characters.

**Usage**

Use this command to enable or disable the call-home messages based on specified alert-groups and severities for the profile.

**Example**

The following command sets an alert group for the profile to send a daily inventory message:

```
subscribe-to-alert-group inventory periodic daily
```
Chapter 40
CAMEL Service Configuration Mode Commands

The CAMEL Service configuration mode provides a set of commands to define the parameters for the Customized Applications for Mobile networks Enhanced Logic (CAMEL) service functionality and the CAMEL interface - the Ge interface.

CAMEL service enables operators of 2.5G/3G networks to provide operator-specific services (such as prepaid GPRS service and prepaid SMS service) to subscribers, even when the subscribers are roaming outside their home public land mobile network (HPLMN).

Mode

Exec > Global Configuration > Context Configuration > CAMEL Service Configuration

configure > context context_name > camel-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-camel-service)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
associate-sccp-network

Configure an association between this CAMEL service and a specified SCCP network.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CAMEL Service Configuration
configure > context context_name > camel-service service_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-camel-service)#
```

**Syntax**

```
associate-sccp-network sccp_network_id
no associate-sccp-network
```

**no**

Removes the association with the CAMEL service configuration.

```
sccp_network_id
```

Identifies an already defined SCCP network.

```
sccp_network_id: Enter an integer from 1 to 12.
```

**Usage**
The SCCP network must be configured prior to use this command. CAMEL service will not function unless an SCCP network is associated.

**Example**
Associate this CAMEL service with SCCP network configuration ID 2:

```
associate-sccp-network2
```
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
exit
```

Usage
Use this command to return to the parent configuration mode.
tcap destination-address

Configure the gsmSCF address to be used to open TC dialogues.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > CAMEL Service Configuration
configure > context context_name > camel-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-camel-service)#

Syntax

tcap destination-address { configured-address | received-address }

default tcap destination-address

configured-address
Default.
Instructs the SGSN to use the SCF address from the GPRS-CSI.

received-address
Instructs the SGSN to overwrite the gsmSCF address with the memorised gsmSCF address that was in the first response message to the InitialDPGPRS and then to use that gsmSCF address.

Usage
This command enables the operator to determine which gsmSCF address is to be used to open new TC dialogues. In accordance with 3GPP 29.078, section 14.1.4.1.3, this command enables the SGSN to establish new TC dialogues within the context of a current GPRS dialogue, based on the operators choice:
- to use a ‘received-address’ where the gprsSSF learns the gsmSCF address used in the first response message to the InitialDPGPRS and uses it to open new TC dialogues, or
- to use a ‘configured-address’ where the gprsSSF uses the gsmSCF address from the GPRS-CSI to open new TC dialogues.

Example
Configure the SGSN to overwrite the SCF address and to use the gsmSCF address received in the response message:

tcap destination-address received-address
timeout

Configure a range of timers needed to support CAMEL service.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > CAMEL Service Configuration

`configure > context context_name > camel-service service_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-camel-service)#
```

Syntax

```
timeout { gprs-apply-charging-report-ack-timer seconds | gprs-entity-release-ack-timer seconds | gprs-event-report-ack-timer seconds | gprs-tssf-timer seconds | sms-event-report-ack-timer seconds | sms-tssf-timer seconds | tc-guard-timer seconds }


default
```

Resets the timers to default values.

```
gprs-apply-charging-report-ack-timer seconds
```

Configure the TCAP invoke timer to set the length of time the SGSN waits for an acknowledgement after sending an ApplyChargingReportGPRS to the SCF.

`seconds`: Enter an integer from 1 to 20. Default: 4

**Important**: This timer value should be less than the value configured for the `tc-guard-timer`.

```
gprs-entity-release-ack-timer seconds
```

Configure the TCAP invoke timer to set the length of time the SGSN waits for an acknowledgement from the SCF after sending Entity Release information.

`seconds`: Enter an integer from 1 to 20. Default: 4

```
gprs-event-report-ack-timer seconds
```

Configure the TCAP invoke timer to set the length of time the SGSN waits for an acknowledgement from the SCF after the SGSN sends an event report.

`seconds`: Enter an integer from 1 to 20. Default: 4
**gprs-tssf-timer seconds**
Configure the GPRS TSSF timer to set the length of time the SGSN waits for an instructions from the SCF. On expiry the SGSN handles the transaction through the default handling specified in the corresponding CSI.
*seconds*: Enter an integer from 1 to 10. Default: 5

**sms-event-report-ack-timer seconds**
Configure the TCAP invoke timer to set the length of time the SGSN waits for an acknowledgement from the SCF after the SGSN sends an event report for SMS.
*seconds*: Enter an integer from 1 to 20. Default: 4

**sms-tssf-timer seconds**
Configure the SMS TSSF timer to set the length of time the SGSN waits for an instructions from the SCF. On expiry the SGSN handles the transaction through the default handling specified in the corresponding CSI.
*seconds*: Enter an integer from 1 to 10. Default: 5

**tc-guard-timer seconds**
Configure the guard tier to start when the SGSN sends ApplyChargingReportGPRS to the SCF. On expiry the SGSN closes the TCAP dialogue if the GPRS Dialogue state is “monitoring”. Default handling complies with 3GPP 23.078.
*seconds*: Enter an integer from 1 to 10. Default: 5

**Important:** This timer value should be greater than the value configured for the gprs-apply-charging-report-ack-timer.

### Usage
The SCCP network must be configured prior to use this command. CAMEL service will not function unless an SCCP network is associated. Repeat the command to configure multiple timers.

### Example
Set the tc-guard timer for 4:

```
tc-guard-timer 4
```
Chapter 41
Card Configuration Mode Commands

Use the Card configuration mode to create and manage the physical cards in the chassis.

**Mode**

Exec > Global Configuration > Card Configuration

```
configure > card card_number
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-card- slot_number)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
aps

Configures the parameters for the automatic protection switching (APS) feature for SONET CLC2 and OLC2 line cards or for multiplexed section (or switching) protection (MSP) type APS for SDH CLC2 and OLC2 line cards. (ASR 5000 only)

⚠️ Important: This command should only be used after APS has been enabled with the **aps-mode** keyword of the **redundancy** command.

**Product**  
SGSN

**Privilege**  
Security Administrator, Administrator

**Mode**  
Exec > Global Configuration > Card Configuration  
**configure > card** card_number

Entering the above command sequence results in the following prompt:

[local]host_name(config-card- slot_number)#

**Syntax**

```plaintext
aps [ 1+1 ] [ uni-directional ] [ non-revertive ] [ -noconfirm ]
no aps
default aps
```

**1+1**

Selects 1+1 line (linear) protection. Traffic is carried simultaneously by the working line and the protection line. GR-253 and ITU-T G.783 require the bridging to be done at the electrical level; therefore, the same payloads are transmitted over the working and protection lines.

**no**

This keyword has been deprecated for releases 14.0 and higher. To disable APS, enter **redundancy port-mode** in this command mode.

For releases prior to 14.0, this keyword disables APS.

**default**

This option is equivalent to: **aps 1+1 uni-directional non-revertive**. This option is only available in releases 14.0 and higher.

**uni-directional**

Enables protection on one end of the connection.
**non-revertive**
Prevents the network from automatically reverting to the original working line/port when the original working line/port is recovered/restored.

**-noconfirm**
Executes the command without additional prompting for command confirmation.

---

**Usage**

*Important:* At this time, it is not necessary to use the `aps` command to configure parameters as all of these parameters are enabled by default when the APS feature is enabled with the `aps-mode` keyword of the `redundancy` command.

Use this command to configure feature parameters for the APS function for SONET CLC2 and OLC2 line cards or to configure MSP-type APS for SDH CLC2 and OLC2 line cards. Based on the card framing configuration (SONET or SDH), the system automatically knows whether the feature is APS or MSP.

**Example**
As all parameters are included by default it is only necessary to enter the command:

```
  aps
```
end

Exits the current configuration mode and returns to the Exec mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

```plaintext
end
```

**Usage**

Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

exit

Usage
Use this command to return to the parent configuration mode.
framing

Configures the type of framing to be used for the signaling generated on a specific line card. (ASR 5000 only)

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Card Configuration
configure > card card_number

Entering the above command sequence results in the following prompt:

[local]host_name(config-card- slot_number)#

Syntax

framing { ethernet | sdh [ ds1 | e1 ] [ ss-bits ] | sonet [ ds1 | e1 ] | unspecified } [ -noconfirm ]

default framing [ -noconfirm ]

default
Reset the framing generated by the card to the default for the particular card type.

ethernet
Configures the system to use Ethernet framing for this line card. This type of framing can only be used on an Ethernet card.
Default: Ethernet framing type is the default for an Ethernet line card.

Important: Using this keyword with an OLC/OLC2 or CLC/CLC2 takes the card offline.

sdh [ ds1 | e1 ] [ ss-bits ]
Configures the system to use SDH signal framing for either an OLC/OLC2 or CLC/CLC2 line card in an SGSN.

Important: Using this keyword with an Ethernet line card takes the line card offline.

In releases 8.1 and higher, you can also set the type of signaling path for a CLC2.

ds1 - configures the card to support a DS1/T1.
e1 - configures the card to support an E1. This is the default for SDH.
ss-bits - enables/disables use of ss-bits (per ITU 1997 G.783 specification) for SDH configured line card.
sonet [ ds1 | el ]

Configures the system to use SONET signal framing for either an OLC/OLC2 or CLC/CLC2 line card in an SGSN.
Default: SONET is the default framing type for an OLC/OLC2 or CLC/CLC2 line card.

**Important:** Using this keyword with an Ethernet line card takes the line card offline.

In releases 8.1 and higher, you can also set the type of signaling path for a CLC2.
- **ds1** - configures the card to support a DS1/T. This is the default for SONET.
- **el** - configures the card to support an E1.

**unspecified**

Configures the system to use the default framing type for the particular line card resident in the identified slot.

**-noconfirm**

Instructs the system to execute the command without additional prompting for command confirmation.

**Usage**

Use the `framing` command to identify the type of signal framing to be used by the line card in the identified slot.
Note that each type of line card uses a different type of signal framing. If you configure the wrong framing type for a line card, the line card is taken offline.

**Important:** This command is not supported on all platforms.

**Example**

Use the following command to configure SDH signal framing on a CLC2. If you do not include the path-type, the default of `el` is automatically included in the card’s framing configuration:

```
framing sdh
```
header-type

Defines the size of the header frame for Frame Relay transmissions over a CLC or CLC2 channelized line card. (ASR 5000 only)

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Card Configuration

configure > card card_number

Entering the above command sequence results in the following prompt:

[local]host_name(config-card- slot_number)#

Syntax

header-type header-size [ -noconfirm ]

default header-type [ -noconfirm ]

default

Resets the configuration to the default header size of 2-bytes.

header-size

Sets the size, number of bytes, for the header frame. header-size must be either 2-bytes or 4-bytes.

-noconfirm

Executes the command without additional prompting for command confirmation.

Usage

Use this command to set the size of the header frame for Frame Relay messages emanating from the line card. The size (2-bytes or 4-bytes) determines the amount of information that can be transmitted in that first information frame.

Important: Not supported on all platforms

Example

Set the header to the smallest size.

    header-type 2-byte
**initial-e1-framing**

Configures the type of framing mode that will initially be available at the time the line card boots. (ASR 5000 only)

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Card Configuration

`configure > card card_number`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-card- slot_number)#
```

**Syntax**

```
initial-e1-framing [ crc4 | standard ]
```

**Usage**

For a CLC-type line card, the default E1 framing mode is CRC4. When a card reboots, all E1s are initialized with CRC4 framing mode and then switch to the configured framing mode. With this keyword, you have the option to choose the initialization framing mode.

**Important:** Only supported on CLC/CLC2

**Example**

```
initial-e1-framing standard
```
link-aggregation

Configures system priority and toggle link settings for Link Aggregation. These parameters are usually changed to match the feature requirements of the remote Ethernet switch.

Product

- WiMAX
- PDSN
- HA
- FA
- GGSN
- SGSN

Privilege

- Security Administrator, Administrator

Mode

Exec > Global Configuration > Card Configuration

`configure > card card_number`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-card- slot_number)#
```

Syntax

```
link-aggregation { system-priority priority | toggle-link } [-noconfirm ]

{ default | no } link-aggregation { system-priority | toggle-link } [-noconfirm ]
```

- **default**
  
  Resets the configuration to the default.

  ```
  link-aggregation system-priority priority
  ```

  This command sets the system priority used by Link Aggregation Control Protocol (LACP) to form the system ID.

  *priority* is a hexadecimal value from 0x0000 through 0xFFFF. Default is 0x8000 (32768).

- **toggle-link**

  Sets the system to toggle link on port switch.

  ```
  -noconfirm
  ```

  Executes the command without additional prompting for command confirmation.
Usage
The system MAC address (6 bytes) and system priority (2 bytes) combine to form the system ID. A system consists of a packet processing card and its associated ASR 5000 QGLCs or XGLCs, or ASR 5500 MIO traffic ports. The highest system ID priority (the lowest number) handles dynamic changes. For additional usage and configuration information for the link aggregation feature, refer to the System Administration Guide.

Important: Not supported on all platforms

Example
The following command configures the link aggregation system-priority to 10640 (0x2990):

    link-aggregation system-priority 0x2990
**mode**

Sets the application processor card’s current administrative state to active or standby.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Card Configuration

```bash
configure > card card_number
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-card- slot_number)#
```

**Syntax**

```bash
mode { active | standby } [ -noconfirm ]
default mode [ -noconfirm ]
```

**default**

Returns the mode to the default value appropriate to the card type.

The default administrative mode for line cards affects a single card and its mated line card. The default state for line cards in the top shelf is active. The default for line cards in the bottom shelf is standby.

The default administrative state for the SPIO in slot 24 is active and the SPIO in slot 25 is standby.

The default administrative mode for packet processing cards is standby.

**Important:** This command results in a migration of processes if the default mode for a card is different than the current state of the card.

**active**

Defines which card type is to be switched from standby to active state. If a card is present in the slot, the packet processing card is automatically selected depending upon the type of card. If no card is present in the slot, a packet processing card is assumed.

**standby**

Sets the packet processing card in the slot to standby mode.

**Caution:** Switching an active packet processing card to standby deletes all port configurations, including bindings, for the attached line cards.

**-noconfirm**

Executes the command without additional prompting for command confirmation.
Usage
Set the desired mode of mated cards. The card targeted for maintenance is placed in the standby state first. The setting of the mode determines which packet processing cards are to be active and which are to be the standby cards for redundancy. Use this command to configure the set of active and standby packet processing cards. The application processor card’s standby priority is then used in conjunction with the set of standby packet processing cards to determine the order in which the standby cards are used for redundancy support.

Important: Not supported on all platforms

Important: This command results in a migration of processes if the mode specified for the card is different than the current state of the card.

Example
The following commands set the state of a card to active and standby, respectively.

    mode active
    mode standby
redundancy

Configures the type of redundancy for a line card or SPIO. (ASR 5000 only)

Product
PDSN
FA
HA
GGSN
SSGN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Card Configuration
configure > card card_number

Entering the above command sequence results in the following prompt:

[local]host_name(config-card- slot_number)#

Syntax

redundancy { aps-mode | card-mode | port-mode } [ -noconfirm ]
default redundancy [ -noconfirm ]

default
Restores redundancy to port-mode type redundancy.

aps-mode
SGSN only.
Enables automatic protection switching (APS), if the card is either a CLC2 or an OLC2 line card with card framing set to SONET. (Refer to the framing command.)
Enables multiplexed section (or switching) protection (MSP) type APS, if the card is a CLC2 line card with card framing set to SDH. (Refer to the framing command.)

Important: Using this keyword with any card type other than a CLC2 or an OLC2 will take the card offline.

Related parameters: You should consider setting appropriate SDSF BER (signal degrade/signal failure bit error rate) threshold settings. Access the hopath-sdsf, lopath-sdsf, and toh-sdsf commands via the port channelized configuration mode -- for a CLC2 line card refer to the Channelized Port Configuration Mode Commands chapter and for an OLC2 line card refer to the ATM Port Configuration Mode Commands chapter.

card-mode
Specifies no port redundancy is used. This is used mostly for legacy products.
**Important:** This keyword has been made obsolete beginning with Release 14.0.

**port-mode**
Enables port redundancy on line cards or on SPIO cards.
This is the default setting used by the system.

**Important:** Port-type redundancy does not affect line card failover/redundancy operations.

**pseudo-aps-mode**
This command has been deprecated.

**-noconfirm**
Instructs the system to execute the command without additional prompting for command confirmation.

**Usage**
Use this command to configure redundancy on a line card (LC) or a SPIO card. With **port-mode** enabled, if an external network device or cable failure occurs that causes a link down failure on the port, the redundant port is used.

**Important:** Not supported on all platforms

**Important:** You do not need to enter this command for each line card or SPIO card, as the system intuitively understands that if the command is entered for an active line card or SPIO card, the standby line card or SPIO card switches to operate in the same mode. For example, if you enter the **port-mode** command for an LC in slot 17, you automatically enable a redundant line card in slot 33 for port redundant operation.

**Important:** **asp-mode** and **port-mode** are mutually exclusive.

**Example**
The following command sets the redundancy mode to port redundancy.

```
redundancy port-mode
```

The following sets APS/MSP 1+1 inter-card redundancy for the specified OLC2 or CLC2 line card:

```
redundancy aps-mode
```
**redundant with**

Enables side-by-side (SBS) redundancy for XGLCs. (ASR 5000 only)

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Card Configuration

```
configure > card card_number
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-card- slot_number)#
```

**Syntax**

```
redundant with card_number
```

*card_number*

Identifies the neighboring top slot number of the card to pair with the XGLC being configured.

*card_number* is an integer between 1 and 48.

**Important:** Attempting to use this command with any card other than an XGLC takes the card offline.

**Usage**

Use this command during configuration to identify the slot holding the XGLC card that will be used to provide redundancy to the XGLC you are configuring. Entering this command enables SBS redundancy when the two XGLCs occupy two upper (top) slots in a chassis.

**Example**

Pair the card in slot 30 with the card being configured:

```
redundant with 30
```
service-type

Configures the type of service that the CLC or CLC2 line card will support. (ASR 5000 only)

**Important:** Supported in software releases 8.1 and higher.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Card Configuration

```bash
configure > card card_number
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-card- slot_number)#
```

**Syntax**

```
service-type { frame-relay | mtp2| multi-service | pwe3-cesopsn | unspecified } [ -noconfirm ]

default service-type [ -noconfirm ]
```

- **default**
  Returns the card configuration to `unspecified`.

- **frame-relay**
  Configures the card to operate in Frame Relay service mode.

- **mtp2**
  Enables MTP2 type service to support narrowband transmissions.

**Important:** MTP2 functionality is not yet supported.

- **multi-service**
  Enables path-level service for multiple simultaneous services (such as frame-relay and mtp2) to run over a single port. For additional information, see the *Channelized Port Configuration Mode Commands* chapter

- **pwe3-cesopsn**

  **Important:** `pwe3-cesopsn` functionality has been replaced by `mtp2`. 
unspecified
This is the default mode for a CLC or CLC2.

Important: You must configure the line card to one of the available service types or the card will not function.

-noconfirm
Executes the command without additional prompting for user input.

Usage
Use this command to configure the operational service mode for the channelized line card (CLC or CLC2). Once you select the service-type, refer to the Channelized Port Configuration Mode Commands chapter to review the commands needed to configure the parameters for the port.

Example

```
service-type frame-relay
```
shutdown

Configures a card for active service or terminates all processes on the card.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Card Configuration

`configure > card card_number`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-card- slot_number)#
```

**Syntax**

```
[ no ] shutdown
```

- **no**
  - no shutdown enables the card.
  - Enter only the **shutdown** keyword to shut the card down.

**Usage**

Shut down a card to remove it from service or to enable a card to put it into service.

**Important:** Do not use this command to remove a card from service for maintenance. Use the command **card halt** to remove a card for service to avoid changing or deleting the active-mode configuration. See the Exec Mode chapter.

**Important:** Not supported on all platforms

**Example**

The following command shuts down the card:

```
shutdown
```

The following command switches the card to online:

```
no shutdown
```
Chapter 42
CBS Service Configuration Mode Commands

The Cell Broadcasting Service (CBS) Configuration Mode is used to create and manage CBS service instances for the current context.

**Mode**

Exec > Global Configuration > Context Configuration > Cell Broadcasting Service Configuration

```
configure > context context_name cbs-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cbs-service)#
```
bind

This command binds the CBS service to the IP address of a logical interface.

Product
HNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Cell Broadcasting Service Configuration
configure > context context_name cbs-service service_name

Syntax
bind address ip_address port port_number

no bind address

Usage
Use this command to associate or tie a CBS service to a specific logical IP address previously configured in the current context and bound to a port.

Example
The following command binds the CBS service to the interface with an IP address of 192.168.1.111 having port number 8888:

bind address 192.168.1.111 port 8888
cbc-address-validation

This command is used for validation of Cell Broadcasting Centre IP address.

Product
HNB-GW

Privilege
Security Administrator, Administrator

Syntax

[ no ] cbc-address-validation

no

Disables the validation of Cell Broadcasting Centre IP address.

Usage
Use this command to validate the Cell Broadcasting Centre IP address.

Example

The following command validates the Cell Broadcasting Centre IP address:

    cbc-address-validation
**cbc-server**

This command configures the CBC server for cell broadcasting service.

**Product**
HNB-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Cell Broadcasting Service Configuration
c

```bash
configure > context context_name cbs-service service_name
```

Entering the above command sequence results in the following prompt:

```
/context_name>host_name(config-cbs-service)#
```

**Syntax**

```
cbc-server address ipv4_address [ port port_number ] [ secondary-address ipv4_address [ port port_number ] ]
```

**no cbc-server address**

- `no`
  - Disables the previously configured CBC server.

- `ipv4_address`
  - Specifies the IPv4 type IP address of CBC server. `ipv4_address` must be expressed in IPv4 dotted-decimal notation.

- `port`
  - Specifies the TCP port of the CBS service. `port` must be an integer between 1 and 65535. Standard port used for service area broadcast protocol (SABP) is 3452 in case no other port is configured. It is an optional parameter.

- `secondary-address`
  - Specifies the address of other CBC server. `ipv4_address` is an IPv4 address, using dotted-decimal notation.

**Usage**

Use this command to configure the CBC server.

**Example**

The following command configures a CBC server with an IP address of `92.168.1.112` having default port number 3452:

```
cbc-server 92.168.1.112
```
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```end```

**Usage**

Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
exit

**Usage**
Use this command to return to the parent configuration mode.
sabp timer

Configures the Service Area Broadcast Protocol (SABP) procedure timer value.

**Product**
HNB-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Cell Broadcasting Service Configuration

```
configure > context context_name cbs-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cbs-service)#
```

**Syntax**

```
[ default | no ] sabp timer timer_value
```

- **default**
  Restores the SABP timer value to the default: 10 seconds.

- **no**
  Disables the previously configured SABP timer value.

- **sabp timer**
  Configures the SABP timer which is the wait time for receiving the SABP response from a peer.
  
  `timer_value` is an integer value between 1 and 30.

**Usage**

This command is used to set/restore the SABP timer value.

**Example**

The following command configures the SABP timer value to 25:

```
sabp timer 25
```
sabp-class2-aggregation

This command configures the SABP class-2 aggregation timeout.

**Product**
HNB-GW

**Privilege**
Security Administrator, Administrator

**Syntax**

```
sabp-class2-aggregation timeout timeout_value
[ default | no ] sabp-class2-aggregation timeout
```

- **default**
  Restores the SABP class-2 aggregation timeout value to the default: 2 seconds.

- **no**
  Disables the previously configured SABP class-2 aggregation timeout value.

- **sabp-class2-aggregation timeout**
  Configures the SABP class-2 aggregation timeout value. `timeout_value` is an integer value between 1 and 10.

**Usage**
This command is used to configure the SABP class-2 aggregation timeout.

**Example**
The following command configures the SABP class-2 aggregation timeout value to 6:

```
sabp-class2-aggregation timeout 6
```
**tcp-keepalive**

This command is TCP Keepalive timer. It is used to check liveness of Cell Broadcasting Centre. The CBS service must be restarted after setting new values.

**Product**

HNB-GW

**Privilege**

Security Administrator, Administrator

**Syntax**

```
tcp-keepalive idle-timeout idle_timeout_value max-retransmission-count count interval value

[ default | no ] tcp-keepalive
```

- **default**
  Restores the TCP Keepalive timer related values to default: idle-timeout(600 seconds), max-retransmission-count (3) and interval (30 seconds).

- **no**
  Disables the TCP Keepalive timer.

**tcp-keepalive idle-timeout**

This is the time in seconds to wait before checking the liveness of Cell Broadcasting Centre. `timeout_value` is an integer value between 60 and 7200.

**max-retransmission-count**

This is the number of attempts to check liveness of Cell Broadcasting Centre after idle time. `count` is an integer value between 2 and 10.

**interval**

This is the time in seconds between attempts to check liveness of Cell Broadcasting Centre after idle time. `value` is an integer value between 10 and 100.

**Usage**

This command is used to check the liveness of Cell Broadcasting Centre.

**Example**

The following command checks the liveness of Cell Broadcasting Centre with `tcp-keepalive idle-timeout` as 66 seconds, `max-retransmission-count` as 5 and `interval` as 15:

```
tcp-keepalive idle-timeout 66 max-retransmission-count 5 interval 15
```
**tcp-mode**

This command configures the mode of TCP connection.

**Product**
HNB-GW

**Privilege**
Security Administrator, Administrator

**Syntax**

```
tcp-mode { client-server | server-only }
```

- **client-server**
  This specifies that the HNBGW can act either as client or server.

- **server-only**
  This specifies that the HNBGW can act only as server.

**Usage**

This command is used to configure the mode of TCP connection.

**Example**

The following command configures the HNBGW as Client and Server.

```
tcp-mode client-server
```
Chapter 43
Channelized Port Configuration Mode Commands

The channelized port configuration mode provides the commands to create, configure, bind, and manage the Frame Relay service ports on the channelized line card.

Important: The commands described in this chapter only run on the ASR 5000 platform. Before using these commands, card framing should be configured for either SDH or SONET with the framing command described in the Card Configuration Mode chapter.

Mode

Exec > Global Configuration > Channelized Port Configuration

configure > port channelized slot_number/port_number

Entering the above command sequence results in the following prompt:

[local]host_name(config-port-slot_number/port_number)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
alarm-disable

Entering this command disables the alarm detection for designated sets of alarms.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Channelized Port Configuration

```bash
configure > port channelized slot_number/port_number
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-port-slot_number/port_number)#
```

**Syntax**

```
alarm-disable { all | ds1-e1 | none | sonet-sdh }

[ no | default ] alarm-disable
```

- **no**
  Deletes the disable configuration.

- **default**
  Returns the settings for disabling alarms to the system default.

- **all**
  Disables detection of all SONET/SDH and DS1/E1 alarms.

- **ds1-e1**
  Disables detection of the DS1/E1 alarms.

- **none**
  None of the alarm detection is disabled so that all DS1/E1 and SONET/SDH alarms are detected.

- **sonet-sdh**
  Disables detection of SONET/SDH alarms.

**Usage**
Configure selected alarm detection for the port.

**Example**
Enter the following command to enable DS1/E1 and SONET/SDH alarm detection.

```
alarm-disable none
```
alarm-soak-timer

This command sets the timer for the duration that a detected alarm will be soaked before the alarm is reported.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Channelized Port Configuration

```bash
configure > port channelized slot_number/port_number
```

Entering the above command sequence results in the following prompt:

```bash
[local]host_name(config-port-slot_number/port_number)#
```

**Syntax**

```bash
alarm-soak-timer  seconds
default alarm-soak-timer
```

**default alarm-soak-timer**

```bash
default
```

Returns the timer settings to the system default.

```bash
seconds
```

Defines the number of seconds the system waits (soaks the alarm) before reporting the alarm.

*seconds*: any integer from 0 to 32767.

**Usage**

Configures the delay before reporting detected alarms.

**Example**

Configure a 20 second alarm report delay.

```bash
alarm-soak-timer 20
```
clock-source

This command sets the source of the port’s transmit clock.

**Important:** This command is only available for releases 8.1 or higher.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Channelized Port Configuration

```
configure > port channelized slot_number/port_number
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-port-slot_number/port_number)#
```

**Syntax**

```
clock-source { internal-timing | loop-timing }
```

- **default clock-source**

  - **default**
    
      Using this command combination sets the port clock source to internal timing.

  - **internal-timing**
    
      Sets the port clock to derive timing from the recovered receive clock.

  - **loop-timing**
    
      Sets the port clock to transmit in sync with the system timing.

**Usage**

Use this command for either SONET or SDH channelized (Frame Relay) ports on the SGSN.

**Example**

The following command resets the transmit clock source to internal timing.

```
default clock-source
```
description

Defines descriptive text that provides useful information about the port.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Channelized Port Configuration

configure > port channelized slot_number/port_number

Entering the above command sequence results in the following prompt:

[local]host_name(config-port-slot_number/port_number)#

Syntax

description text

no description

no

Erases the port’s description from the configuration file.

text

text must be a string of 1 to 79 alphanumeric characters with no spaces or a string within double quotes that includes printable characters. The description is case-sensitive.

Usage

Set the description to provide helpful information, for example the port’s primary function, services, end users. Define any information, the only limit is the number of characters.

Example

description samplePortDescriptiveText

description “This is a sample description”
dlci

Identifies a data link connection identifier (DLCI), a frame relay logical connection, and binds it with a specific channelized path configuration. Once the DLCI is bound to the path, the system enters DLCI configuration mode.

**Important:** The `path` command must be configured prior to attempting configuration with the `dlci` command.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Channelized Port Configuration

```
configure > port channelized slot_number/port_number
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-port-slot_number/port_number)#
```

**Syntax**

```
dlci path path_id { ds1 | e1 } connects { dlci dlci_id | timeslots slot# dlci dlci_id }
```

```
no dlci path path_id { ds1 | e1 } connects
```

Disables the configured DLCI.

```
path path_id
```

Identifies a specific path configuration, set with the `path` command in this configuration mode, that will be associated with a DLCI.

`path_id` must be an integer from 1 to 3.

```
ds1 connects | e1 connects
```

Selects the framing speed for the connection.

**DS1:** Is associated with North American networks and would be the best choice to work with the SONET framing selected with the `card` configuration command.

`connects:` Defines the number of logical connections supported via the DS1. The selection must be an integer from 1 to 28.

**E1:** Is associated with European networks and would be associated with the SDH framing selected with the `card` configuration command.

`connects:` Defines the number of logical connections supported via the E1. The selection must be an integer from 1 to 21.

```
dlci dlci_id
```

Identifies a specific Frame Relay PVC DLCI to associate with the path.

`dlci_id:` an integer from 16 to 991.
timeslot slot#

Identifies one of the timeslots within a timeslot group configured with the `path` command for the E1, DS1 or fractional E1 port. Identifying one slot in a group means that all the slots in that group will have the Frame Relay parameters configured in the same manner.

*slot#: Must be an integer from 1 to 31.

**Usage**

Associating a routing path with a specific frame relay DLCI is a significant part of the process for defining the frame relay interface.

**Example**

Associate path 1 with DLCI 123.

```
dlci path 1 ds1 21 dlci 123
```
end

Exits the Channelized Port configuration mode and returns to the Exec mode.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**
end

**Usage**
Change the mode back to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Use this command to return to the parent configuration mode.
frame-relay

Configures the parameters for the Frame Relay connections for E1, DS1 and fractional E1 ports created with the `path` command. Frame

⚠️ **Important:** The `path` command must be configured prior to attempting configuration with the `frame-relay` command.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
frame-relay path path_id { dsl connects | el connects } timeslot slot# [ intf-type intf_type ] [ lmi_type lmi_type ]
```

- **path  path_id**
  Identifies a specific path configuration, set with the `path` command in this configuration model. `path_id` must be an integer from 1 to 3.

- **dsl connects | el connects**
  Selects the pipe splitting for the connection. 
  - **DS1:** Is associated with North American networks and would be the best choice to work with the SONET framing selected with the `card` configuration command. DS1 splits the path into 28 logical connections.
  - **connects:** Defines the number of logical connections supported via the DS1. The selection must be an integer from 1 to 28.
  - **E1:** is associated with European networks and would be associated with the SDH framing selected with the `card` configuration command. E1 splits the path into 21 logical connections.
  - **connects:** Defines the number of logical connections supported via the E1. The selection must be an integer from 1 to 21.

- **timeslot  slot#**
  Identifies one of the timeslots within a timeslot group configured with the `path` command for the E1, DS1 or fractional E1 port. Identifying one slot in a group means that all the slots in that group will have the Frame Relay parameters configured in the same manner.
  - `slot#`: Must be an integer from 1 to 31.

- **intf-type  intf_type**
  Selecting the interface type specifies signaling parameters for the DLCI, options include:
  - **dce:** Selects data circuit-terminating equipment -type signaling.
  - **dte:** Selects data terminal equipment -type signaling.
  - **nni:** Selects the network-to-network interface

Default: DTE for Release 8.0
Default: DCE for Release 8.1
**frame-relay lmi_type lmi_type**

Default: **none**.

Line management options include:
- **ansi** - ANSI ANNEXED LMI, may include option:
- **cisco** - Cisco/Gang Of Four LMI
- **none** - LMI Disabled
- **q933a** - Q.933A LMI

Any of the above LMI types can take one or more additional options
- **n391** *value* - Number of keep exchanges before requesting a full status message. Default is 6. *value* must be an integer from 1 to 255.
- **n392** *value* - Error Threshold value. Default is 2. *value* must be an integer from 1 to 10.
- **n393** *value* - Monitored events count value. Default is 2. *value* must be an integer from 1 to 10.
- **t391** *value* - Timer to send messages. Default is 10. *value* must be an integer from 5 to 30.
- **t392** *value* - Polling verification timer value. Default is 15. *value* must be an integer from 5 to 30.

**Usage**

Use this command to define LMI type and timers and to associate time group 2 with the Frame Relay connection.

**Example**

```
frame-relay path le1 3 timeslot 2
```
hopath-sdsf

Configures the high-order path for degrade/signal failure (SDSF) bit error rate (BER) thresholds.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

hopath-sdsf hopath_value

hopath_value

- 0: Disabled
- 1 - 1.0E-03
- 2 - 1.0E-04
- 3 - 1.0E-05
- 4 - 1.0E-06
- 5 - 1.0E-07
- 6 - 1.0E-08
- 7 - 1.0E-09
- 8 - 1.0E-10

Usage
Sets a standard option for the high-order path for SDSF. The SD is kept at a value of 100 erroredBits/sec less than the corresponding value of the SF. So if the SD threshold is configured at 1 error in every 100000 bits/sec, then the SF threshold automatically becomes 1 error in every 1000 bits/sec.

Example

    hopath-sdsf 1
**line-timing**

This command enables the SPIO to recover transmit timing source via the line attached to the selected port. By default, line-timing is not enabled.

**Important:** To employ line-timing recovery, the SPIO card(s) must be equipped with the optional Stratum 3 clock module.

<table>
<thead>
<tr>
<th>Product</th>
<th>SGSN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privilege</td>
<td>Security Administrator, Administrator</td>
</tr>
</tbody>
</table>

**Syntax**

```
[ no ] line-timing
```

- **no**
  Disables line-timing as the source for the transmit clock.

**Usage**

The port must be enabled (with the `no shutdown` command) to enable recovery of timing source via the line. As well, the card’s slot number must be entered in the `recover line#` command of the BITS port configuration mode.

**Important:** If the SPIO is connected to an external Building Integrated Timing Supply (BITS) source, BITS timing always takes precedence over line-timing.

**Example**

Disable timing clock recovery on this port.

```
no line-timing
```
loopback

Configures the type of loopback mode used for diagnostic testing.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax
loopback { ds1-e1-diag | ds1-e1-line | none | sonet-sdh-diag | sonet-sdh-line }

- **ds1-e1-diag**
  Enables a system generated diagnostic lookback signal at the DS1/E1 layer.

- **ds1-e1-line**
  Loops back a network diagnostic signal at the DS1/E1 layer.

- **none**
  Stops diagnostic loopback signaling.

- **sonet-sdh-diag**
  Enables a system generated diagnostic lookback signal at the SONET/SDH layer.

- **sonet-sdh-line**
  Loops back a network diagnostic signal at the SONET/SDH layer.

Usage
Setup diagnostic loopback signals for troubleshooting purposes.

Example
loopback ds1-e1-diag
lopath-sdsf

Configures the low-order path for signal degrade/signal failure (SDSF) bit error rate (BER) thresholds.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

`lopath-sdsf lopath_value`

`lopath_value`

- 0: Disabled
- 1 - 1.E-03
- 10 - 1.E-12
- 2 - 1.E-04
- 3 - 1.E-05
- 4 - 1.E-06
- 5 - 1.E-07
- 6 - 1.E-08
- 7 - 1.E-09
- 8 - 1.E-10
- 9 - 1.E-11

Usage
Sets a standard option for the low-order path for SDSF.
The SD is kept at a value of 100 erroredBits/sec less than the corresponding value of the SF. So if the SD threshold is configured at 1 error in every 100000 bits/sec, then the SF threshold automatically becomes 1 error in every 1000 bits/sec.

Example

`lopath-sdsf 1`
**path**

This command configures the parameters that define the routing path for a DLCI. It must match with the DLCI configuration parameters. The values entered with these commands should be noted as they will be needed to configure the `frame-relay` and `dlci` commands also in this configuration mode.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Syntax**

```
path path_id { ds1 connects | el connects } service-type { frame-relay | mtp2 } frame-mapping multiplexing index# index# framing mode mapping-mode { bit-sync | byte-sync } [ timeslots slot# [ slot# ] | frame-relay [ intf-type intf_type [ lmi_type lmi_type ] ] ]
```

```
no path path_id { ds1 | el }connects
```

`no` Deletes the routing path entry from the configuration.

```
path path_id
```

Identifies a specific path configuration that will be associated with a DLCI. The `path_id` must be an integer from 1 to 3.

```
ds1 connects | el connects
```

Selects the channelization for the connection.

**DS1**: (AKA: T1) Is associated with North American networks and would be the best choice to work with the SONET (can also work with SDH) framing selected with the `card` configuration command. DS1 splits the path into 28 logical connections.

**connects**: Defines the number of logical connections supported via the DS1. The selection must be an integer from 1 to 28.

**E1**: Is associated with European networks and would be associated with the SDH (can also work with SONET) framing selected with the `card` configuration command. E1 splits the path into 21 logical connections.

**connects**: Defines the number of logical connections supported via the E1. The selection must be an integer from 1 to 21.

```
service-type { frame-relay | mtp2 }
```

Specifies the service type to be used for this path. When `multi-service` is enabled at the card level, different services are supported at the path-level for this port. For additional information, refer to the description of the `service-type` command in the `Card Configuration Mode Commands` chapter.

- **frame-relay**: Specifies Frame Relay mode for this path.
- **mtp2**: Specifies MTP2 service for this path.
frame-mapping

Frame mapping sets the channelization according to the national standards that correlate with the framing/speed standards. This option selects the mapping of containers (C), virtual containers (VC), tributary units (TU), and tributary unit groups (TUG), that is appropriate for the channel characteristics:

- **tu11-au3**: Appropriate for DS1 in SDH. Maps as follows AU-3 — VC-3 — m# — TUG-2 — m# — TU-12 — VC-12 — C-12
- **tu11-au4**: Appropriate for DS1 in SDH. Maps as follows AU-4 — VC-4 — TUG-3 — m# — TUG-2 — m# — TU-11 — VC-11 — C-11
- **tu12-au3**: Appropriate for E1 in SDH. Maps as follows AU-3 — VC-3 — m# — TUG-2 — m# — TU-12 — VC-12 — C-12
- **tu12-au4**: Appropriate for E1 in SDH. Maps as follows AU-4 — VC-4 — TUG-3 — m# — TUG-2 — m# — TU-12 — VC-12 — C-12

Frame Mapping for E1 and DS1 to STM-n Interfaces

- **vt1.5**: Only appropriate for DS1 in SONET framing.
- **vt2**: Only appropriate for E1 in SONET framing.

multiplexing index# index#

index#: TUG-2 index - Must be an integer from 1 to 7 to identify a multiplex channel between TUG-2 and VC-3 (E1) or TUG-3 (DS1).
index#: TU index - Must be an integer from 1 to 4 (DS1) or 1 to 3 (E1) to identify a multiplex channel between TU-11 (DS1) and TUG-2 or between TU-12 (E1) and TUG-2.

framing mode

Defines the framing modes to be used for the channelization to E1 or T1 of the (optical) port.

- **options for E1:**
  - **cas**: standard mapping with CAS
  - **cas-crc4**: CRC4 mapping with CAS
  - **crc4**: CRC4 mapping
  - **standard**: mapping

- **options for DS1:**
  - **esf**: extended superframe mapping
  - **sf**: superframe mapping
• option for either E1 or DS1:
  • unframed

mapping-mode
  • bit-sync
  • byte-sync

timeslots timeslots
Defines up to 8 timeslot groupings for multiple fractional DS1/E1 channels. Each slot is 2.048/32 Mbytes. Slots 0 and 16 are reserved for synchronization and alarms. Slots 1-15 and 17-31 are used for data. Timeslots must be unique -- a timeslot can not be used in more than one grouping.

frame-relay
Enables definition of a Frame Relay connection with the frame-relay command.

Important: For release 8.1 and higher, this feature has been moved to the frame-relay command.

intf-type intf_type
Selecting the interface type specifies signaling parameters for the DLCI, options include:
  • dce: Selects data circuit-terminating equipment -type signaling.
  • dte: Selects data terminal equipment -type signaling.
  • nni: Selects the network-to-network interface

Default: DTE for Release 8.0
Default: DCE for Release 8.1

Important: For release 8.1 and higher, this feature has been moved to the frame-relay command.

lmi_type lmi_type
Default: none.
Line management type options include:
  •ansi - ANSI ANNEXED LMI, may include option:
  •cisco - Cisco/Gang Of Four LMI
  •none - LMI Disabled
  •q933a - Q.933A LMI

Any of the above LMI types can take one or more additional options
  •n391 value - Number of keep exchanges before requesting a full status message. Default is 6. value must be an integer from 1 to 255.
  •n392 value - Error Threshold value. Default is 2. value must be an integer from 1 to 10.
**Path**

- **n393** value - Monitored events count value. Default is 2. *value* must be an integer from 1 to 10.
- **t391** value - Timer to send messages. Default is 10. *value* must be an integer from 5 to 30.
- **t392** value - Polling verification timer value. Default is 15. *value* must be an integer from 5 to 30.

**Important:** For release 8.1 and higher, this feature has been moved to the `frame-relay` command.

**Usage**

Defines the signaling characteristics of a frame relay connection or timeslots for a fractional connection.

Use this command to create E1 ports or fractional E1 ports. Fractional E1 ports are created with the timeslot definitions. The fractional E1 port can consist of one or more or all of the timeslots.

**Example**

In the first example, define timers for the q933a LMI-type.

```plaintext
path 1 e1 1 tu12-au4 1 1 framing crc4 mapping-mode bit-async frame-relay intf-type dce lmi_type q933a n391 6 n392 2 n393 2 t391 10 t392 15
```

The next example defines 3 groups of fractional timeslots with group 1 having slots 1-5 and 8, group 2 having slot 22-25, and group 3 having slots 31.

```plaintext
path 1 e1 1 tu12-au3 1 1 framing cas mapping-mode bit-async timeslots 1-5,8 22-25 31
```
preferred slot

Identifies which card in a chassis should assume revertive (redundancy auto-recovery) functionality should the slot/port being configured go down. This command must be issued on a per port basis, allowing you to configure specific ports to be used on individual LCs or SPIO cards. For example, ports 1 through 4 could be configured as “preferred” on the LC in slot 17 while ports 5 through 8 are “preferred” on the LC in slot 33. In this scenario, both LCs would be in an Active operational state while still providing LC and port redundancy for the other.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax
preferred slot slot#

no preferred slot

slot#

Identifies the physical slot in the chassis where the line card is installed.

no

Disables revertive, or auto-recovery, operation for the port.

Usage
This command enables or disables revertive port redundancy. So after a port failover, when the original port is restored to service (i.e. link up) the system will return service to that port automatically. Disabled, which is the default setting, causes non-revertive operation; requiring an administrative user to manually issue a port switch to command to return service to the original port.

Example
preferred slot 17
pwe3-cesopsn

This command has been deprecated and replaced by the mtp2 command.
shutdown

Terminates all processes supporting the port or blocks the shutting down of the port. Conversely, this command with the no keyword enables the port.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

[ no ] shutdown

no

Enables the port’s administrative state. When omitted the card is shutdown (removed from service).

Usage
Shut down a port prior to re-cabling and/or other maintenance activities. This command with the no keyword is required to bring a port into service.

Example
Use the following command to disable a port:

    shutdown

Use the following command to enable a port for service:

    no shutdown
snmp trap link-status

Enables/disables the generation and sending of an SNMP (notification) trap when the port experiences a change of state (up or down).

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
[ no ] snmp trap link-status
```

- **no**

Disables the sending of traps for link-status changes.

**Usage**

Enable the sending of link-status change traps if there is a monitoring facility that can use the information or if there are troubleshooting activities in progress.

**Example**

```
snmp trap link-status
```
threshold high-activity

Configures the port’s high and low activity thresholds.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

```
threshold high-activity high_thresh [ clear low_thresh ]
```

<table>
<thead>
<tr>
<th>high_thresh</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default: 50</td>
</tr>
<tr>
<td>Sets the threshold for the highest percentage of port activity that must be met or exceeded, within the polling interval, to generate an alert or alarm.</td>
</tr>
<tr>
<td>high_thresh_% can be configured to any integer value between 0 and 100.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>clear low_thresh</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default: 50</td>
</tr>
<tr>
<td>Sets the threshold for the lowest percentage level of port activity that must be met to generate and send a clear alarm. If port activity does not drop to or below this threshold then the alarm is maintained.</td>
</tr>
<tr>
<td>low_thresh_% can be configured to any integer value between 0 and 100.</td>
</tr>
</tbody>
</table>

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

High port activity thresholds generate alerts or alarms based on the utilization percentage of each configured port during the specified polling interval. This threshold is configured on a per-port basis. Alerts or alarms are triggered for high port activity based on the following rules:

- **Enter condition:** Actual percent utilization of a port > High Threshold
- **Clear condition:** Actual percent utilization of a port < Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the threshold poll command in the Global Configuration Mode Commands chapter of this reference to configure the polling interval and the threshold monitoring command in this chapter to enable thresholding for this value.

Example

The following command configures a high port utilization threshold percent of 70 and a low threshold of 50 for an system using the Alarm thresholding model:

```
threshold high-activity 70 clear 50
```
threshold monitoring

Enables thresholding for port-level values.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

[ no ] threshold monitoring

no

Disables threshold monitoring for port-level values. This is the default setting.

Usage

Thresholding on the system is used to monitor the system for conditions that could potentially cause errors or outage. Typically, these conditions are temporary (i.e. high-activity) and are quickly resolved. However, continuous or large numbers of these error conditions within a specific time interval may be indicative of larger, more severe issues. The purpose of thresholding is to help identify potentially severe conditions so that immediate action can be taken to minimize and/or avoid system downtime.

Thresholding reports conditions using one of the following mechanisms:

- **SNMP traps**: SNMP traps have been created that indicate the condition (high threshold crossing and/or clear) of each of the monitored values. Complete descriptions and other information pertaining to these traps is located in the starentMIB(8164).starentTraps(2) section of the SNMP MIB Reference.

- **Logs**: The system provides a facility called threshold for which active and event logs can be generated. As with other system facilities, logs are generated. Log messages pertaining to the condition of a monitored value are generated with a severity level of WARNING.

- **Alarm System**: High threshold alarms generated within the specified polling interval are considered “outstanding” until a the condition no longer exists and/or a condition clear alarm is generated. “Outstanding” alarms are reported to through the system’s alarm subsystem and are viewable through the system’s CLI.

The following table indicates the reporting mechanisms supported by each of the above models.

<table>
<thead>
<tr>
<th>Model</th>
<th>SNMP Traps</th>
<th>Logs</th>
<th>Alarm System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Alarm</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

This command enables thresholding for port-level values. Refer to the `threshold high-activity`, `threshold rx-utilization`, and `threshold tx-utilization` commands in this chapter for information on configuring these values. In addition refer to the `threshold poll` command in the...
Global Configuration Mode Commands chapter of this reference for information on configuring the polling interval over which these values are monitored.

**Example**

Use the following command to terminate thresholding:

```plaintext
no threshold monitoring
```
threshold rx-utilization

Configures thresholds for receive-port utilization.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

```bash
threshold rx-utilization high_thresh [ clear low_thresh ]
```

**high_thresh**

Default: 80
The high threshold receive port utilization percentage that must be met or exceeded within the polling interval to generate an alert or alarm.
The percentage can be configured to any integer value between 0 and 100.

**clear low_thresh**

Default: 80
Allows the configuration of the low threshold.
The low threshold receive port utilization percentage that maintains a previously generated alarm condition.
If the utilization percentage falls below the low threshold within the polling interval, a clear alarm will be generated.
The percentage can be configured to any integer value between 0 and 100.

**Important**: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**

Receive port utilization thresholds generate alerts or alarms based on the utilization percentage of each configured port in relation to data received during the specified polling interval. This threshold is configured on a per-port basis.

**Important**: Ports configured for half-duplex do not differentiate between data received and data transmitted. Therefore, to avoid redundant alarms, it is recommended that only the receive or transmit utilization threshold be configured.

Alerts or alarms are triggered for receive port utilization based on the following rules:

- **Enter condition**: Actual percent utilization of a port for received data ≥ High Threshold
- **Clear condition**: Actual percent utilization of a port for received data < Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the `threshold poll` command in the Global Configuration Mode Commands chapter of this reference to configure the polling interval and the `threshold monitoring` command in this chapter to enable thresholding for this value.

**Example**

The following command configures a receive port high utilization threshold percent of 70 and a low threshold of 50 for a system using the Alarm thresholding model:

```
threshold rx-utilization 70 clear 50
```
threshold tx-utilization

Configures thresholds for transmit port utilization.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

\texttt{threshold \textit{tx-utilization}} high\_thresh \ [ clear \ low\_thresh ]

\texttt{high\_thresh}
Default: 80
The high threshold transmit port utilization percentage that must be met or exceeded within the polling interval to generate an alert or alarm.
The percentage can be configured to any integer value between 0 and 100.

\texttt{clear \ low\_thresh}
Default: 80
Allows the configuration of the low threshold.
The low threshold transmit port utilization percentage that maintains a previously generated alarm condition.
If the utilization percentage falls below the low threshold within the polling interval, a clear alarm will be generated.
The percentage can be configured to any integer value between 0 and 100.

\textbf{Important:} This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Transmit port utilization thresholds generate alerts or alarms based on the utilization percentage of each configured port in relation to data transmitted during the specified polling interval. This threshold is configured on a per-port basis.

\textbf{Important:} Ports configured for half-duplex do not differentiate between data received and data transmitted. Therefore, to avoid redundant alarms, it is recommended that only the receive or transmit utilization threshold be configured.

Alerts or alarms are triggered for transmit port utilization based on the following rules:

- **Enter condition:** Actual percent utilization of a port for transmit data \( \geq \) High Threshold
- **Clear condition:** Actual percent utilization of a port for transmit data \(< \) Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the `threshold poll` command in the Global Configuration Mode Commands chapter of this reference to configure the polling interval and the `threshold monitoring` command in this chapter to enable thresholding for this value.

**Example**

The following command configures a transmit port high utilization threshold percent of 70 and a low threshold of 50 for an system using the Alarm thresholding model:

```
threshold tx-utilization 70 clear 50
```
**toh-sdsf**

Enable/disable line SDSF BER thresholds and configure the line transport overhead (TOH) signal degrade and signal failure (SDSF) bit error rate (BER) threshold.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

toh-sdsf toh_value

default toh-sdsf

default

Resets the default which disables this threshold.

toh_value

To facilitate configuration the SD and SF rates have been combined into a single setting. .
- 0: Disabled
- 1 - 1E-04
- 2 - 1E-05
- 3 - 1E-06
- 4 - 1E-07
- 5 - 1E-08
- 6 - 1E-09
- 7 - 1E-10
- 8 - 1E-11

**Usage**
This command can be used to configure the line threshold whether the port is active or standby and sets a standard option for the paired values of the line’s signal degrade and signal failure (SDSF) BER. The SD is kept at a value of 100 erroredBits/sec less than the corresponding value of the SF. So if the SD threshold is configured at 1 error in every 100000 bits/sec, then the SF threshold automatically becomes 1 error in every 1000 bits/sec. The port will go operationally down as soon as the SD threshold is crossed.

**Example**

toh-sdsf 1
vc-mapping

This command has been deprecated. Go to the frame-mapping keyword in the path command to configure this functionality.
Chapter 44
Cipher Suite Configuration Mode Commands

The Cipher Suite Configuration Mode is used to configure the building blocks for SSL cipher suites, including the encryption algorithm, hash function, and key exchange.

**Mode**

Exec > Global Configuration > Context Configuration > Cipher Suite Configuration

`configure > context context_name > cipher-suite cipher_suite_name`

Entering the above command sequence results in the following prompt:

`[context_name]host_name(cfg-ctx-cipher-suite)#`

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
encryption

Specifies the encryption algorithm for the SSL cipher suite.

Product
SCM (P-CSCF, A-BG)

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > Cipher Suite Configuration
configure > context context_name > cipher-suite cipher_suite_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(cfg-ctx-cipher-suite)#

Syntax

encryption { 3des | aes-128 | null | rc4 }

default encryption

default

Sets the encryption option to its default value of RC4.

encryption 3des | aes-128 | null | rc4

Specifies the encryption algorithm.
3des: Encryption algorithm 3DES (Triple Encryption Algorithm). 3DES applies the Data Encryption Standard (DES) cipher algorithm three times to each data block.
aes-128: Encryption algorithm AES-128 (Advanced Encryption Standard-128). AES-128 is a symmetric-key encryption standard which has a 128-bit block size, with key size of 128.
null: Encryption algorithm Null.
rc4: Encryption algorithm RC4 (Rivest Cipher 4). RC4 is a stream cipher used with SSL protocol.

Usage

Use this command to specify encryption for the SSL cipher suite.

Example

The following command sets the encryption option to its default value, which is RC4:

cipher rc4
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
   end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Use this command to return to the parent configuration mode.
**hmac**

Specifies the HMAC (keyed-Hash Message Authentication Code) for the SSL cipher suite.

**Product**
SCM (P-CSCF, A-BG)

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Cipher Suite Configuration

**Syntax**

```
hmac { sha1 }  
default hmac 
```

**default hmac**

Sets the HMAC option to its default value of SHA-1.

**hmac sha1**

Specifies the SHA-1 (Secure Hash Algorithm-1) HMAC for the SSL cipher suite. SHA-1 uses a 160-bit secret key and produces a 160-bit digest.

**Usage**
Use this command to specify the SHA-1 HMAC for the SSL cipher suite. The default and only currently available option is SHA-1.

A keyed-Hash Message Authentication Code, or HMAC, is a type of message authentication code (MAC) calculated using a cryptographic hash function in combination with a secret key to verify both data integrity and message authenticity.

**Example**

The following command sets the HMAC option to its default value, which is SHA-1:

```
hmac sha1
```
key-exchange

Specifications the key exchange algorithm for the SSL cipher suite.

Product
SCM (P-CSCF, A-BG)

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > Cipher Suite Configuration

configure > context context_name > cipher-suite cipher_suite_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(cfg-ctx-cipher-suite)#

Syntax

key-exchange { rsa }

default key-exchange

default
Sets the key exchange option to its default value of RSA.

key-exchange rsa

Specifies the RSA (Rivest, Shamir, and Adleman) key exchange algorithm for the SSL cipher suite. With RSA, the secret key is encrypted with the receiver's public key, and a public-key certificate from the receiver's key must be made available.

Usage
Use this command to specify the RSA key exchange for the SSL cipher suite. The default and only currently available option is RSA.

The key exchange algorithm provides the means by which the cryptographic keys for conventional encryption and MAC calculations are exchanged.

Example
The following command sets the key exchange option to its default value, which is RSA:

    key-exchange rsa
Chapter 45
Class-Map Configuration Mode Commands

Class-Map is used to configure a packet classifier for the flow-based Traffic Policing feature within destination context. It filters egress and/or ingress packets of a subscriber session based on rules configured in a subscriber context.

```
Mode
Exec > Global Configuration > Context Configuration > Class-Map Configuration
configure > context context_name > class-map class_map_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-class-map)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
end

**Usage**
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
exit
```

**Usage**

Use this command to return to the parent configuration mode.
### match any

Allows all traffic types in this class map.

**Product**
- PDSN
- HA
- ASN-GW
- HSGW
- P-GW
- SAEGW
- SCM

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Class-Map Configuration

```bash
configure > context context_name > class-map class_map_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-class-map)#
```

**Syntax**

```
match any
```

**Usage**
Sets the match rule to allow all traffic flow for specific class map.

**Example**

The following command allows all packets going to a system with this class map.

```
match any
```
**match dst-ip-address**

Specifies a traffic classification rule based on the destination IP address of packets.

**Product**

- PDSN
- HA
- ASN-GW
- HSGW
- P-GW
- SAEGW
- SCM

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > Class-Map Configuration

```
configure > context context_name > class-map class_map_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-class-map)#
```

**Syntax**

```
match dst-ip-address dst_ip_address /subnet_mask
```

**Usage**

Sets the match rule based on the destination IP address of packets for specific Class Map.

**Example**

The following command specifies the rule for packets going to a system having an IP address 10.1.2.6.

```
match dst-ip-address 10.1.2.6
```
**match dst-port-range**

Specifies a traffic classification rule based on the range of destination ports for L4 packets.

**Product**
- PDSN
- HA
- ASN-GW
- HSGW
- P-GW
- SAEGW
- SCM

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Class-Map Configuration

`configure > context context_name > class-map class_map_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-class-map)#
```

**Syntax**

```
match dst-port-range initial_port_number [ to last_port_number ]
```

```
initial_port_number [ to last_port_number ]
```

Specifies the destination port or range of ports of L4 packets.

- `initial_port_number` is the starting port number and must be an integer 1 to 65535 but less than `last_port_number`, if specified.
- `last_port_number` is the end port number and must be an integer from 1 to 65535 but more than `initial_port_number`.

**Usage**
Sets the match rule based on the destination port number or range of ports of L4 packets for specific Class Map.

**Example**
The following command specifies the rule for packets having destination port number from 23 to 88.

```
match dst-port-range 23 to 88
```
match ip-tos

Specifies a traffic classification rule based on the IP Type of Service value in ToS field of packet.

Product
PDSN
HA
ASN-GW
HSGW
P-GW
SAEGW
SCM

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > Class-Map Configuration

class > context context_name > class-map class_map_name

The above command sequence results in the following prompt:

[context_name]host_name(config-class-map)#

Syntax

match ip-tos { service_value [ ip-tos-mask mask_value ] | tos-range low_value to high_value }

<table>
<thead>
<tr>
<th>service_value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the IP Type-of-Service value to match inside the ToS field of packets as an integer from 0 to 255.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ip-tos-mask mask_value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the IP Type-of-Service mask value to match inside the ToS field of packets as an integer from 1 to 255.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>tos-range low_value to high_value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies a range that a ToS value in a received packet must fall within to be considered a match. low_value and high_value must be an integer from 0 to 255.</td>
</tr>
</tbody>
</table>

Usage
Sets the match rule based on the IP ToS value in ToS field of packets for specific Class Map.

Example
The following commands specifies the IP ToS value of 3 is the value to match in a ToS field in received packets.

match ip-tos 3
match ipsec-spi

Specifies a traffic classification rule based on the IPSec Security Parameter Index (SPI) value in the SPI field of packet.

Product
- PDSN
- HA
- ASN-GW
- HSGW
- P-GW
- SAEGW
- SCM

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Class-Map Configuration

configure > context context_name > class-map class_map_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-class-map)#

Syntax

```plaintext
match ipsec-spi index_value
```

index_value

Specifies the IPSec SPI value to match inside the SPI field of packets as an integer from 1 to 65535.

Usage
Sets the match rule based on the IPSec SPI value in SPI field of packets for specific Class Map.

Example

The following command specifies the IPSec SPI value as 1234 for the SPI field in packets.

```plaintext
match ipsec-spi 1234
```
**match packet-size**

Specifies a traffic classification rule based on the size of packet.

**Product**
PDSN
HA
ASN-GW
HSGW
P-GW
SAEGW
SCM

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Class-Map Configuration

```
configure > context context_name > class-map class_map_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-class-map)#
```

**Syntax**

```
match packet-size [ gt | lt ] size
```

- `[ gt | lt ] size`
  - Specifies the packet length in bytes.
  - `gt`: indicates a packet size greater than the specified size.
  - `lt`: indicates a packet size less than the specified size.
  - `size` must be an integer from 1 to 65535.

**Usage**

Sets the match rule based on the size of packets for specific Class Map. This command is only applicable for static policies; it is not available for dynamic policies.

**Example**

The following command specifies the packet length to be **1024** bytes.

```
match packet-size 1024
```
match protocol

Specifies a traffic classification rule based on the protocol used for session flow.

**Product**
- PDSN
- HA
- ASN-GW
- HSGW
- P-GW
- SAEGW
- SCM

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration > Context Configuration > Class-Map Configuration
- `configure > context context_name > class-map class_map_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-class-map)#
```

**Syntax**

```
match protocol { gre | ip-in-ip | number | rtp | sip | tcp | udp }
```

---

**gre**

Sets the match rule for session flow using Generic Routing Encapsulation (GRE) Protocol. It matches the protocol field to GRE inside the packet.

**ip-in-ip**

Sets the match rule for session flow using IP-in-IP encapsulation protocol. It matches the protocol field to ip-in-ip inside the packet.

**number**

Sets the match rule for a session flow using Transmission Control Protocol (TCP). It matches the specified protocol field inside the packet.

**rtp**

Sets the match rule for a session flow using Real Time Protocol (RTP). It matches the specified protocol field inside the packet.

**sip**

Sets the match rule for a session flow using Session Initiation Protocol (SIP). It matches the specified protocol field inside the packet.
**tcp**
Sets the match rule for a session flow using Transmission Control Protocol (TCP). It matches the protocol field to TCP inside the packet.

**udp**
Sets the match rule for a session flow having User Datagram Protocol (UDP). It matches the protocol field to UDP inside the packet.

**Usage**
Sets the match rule based on the protocol of packet flow for a specific Class Map.

**Example**
The following command specifies the rule for packet flow using IP-in-IP protocol.

```
match protocol ip-in-ip
```
match src-ip-address

Specifies a traffic classification rule based on the source IP address of packets.

Product

PDSN
HA
ASN-GW
HSGW
P-GW
SAEGW
SCM

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > Context Configuration > Class-Map Configuration
configure > context context_name > class-map class_map_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-class-map)#

Syntax

match src-ip-address src_ip_address/subnet_mask

src_ip_address/subnet_mask

Specifies the destination IP address of the packets.
src_ip_address must be entered in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.
subnet_mask is an option that is entered in CIDR notation.

Usage

Sets the match rule based on the source IP address of packets for specific Class Map.

Example

The following command specifies the rule for packets coming from a system having an IP address 10.1.2.3.

    match src-ip-address 10.1.2.3
match src-port-range

Specifies a traffic classification rule based on the range of source ports of L4 packets.

**Product**
PDSN
HA
ASN-GW
HSGW
P-GW
SAEGW
SCM

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Class-Map Configuration

```plaintext
configure > context context_name > class-map class_map_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-class-map)#
```

**Syntax**

```plaintext
match src-port-range initial_port_number [ to last_port_number ]
```

Specifies the source port or range of ports of the L4 packets.

*initial_port_number* is the starting port number and must be an integer from 1 to 65535 but less than *last_port_number*, if specified.

*last_port_number* is the end port number and must be an integer from 1 to 65535 but more than *initial_port_number*.

**Usage**

Sets the match rule based on source port number or range of ports of L4 packets for specific Class Map.

**Example**

The following command specifies the rule for packets having source port number from 23 to 88.

```plaintext
match src-port-range 23 to 88
```
Chapter 46
CGW Service Configuration Mode Commands

Creates Convergence Gateway (CGW) service and enters CGW service configuration mode.

**Mode**

Exec > Global Configuration > Context Configuration > CGW Configuration

```
configure > context context_name > cgw-service cgw_service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cgw-service)#
```

ℹ️ **Important**: Available commands or keywords/variables vary based on platform type, product version, and installed license(s).
**associate**

This command associates another service to this CGW service.

**Product**
SaMOG

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CGW Configuration

```
configure > context context_name > cgw-service cgw_service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cgw-service)#
```

**Syntax**

```
associate { egress-egtp-service egress_egtp_service | mrme-service mrme_service | qci-qos-mapping qci_qos_mapping | subscriber-map subscriber_map }

no associate { egress-egtp-service | ingress-lma-service | qci-qos-mapping | subscriber-map }
```

**no**

Disables association to CGW service.

**egress-egtp-service egress_egtp_service**

Configures the egtp-service which provides S2A functionality to the CGW service.

*egress-egtp-service* is a string and the value must be between 1 and 63.

**mrme-service mrme_service**

Configures the association of egress MRME service for this CGW service.

*mrme_service* is a string and the value must be between 1 and 63.

**qci-qos-mapping qci_qos_mapping**

Configuration related QCI to QoS mapping.

*qci-qos-mapping* is a string and the value must be between 1 and 63.

**subscriber-map subscriber_map**

Configures subscriber map association.

*subscriber_map* is a string and the value must be between 1 and 64.

**ingress-lma-service**

Configuration of the ingress LMA for this CGW service.
**Usage**

Use this command to associate another service to this CGW service.

**Example**

The following command is used to associate the configuration of egress EGTP service `egts` for this CGW service:

```
associate egress-egtp-service egts
```
**bind**

This command binds ip-address for LMA driver.

**Product**
SaMOG

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CGW Configuration

configure > context context_name > cgw-service cgw_service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-cgw-service)#

**Syntax**

```
bind { ipv4-address ipv4_address  [ ipv6-address ipv6_address ] | ipv6-address ipv6_address  }
```

```
no bind { ipv4-address ipv4_address  [ ipv6-address ipv6_address ] | ipv6-address ipv6_address  }
```

**no**

Disables binding.

```
bind ipv4-address ipv4_address
```

Designates the address of the LMA service. This must be followed by IPv4 address.

`ipv4_address` is IPv4 address, using dotted-decimal notation.

```
bind ipv6-address ipv6_address
```

Designates an IPv6 address. This must be followed by IPv6 address.

`ipv6_address` is IPv4 address, using dotted-decimal notation.

**Usage**

Use this command to bind ip-address for LMA driver.

**Example**

The following command binds an IPv4 address for LMA driver.

```
bind ipv4-address 1.2.3.4
```
enable-bra-failure-handling

This command enables the HAMGR to select the first session incase the Binding Revocation Ack (BRA) does not have required parameters and the session lookup fails.

**Product**
SaMOG

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CGW Configuration

```
configure > context context_name > cgw-service cgw_service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cgw-service)#
```

**Syntax**

```
enable-bra-failure-handling

no enable-bra-failure-handling
```

Disables Binding Revocation Ack failure handling.

**Usage**

Use this command to enable Binding Revocation Ack failure handling.

**Example**

The following command enables Binding Revocation Ack failure handling.

```
enable-bra-failure-handling
```
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
```
end
```

**Usage**
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Use this command to return to the parent configuration mode.
**reg-lifetime**

Configures Mobile IPV6 session registration lifetime in seconds.

**Product**
SaMOG

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CGW Configuration

```
configure > context context_name > cgw-service cgw_service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cgw-service)#
```

**Syntax**

```
reg-lifetime seconds
```

**default reg-lifetime**

- **default** Configures Mobile IPV6 session registration lifetime, in seconds to its default value, **600**.

```
reg-lifetime seconds
```

- **Usage**

  Configures Mobile IPV6 session registration lifetime.

  *seconds* is the number of seconds, an integer value between 1 and **262140**.

- **Example**

  Use this command to configure Mobile IPV6 session registration lifetime, in seconds.

  The following command configures Mobile IPV6 session registration lifetime to 500 seconds.

  ```
  reg-lifetime 500
  ```
revocation

Configures Binding Revocation support for specific CGW service.

**Product**
SaMOG

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CGW Configuration

```bash
configure > context context_name > cgw-service cgw_service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cgw-service)#
```

**Syntax**

```bash
revocation { enable | max-retransmission max_retransmission | retransmission-timeout msecs }
```

**Default revocation**

```bash
default revocation { enable | max-retransmission | retransmission-timeout }
```

**no revocation enable**

```bash
default reg-lifetime
```

**Default**

Resets the revocation to its default value.

**no**

Disables revocation.

```bash
revocation { enable | max-retransmission max_retransmission | retransmission-timeout msecs }
```

**enable**: Enables the Binding Revocation Support. Default is disabled.

**max-retransmission**

```bash
max_retransmission
```

**retransmission-timeout**

```bash
msecs
```

**Usage**

Use this command to configure Binding Revocation support for specific CGW service.

**Example**

The following command configures the retransmission timeout to 1000 milli seconds.

```bash
revocation retransmission-timeout 1000
```
session-delete-delay

Configures CGW to retain the session on receiving a termination request till configured delay time for session continuity in case of break-before-make scenario.

Product
SaMOG

Privilege
Security Administrator, Administrator

Syntax

```bash
session-delete-delay timeout delay_msecs
default session-delete-delay timeout
no session-delete-delay timeout
```

- **default**
  Configures session delete delay to its default value, disabled. Default timeout when enabled is 10000 msecs.

- **no**
  Enables / disables session delete delay to its default value.

- **session-delete-delay timeout delay_msecs**
  `timeout`: Configuration to retain session till configured time in msecs when enabled.
  `delay_msecs` is the number of milli seconds, an integer value between 1000 and 60000.

Usage
Use this command to configure CGW to retain the session on receiving a termination request till configured delay time for session continuity in case of break-before-make scenario.

Example
The following command configures CGW to retain the session timeout to 1500 milli seconds.

```bash
session-delete-delay timeout 1500
```
timestamp-option-validation

Confugures validation of Timestamp Option in Binding Update messages. By default Timestamp option is mandatory.

Product
SaMOG

Privilege
Security Administrator, Administrator

Syntax

    timestamp-option-validation
    no  timestamp-option-validation
    default  timestamp-option-validation

    no
    Disables the Timestamp Option in Binding Update messages.

    default
    Confugures validation of Timestamp Option in Binding Update messages to its default value.

Usage
Use this command to confugure validation of Timestamp Option in Binding Update messages.

Example
The following command confugures validation of Timestamp Option in Binding Update messages.

    timestamp-option-validation
**timestamp-replay-protection**

This command designates timestamp replay protection scheme as per RFC 4285.

**Product**
SaMOG

**Privilege**
Security Administrator, Administrator

**Syntax**

```
timestamp-replay-protection  tolerance  seconds
no  timestamp-replay-protection
default  timestamp-replay-protection  tolerance
```

*no*  
Disables the timestamp replay protection scheme.

*default*  
Designates default value to timestamp replay protection scheme. The default value of the acceptable difference in timing (between timestamps) before rejecting packet is 7 seconds.

**Usage**

Use this command to designate timestamp replay protection scheme as per RFC 4285.

**Example**

The following command designates timestamp replay protection for 500 seconds.

```
timestamp-replay-protection  tolerance  500
```
Chapter 47
Congestion Action Profile Configuration Mode Commands

The Congestion Policy Configuration Mode is used to create and manage the action profiles to be associated with congestion control policies supporting MME configurations on the system.

Mode

Exec > Global Configuration > LTE Policy Configuration > Congestion Action Profile Configuration
configure > lte-policy > congestion-action-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(congestion-action-profile)#

⚠️ Important: Available commands or keywords/variables vary based on platform type, product version, and installed license(s).
drop

Specifies that incoming packets containing new session requests be dropped when a congestion control threshold has been reached.

Product
MME

Privilege
Administrator

Mode
Exec > Global Configuration > LTE Policy Configuration > Congestion Action Profile Configuration

configure > lte-policy > congestion-action-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(congestion-action-profile)#

Syntax

drop { addn-brr-requests | addn-pdn-connects | combined-attaches | handovers | ps-attaches | sl-setups | service-request | tau-request }

- **addn-brr-requests**
  Drops packets containing UE initiated bearer resource requests.
  This keyword option will be available only if a valid license is installed.

- **addn-pdn-connects**
  Drops packets containing additional PDN context connections.
  This keyword option will be available only if a valid license is installed.

- **combined-attaches**
  Drops packets containing combined Attach requests.

- **handovers**
  Drops packets containing handover attempts.

- **ps-attaches**
  Drops packets containing packet switched Attach requests.

- **sl-setups**
  Drops packets containing S1 setup attempts.
  This keyword option will be available only if a valid license is installed.

- **service-request**
  Drops packets containing all service requests.
  This keyword option will be available only if a valid license is installed.
**Usage**

Creates a congestion action profile that drops packets containing a specified request when a threshold is reached.

Some keyword options are available only if a valid license is installed. For more information, contact your Cisco account representative.

**Example**

The following command drops packets containing Tracking Area Update (TAU) requests when a congestion threshold has been reached:

```
drop tau-request
```
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

end

Usage
Use this command to return to the Exec mode.
**exclude-emergency-events**

Excludes emergency events when a congestion control threshold is reached. Emergency events continue to be processed when the threshold has been exceeded.

**Product**
ePDG  
MME

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > LTE Policy Configuration > Congestion Action Profile Configuration  
configure > lte-policy > congestion-action-profile profile_name

Entering the above command sequence results in the following prompt:

```
[local]host_name(congestion-action-profile)#
```

**Syntax**

```
[no] exclude-emergency-events
```

- **no**  
  Removes the specified option from the system.

**Usage**

Create a congestion action profile that allows emergency events to be processed when a congestion threshold has been reached.  
When exclude-emergency is configured, congestion actions will not be applied for the following messages for emergency attached UEs:

- tau-request  
- service-request  
- handovers

When exclude-emergency is configured and addn-pdn-requests are configured for reject or drop actions, the reject or drop action on addn-pdn-requests for emergency PDN will not be applied.

**Example**

The following command allows emergency events to be processed:

```
exclude-emergency-events
```
**exclude-voice-events**

Excludes voice calls when a congestion control threshold is reached. Voice calls continue to be processed when the threshold has been exceeded.

**Product**
MME

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > LTE Policy Configuration > Congestion Action Profile Configuration

`configure > lte-policy > congestion-action-profile profile_name`

Entering the above command sequence results in the following prompt:

```
[local] host_name(congestion-action-profile)#
```

**Syntax**

```
[no] exclude-voice-events
```

no

Removes the specified option from the system.

**Usage**

Create a congestion action profile that allows voice calls to be processed when a congestion threshold has been reached.

**Example**

The following command allows voice calls to be processed:

```
exclude-voice-events
```
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Use this command to return to the parent configuration mode.
**none**

Specifies that no congestion control action be taken on an incoming request when a congestion control threshold has been reached.

**Product**

MME

**Privilege**

Administrator

**Mode**

Exec > Global Configuration > LTE Policy Configuration > Congestion Action Profile Configuration

```
configure > lte-policy > congestion-action-profile profile_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(congestion-action-profile)#
```

**Syntax**

```
none { addn-brr-requests | addn-pdn-connects | combined-attaches | handovers | ps-attaches | sl-setups | service-request | tau-request }
```

---

**addn-brr-requests**

No congestion control action is taken for additional bearer requests when a congestion threshold is reached.

---

**addn-pdn-connects**

No congestion control action is taken for additional PDN context connections when a congestion threshold is reached.

---

**combined-attaches**

No congestion control action is taken for combined Attach requests when a congestion threshold is reached.

---

**handovers**

No congestion control action is taken for handover attempts when a congestion threshold is reached.

---

**ps-attaches**

No congestion control action is taken for packet switched Attach requests when a congestion threshold is reached.

---

**sl-setups**

No congestion control action is taken for S1 setup attempts when a congestion threshold is reached.

---

**service-request**

No congestion control action is taken for service requests when a congestion threshold is reached.
tau-request

No congestion control action is taken for Tracking Area Update requests when a congestion threshold is reached.

Usage

Specifies that no congestion control action be taken for the specified request when a threshold is reached. For all of the above requests, ‘none’ is the default action; requests are processed normally even when a congestion threshold has been reached.

Example

The following command configures the congestion action profile to take no Congestion Control action for Tracking Area Update (TAU) requests when a congestion threshold is reached, so TAU procedure proceeds normally:

```
none tau-request
```
reject

Processes a specified request when a congestion control threshold has been reached and responds with a reject message.

Product
MME

Privilege
Administrator

Mode
Exec > Global Configuration > LTE Policy Configuration > Congestion Action Profile Configuration

configure > lte-policy > congestion-action-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(congestion-action-profile)#

Syntax

reject { addn-brr-requests | addn-pdn-connects | combined-attaches | handovers | ps-attaches | sl-setups time-to-wait { 1 | 10 | 2 | 20 | 50 | 60 } | service-request | tau-request }

- **addn-brr-requests**
  Rejects UE initiated bearer resource requests.
  This keyword option will be available only if a valid license is installed.

- **addn-pdn-connects**
  Rejects additional PDN context connections.
  This keyword option will be available only if a valid license is installed.

- **combined-attaches**
  Rejects combined Attach requests.

- **handovers**
  Rejects handover attempts.

- **ps-attaches**
  Rejects packet switched Attach requests.

- **sl-setups time-to-wait { 1 | 10 | 2 | 20 | 50 | 60 }**
  Rejects S1 setup attempts with an eNodeB after 1, 2, 10, 20, 50 or 60 seconds.
  This keyword option will be available only if a valid license is installed.

- **service-request**
  Rejects all service requests.
  This keyword option will be available only if a valid license is installed.


tau-request

Rejects all Tracking Area Update requests.

---

**Usage**

Creates a congestion action profile that rejects a specified request when a congestion threshold is reached. Some keyword options are available only if a valid license is installed. For more information, contact your Cisco account representative.

**Example**

The following command rejects Tracking Area Update (TAU) requests when a congestion threshold has been reached:

```
reject tau-request
```
report-overload

Enables the MME to report overload conditions to eNodeBs to alleviate congestion scenarios.

**Product**
MME

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > LTE Policy Configuration > Congestion Action Profile Configuration

configure > lte-policy > congestion-action-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(congestion-action-profile)#

**Syntax**

```
report-overload { permit-emergency-sessions-and-mobile-terminated-services | permit-high-priority-sessions-and-mobile-terminated-services | reject-delay-tolerant-access | reject-new-sessions | reject-non-emergency-sessions } enodeb-percentage percent

[no] report-overload
```

### No

Removes the ‘report-overload’ action from this congestion action profile.

### permit-emergency-sessions-and-mobile-terminated-services

Specifies in the overload message to the eNodeB that only emergency sessions are allowed to access the MME during the overload period.

### permit-high-priority-sessions-and-mobile-terminated-services

Specifies in the overload message to the eNodeB that only high-priority sessions and mobile-terminated services are allowed to access the MME during the overload period.

### reject-delay-tolerant-access

Specifies in the overload message to the eNodeB that delay-tolerant access destined for the MME will be rejected during the overload period.

### reject-new-sessions

Specifies in the overload message to the eNodeB that all new connection requests destined for the MME will be rejected during the overload period.

### reject-non-emergency-sessions

Specifies in the overload message to the eNodeB that all non-emergency sessions will be rejected during the overload period.
**enobeb-percentage percentage**

Configures the percentage of known eNodeBs that will receive the overload report. **percentage** must be an integer from 1 through 100.

**Usage**

Configures the MME to invoke the S1 overload procedure (using the S1AP OVERLOAD START message) to report overload conditions to the specified proportion of eNodeBs to which this MME has an S1 interface connection. The MME selects the eNodeBs at random, such that two overloaded MMEs in the same pool do not send overload messages to the same eNodeBs. When the MME has recovered and can increase its load, the it sends an OVERLOAD STOP message to the eNodeBs.

**Important:** The ‘report-overload’ option must be configured before the threshold is exceeded in order for the action to take place.

**Example**

The following command configures the MME to report an overload condition to 50% of all known eNodeBs and to request the eNodeBs to reject all non-emergency sessions to this MME until the overload condition is cleared:

```
report-overload reject-non-emergency-sessions enodeb-percentage 50
```
Chapter 48
Connected Apps Configuration Mode Commands

The Connected Apps (CA) Configuration Mode is used to define CA client session parameters and High Availability (HA) settings for ASR 9000 VSMs supporting wsg-service virtual machines (VMs)

**Important:** The StarOS commands described in this chapter are only supported for VPC running within a VM on the ASR 9000 VSM.

**Mode**

Exec > Global Configuration > Connected Apps Configuration

```
configure > connectedapps
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-connectedapps)#
```
activate

Initiates a ConnectedApps (CA) client session with the IOS-XR server on the ASR 9000.

Product
SecGW (WSG)

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Connected Apps Configuration

configure > connectedapps

Entering the above command sequence results in the following prompt:

[context_name] host_name(config-connectedapps) #

Syntax
activate

no activate

Usage
Use this command to establish or disconnect a ConnectedApps (CA) client session with the IOS-XR server on the ASR 9000. CA client session parameters must have been previously entered for this command to work.

Example
The following command establishes a CA client session:

activate
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Use this command to return to the parent configuration mode.
ha-chassis-mode

Sets the High Availability (HA) mode for wsg-service virtual machines on VSMs in an ASR 9000.

Product
SecGW (WSG)

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Connected Apps Configuration

configure > connectedapps

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-connectedapps)#

Syntax

ha-chassis-mode { inter | intra | standalone }

no ha-chassis-mode

no

Disables the current HA chassis mode

{ inter | intra | standalone }

Specifies the type of chassis mode as:

• inter – HA is established between VSMs in two ASR 9000 chassis.
• intra – HA is established between VSMs in a single ASR 9000 chassis.
• standalone – This is a standalone card; HA cannot be enabled.

Usage

Use this command to set or disable HA for VSMs within or across ASR 9000 chassis. To complete HA configuration you must also set its network mode.

Example

The following command sets HA mode between two ASR 9000 chassis:

ha-chassis-mode inter
ha-network-mode

Sets the network mode for High Availability (HA) network configuration between VSMs in ASR 9000 chassis.

Product
SecGW (WSG)

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Connected Apps Configuration

    configure > connectedapps

Entering the above command sequence results in the following prompt:

    [context_name]host_name(config-connectedapps)#

Syntax

ha-network mode { L2 | L3 | NA }

no ha-network mode

no

Deletes the current setting for HA network mode.

{ L2 | L3 | NA }

Specifies the desired HA network mode as:

• L2 – Layer 2
• L3 – Layer 3
• NA – Not Applicable (standalone VSM)

Usage

Use this command to set the network mode for the HA network configuration between VSMs in ASR 9000 chassis.

Example

The following command sets the HA network mode to Layer 2:

    ha-network-mode L2
**sess-ip-address**

Sets the IP address for a Connected Apps (CA) session.

**Product**
SecGW (WSG)

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Connected Apps Configuration

```
configure > connectedapps
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-connectedapps)#
```

**Syntax**

```
sess-ip-address  ip_address
```

```
o sess-ip-address
```

```
no
```

Deletes the current CA session IP address.

```
no  ip_address
```

Specifies the IP address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

**Usage**

Use this command to set the IP address for a Connected Apps (CA) session.

**Example**

The following command sets an IPv4 address for a CA session.

```
sess-ip-address 10.10.1.1
```
**sess-name**

Sets the name for a CA session.

**Product**
SecGW (WSG)

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Connected Apps Configuration

```
configure > connectedapps
```

Entering the above command sequence results in the following prompt:

```
[context_name] host_name(config-connectedapps)#
```

**Syntax**

```
sess-name session_name

no sess-name
```

- **no**
  - Deletes the current CA session name.

  ```
  no
  ```

- **session_name**
  - Specifies the CA session name as an alphanumeric string of 1 through 125 characters.

  ```
  session_name
  ```

**Usage**

Use this command to set the name for a CA client session.

**Example**

The following command sets the CA session name to *vsm0-1*:

```
sess-name vsm0-1
```
**sess-passwd**

Sets a password for a CA session.

**Product**
SecGW (WSG)

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Connected Apps Configuration

```
configure > connectedapps
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-connectedapps)#
```

**Syntax**

```
(sess-passwd { encrypted | password } password)
```

**no sess-passwd**

```
no
```

Deletes the current CA session password.

**encrypted**

This keyword is only used by StarOS when you save the configuration file. StarOS displays the encrypted keyword in the configuration file as a flag indicating that the variable following the keyword is the encrypted version of the plain text password. Only the encrypted password is saved as part of the configuration file.

**password**

Specifies that the password will appear in plain text in the configuration file.

```
password
```

Specifies the password as an alphanumeric string of 1 through 63 characters that is case sensitive.

**Usage**

Use this password to set a password for a CA session.

**Example**

The following command sets a plain text password for a CA session:

```
sess-passwd password admin012
```
**sess-userid**

Defines a user identifier (username) for the CA session.

**Product**
SecGW (WSG)

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Connected Apps Configuration

```
configure > connectedapps
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-contractedapps)#
```

**Syntax**

```
(sess-userid  username

no sess-userid
```

- **no**
  - Deletes the current user identifier for the CA session.

- **username**
  - Specifies the user identifier for the CA session as an alphanumeric string of 1 through 64 characters.

**Usage**

Use this command to define a user identifier (username) for the CA session.

**Example**

The following command sets the user identifier to `vsm-admin02`:

```
sess-userid vsm-admin02
```
Chapter 49
Content Filtering Policy Configuration Mode Commands

The Content Filtering Policy Configuration Mode allows you to configure analysis and action when Content Filtering (CF) matches a Content Filtering Category Policy Identifier.

**Mode**

Exec > ACS Configuration > CFP Configuration

`active-charging service service_name > content-filtering category policy-id cf_policy_id`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-content-filtering-policy)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
analyze

Specifies the action to take for the indicated result after content filtering analysis.

**Product**
CF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > CFP Configuration

```
active-charging service service_name > content-filtering category policy-id cf_policy_id
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-content-filtering-policy)#
```

**Syntax**

In 12.2 and later releases:

```
analyze priority priority { all | category category | x-category string } action { allow | content-insert content_string | discard | redirect-url url | terminate-flow | www-reply-code-and-terminate-flow reply_code } [ reporting-edr reporting_edr_format_name ]
```

```
no analyze priority priority
```

In 12.1 and earlier releases:

```
analyze priority priority { all | category category | x-category string } action { allow | content-insert content_string | discard | redirect-url url | terminate-flow | www-reply-code-and-terminate-flow reply_code } [ edr edr_format_name ]
```

```
no analyze priority priority
```

**no**
Removes the specified analyze priority configuration.

**priority priority**

Specifies the precedence of a category in the content filtering policy.

**priority** must be an integer from 1 to 65535 that is unique in the content filtering policy.

**all**

Specifies the default action to take if the category returned after rating is not configured in the subscriber’s content filtering policy. This has the lowest priority.

**category category**

Specifies the category.

**category** must be one of the following:

- ABOR
- ADULT
• ADVERT
• ANON
• ART
• AUTO
• BACKUP
• BLACK
• BLOG
• BUSI
• CAR
• CDN
• CHAT
• CMC
• CRIME
• CULT
• DRUG
• DYNAM
• EDU
• ENERGY
• ENT
• FIN
• FORUM
• GAMB
• GAME
• GLAM
• GOVERN
• HACK
• HATE
• HEALTH
• HOBBY
• HOSTS
• KIDS
• LEGAL
• LIFES
• MAIL
• MIL
• NEWS
• OCCULT
Content can simultaneously match multiple categories, therefore specific priority must be used for required evaluation precedence.

**Important:**

```
x-category string
```

This keyword can be used to configure runtime categories not present in the CLI.

- string specifies the unclassified category to be rated, and must be an alphanumeric string of 1 through 6 characters.
- A maximum of 10 x-categories can be configured.

```
action { allow | content-insert content_string | discard | redirect-url url | terminate-flow | www-reply-code-and-terminate-flow reply_code }
```

Specifies the action to take for the indicated result of content filtering analysis.

- **allow:** With static content filtering, this option allows the request for content. In dynamic content filtering it allows the content itself.
**content-insert content_string**: Specifies the content string to be inserted in place of the message returned from prohibited/restricted site or content server. For static content filtering, `content_string` is used to create a response to the subscriber’s attempt to get content. In dynamic content filtering, it is used to replace the content returned by a server. `content_string` must be an alphanumeric string of 1 through 1023 characters.

**discard**: For static content filtering, this option discards the packet(s) that requested. In dynamic content filtering, it discards the packet(s) that contain(s) the content.

**redirect-url url**: Redirects the subscriber to the specified URL. `url` must be an alphanumeric string of 1 through 1023 characters in the `http://search.com/subtarg=#HTTP.URL#` format.

**terminate-flow**: Terminates the TCP connection gracefully between the subscriber and server, and sends a TCP FIN to the subscriber and a TCP RST to the server.

**www-reply-code-and-terminate-flow reply_code**: Terminates the flow with the specified reply code. `reply_code` must be a reply code that is an integer from 100 through 599.

---

**Important**: Static-and-Dynamic Content Filtering is only supported in 9.0 and later releases.

```
edr edr_format_name
```

**Important**: This option is available only in 12.1 and earlier releases. In 12.2 and later releases, it is deprecated and replaced by the `reporting-edr` option.

Generates separate EDRs for content filtering based on action and content category using a specified EDR file format name.

`edr_format_name` is the name of a pre-defined EDR file format name in the EDR Format Configuration Mode, and must be an alphanumeric string of 1 through 63 characters.

---

**Important**: EDRs generated through this keyword are different from charging EDRs generated for subscriber accounting and billing. For more information on generation of charging EDRs, refer to the `ACS Rulebase Configuration Mode Commands` chapter.

```
reporting-edr reporting_edr_format_name
```

**Important**: This option is available only in 12.2 and later releases.

Generates separate reporting EDRs for Content Filtering based on the action and content category using the specified EDR file format name.

`reporting_edr_format_name` must be an alphanumeric string of 1 through 63 characters.

---

**Usage**

Use this command to specify the action and priorities for the indicated result of content filtering analysis. Up to 64 priorities and actions can be entered with this command.

**Example**

The following command sets priority 10 for category `ADULT` with action as `terminate-flow`:

```
analyze priority 10 category ADULT action terminate-flow
```
**discarded-flow-content-id**

Accounts for packets discarded as a result of content filtering action.

**Product**
CF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > CFP Configuration

```
active-charging service service_name > content-filtering category policy-id cf_policy_id
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-content-filtering-policy)#
```

**Syntax**

```
discarded-flow-content-id content_id

no discarded-flow-content-id
```

```
content_id
```

Specifies the content ID for discarded flows as an integer from 1 through 65535.

**Usage**

Use this command in the configuration to account for packets discarded as a result of CF action.

A flow end-condition EDR would be generated as a charging EDR for content-filtered packets. No billing EDRs (even with flow-end) would be generated for a discarded packet as the flow will not end. Dual EDRs would exist for customers who want to use “flow end” to get EDRs for charging, plus CF-specific EDRs. The second EDR for charging comes from the flow end-condition content-filtering configuration in the Rulebase Configuration Mode.

The **discarded-flow-content-id** configuration can be used for accumulating statistics for UDR generation in case CF discards the packets. These statistics for UDR generation (based on the CF content ID) would also be accumulated in case of ACS error scenarios where the packets are discarded but the flow does not end.

If, in the Rulebase Configuration Mode, the **content-filtering flow-any-error** configuration is set to **deny**, then all the denied packets will be accounted for by the **discarded-flow-content-id** config. That is, the **content_id** will be used to generate UDRs for the denied packets in case of content filtering.

**Example**

Use the following command to set the accumulation of statistics for UDR generation based on the CF content ID 1003:

```
discarded-flow-content-id 1003
```
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
**exit**

Exits the current mode and returns to the parent configuration mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

`exit`

**Usage**

Use this command to return to the parent configuration mode.
failure-action

Specifies the failure action when the content filtering analysis results are not available to analyze.

Product: CF
Privilege: Security Administrator, Administrator
Mode: Exec > ACS Configuration > CFP Configuration

active-charging service service_name > content-filtering category policy-id cf_policy_id

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-content-filtering-policy)#

Syntax

failure-action { allow | content-insert content_string | discard | redirect-url url | terminate-flow | www-reply-code-and-terminate-flow reply_code } [ edr edr_format_name ]

default failure-action [ edr edr_format_name ]

default

Configures the default setting of discard.

allow

In static content filtering, this option allows the request for content. In dynamic content filtering it allows the content itself.

**Important:** Static-and-Dynamic Content Filtering is only supported in 9.0 and later releases.

content-insertion content_string

Specifies the content string to be inserted in place of the message returned from the content server due to connection timeout or when no category policy ID is available for the content. For content filtering, the content_string is used to create a response to the subscriber’s attempt to get content. In dynamic content filtering it replaces the content returned by a server. content_string is an alphanumeric string of 1 through 1023 characters.

**Important:** Static-and-Dynamic Content Filtering is only supported in 9.0 and later releases.

discard

In static content filtering, specifies discarding the packet(s) that requested. In dynamic content filtering it discards the packet(s) that contain the content.
**Important:** Static-and-Dynamic Content Filtering is only supported in 9.0 and later releases.

```markdown
redirect-url url
```

Redirecets the subscriber to the specified URL.

*url* must be an alphanumeric string of 1 through 1023 characters, in the following format:

```
http://search.com/subtarg=#HTTP.URL#
```

```markdown
terminate-flow
```

Terminates the TCP connection gracefully between the subscriber and external server and sends a TCP FIN to the subscriber and a TCP RST to the server.

```markdown
www-reply-code-and-terminate-flow reply_code
```

Sets action as terminate-flow with a reply code that is a 3-digit integer from 100 through 599.

```markdown
edr edr_format_name
```

Specifies the name of a pre-defined EDR format to be generated on the content filtering action as an alphanumeric string of 1 through 63 characters.

**Usage**

Use this command to set the failure action to take when no content filtering analysis result is available to analyze for `analyze priority priority category category_string` command.

**Example**

The following command sets the failure action as `discard`:

```
failure-action discard
```
timeout action

This command has been deprecated, and is replaced by the failure-action command.
Content Filtering Server Group Configuration Mode sets the parameters for interoperating with a group of external servers. It is accessed by entering the `content-filtering server-group` command in the Context Configuration Mode.

Mode

`Exec > Global Configuration > Context Configuration > CFSG Configuration`  
`configure > context context_name > content-filtering server-group server_name`

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-content-filtering)#`

⚠️ **Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
connection retry-timeout

Configures the TCP connection retry timer for Internet Content Adaptation Protocol (ICAP) server and client.

Product
CF

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > CFSG Configuration

configure > context context_name > content-filtering server-group server_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-content-filtering)#

Syntax

connection retry-timeout duration

{ default | no } connection retry-timeout

---

default

Configures the default setting of 30 seconds.

no

Removes the connection retry timeout configuration.

duration

Specifies the duration (in seconds) as an integer from 1 to 3600. Default: 30

---

Usage

Use this command to configure the connection retry timer between ICAP server and client TCP connection, i.e. how long to wait before re-attempting to establish a TCP connection.

Example

The following command sets the ICAP client and server connection retry timer to 120 seconds:

connection retry-timeout 120
deny-message

Configures the text message that is returned to the subscriber in a deny response.

**Important:** This command is obsolete in 10.0 and later releases.

**Product**
CF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CFSG Configuration

```
configure > context context_name > content-filtering server-group server_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-content-filtering)#
```

**Syntax**

deny-message string

```
{ default | no } deny-message
```

**Usage**
Use this command to define a text message that is returned to the subscriber in a deny response.

**Example**
The following command sets the text message to no_Authorization in a deny message:

```
deny-message no_Authorization
```
deny-response code

Configures the deny response message that is to be sent from the ICAP server to the subscribers.

**Product**
ICAP

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CFSG Configuration

```
configure > context context_name > content-filtering server-group server_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-content-filtering)#
```

**Syntax**

```
deny-response code { 200 message string | 403 }
{ default | no } deny-response code
```

- **default**
  
  Configures the default setting of `deny-response code 200`.

- **no**
  
  Removes previously configured deny response message setting.

```
deny-response code 200 message string
```

- Specifies a text message that is to be returned to the subscriber in a code 200 deny response, as an alphanumeric string of 1 through 511 characters.

  If `deny-response code 200` is configured, the response sent to the subscriber will be of the form 200 OK with deny messages denied. If a message is configured for response code 200, that message will be used instead of "Access denied".

```
deny-response code 403
```

- This keyword is used to set response code 403 for the deny response message.

  When this keyword is configured, the deny response from the ICAP server will be sent “as is” to the subscriber.

**Usage**
Use this command to define a text message that is returned to the subscriber in a deny response.

**Example**

The following command sets the text message to *Not allowed* in a deny response message:

```
deny-response code 200 message Not allowed
```
dictionary

Specifies the dictionary to use for requests to the server(s) in this Content Filtering Server Group (CFSG).

**Product**
CF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CFSG Configuration

```
configure > context context_name > content-filtering server-group server_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-content-filtering)#
```

**Syntax**

```
dictionary { custom1 | custom2 | standard }
```

```
{ default | no } dictionary
```

---

**default**

Sets the default dictionary.
Default: **default**

---

**no**

Removes the previously configured dictionary setting.

---

**custom1**

Specifies a custom-defined dictionary that conforms to TS 32.015 v 3.6.0 for R99. It provides proprietary header fields for MSISDN and APN/subscriber. Please contact your local Cisco representative for more information.

---

**custom2**

Custom-defined dictionary. Please contact your local Cisco representative for additional information.

---

**custom3**

Custom-defined dictionary. Please contact your local Cisco representative for additional information.

---

**standard**

Default: Enabled
This dictionary uses an HTTP Get Request to specify the URL. It conforms to TS 32.215 v 4.6.0 for R4 (and also R5 - extended QoS format).
Usage
Use this command to specify the standard and customized encoding mechanism used for elements included in messages.

Example
The following command configures the system to use standard dictionary to encode messages:

```
default dictionary
```
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**
Use this command to return to the parent configuration mode.
failure-action

Specifies the actions to be taken when communication between ICAP endpoints within this Content Filtering Server Group (CFSG) fail.

Product
CF

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > CFSG Configuration
configure > context context_name > content-filtering server-group server_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-content-filtering)#

Syntax

failure-action { allow | content-insertion content_string | discard | redirect-url url | terminate-flow }

{ default | no } failure-action

default
Configures the default setting of terminate-flow.

no
Removes previously configured failure action.

allow
For static content filtering, this option allows the request for content. In dynamic content filtering, it allows the content itself.

content-insertion content_string
Specifies the content string to be used for failure action.
For static content filtering, the specified text is used to create a response to the subscriber’s attempt to get content. In dynamic content filtering, the specified text replaces the content returned by a server. content_string must be an alphanumeric string of 1 through 128 characters.

discard
For static content filtering, this option discards the packet(s) requested. In dynamic content filtering, it discards the packet(s) that contain(s) the content.

redirect-url url
Redirects the subscriber to the specified URL.
url must be an alphanumeric string of 1 through 128 characters in the following format:
http://search.com/subtarg=#HTTP.URL#

terminate-flow

For TCP, gracefully terminates the connection between the subscriber and external server, and sends a TCP FIN to the subscriber and a TCP RST to the server.

For WAP-Connection Oriented, the WSP session is gracefully terminated by sending WTP Aborts for each of the outstanding requests, and WSP Disconnect to the client and the server. For WSP-Connectionless, only the current WSP request is rejected.

Usage

Use this command to set the actions on failure for server connection.
ICAP rating is enabled for retransmitted packets when the default ICAP failure action was taken on an ICAP request for that flow. ICAP default failure action is taken on the pending ICAP request for a connection when the connection needs to be reset and there is no other redundant connection available. For example, in the ICAP request timeout and ICAP connection timeout scenarios, the retransmitted packet in the uplink direction is sent for ICAP rating again.

For WAP CO, uplink retransmitted packets for the WAP transactions for which ICAP failure action was taken will be sent for ICAP rating. The WSP header of the retransmitted packet is not parsed by the WSP analyzer. The URL received in the previous packet for that transaction is used for ICAP rating. If failure action was taken on multiple WTP transactions for the same flow (case: WTP concatenated GET request), the uplink retransmitted packet for each of the transactions is sent for rating again.

For HTTP, uplink retransmitted packets for the HTTP flow on which ICAP failure action is taken are sent for ICAP rating. The URL present in the current secondary session (last uplink request) is used for ICAP rating. However, if there were multiple outstanding ICAP requests for the same flow (pipelined request), the retransmitted packet for the URL sent for rating will be that of the last GET request.

Retransmission in various cases of failure-action taken on retransmitted packets when the ICAP response is not received for the original request and the retransmitted request comes in:
- WSP CO:
  - Permit: The uplink packet is sent for ICAP rating and depending on the ICAP response the WTP transaction is allowed/blocked. It is possible that the WAP gateway sends the response for the permitted GET request. Hence, there is a race condition and the subscriber may be able to view the web page even thought the rating was redirect or content insert.
  - Content Insert: The retransmitted packet is not sent for ICAP rating.
  - Redirect: The retransmitted packet is not sent for ICAP rating.
  - Discard: The uplink packet is sent for ICAP rating and depending on the ICAP response the WTP transaction is allowed/blocked.
  - Terminate flow: The uplink packet is sent for ICAP rating and depending on the ICAP response the WTP transaction is allowed or blocked. The WAP gateway may send an Abort transaction for this GET request if the WSP disconnect packet sent while terminating the flow is received by the WAP gateway.
- HTTP:
  - Permit: The uplink packet is sent for ICAP rating and depending on the ICAP response the last HTTP GET request. It is possible that the HTTP server sends the response for the permitted GET request. Hence there is a race condition and the subscriber may be able to view the web page even thought the rating was redirect or content insert.
  - Content Insert: Retransmitted packets are dropped and not charged.
- Redirect: Retransmitted packets are dropped and not charged.
- Discard: The uplink packet is sent for ICAP rating and depending on the ICAP response the WTP transaction allowed/blocked.
- Terminate flow: Retransmitted packets will be dropped and not charged.

**Example**

The following command sets the failure action to terminate:

```
failure-action terminate-flow
```
icap server

Adds an Internet Content Adaptation Protocol (ICAP) server configuration to the current Content Filtering Server Group (CFSG).

**Important:** In 8.1 and later releases, a maximum of five ICAP servers can be configured per Content Filtering Server Group. In 8.0 and earlier releases, only one ICAP Server can be configured per Content Filtering Server Group.

**Product:** CF

**Privilege:** Security Administrator, Administrator

**Mode:**

Exec > Global Configuration > Context Configuration > CFSG Configuration

`configure > context context_name > content-filtering server-group server_name`

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-content-filtering)#`

**Syntax**

```
icap server ip_address [ port port_number ] [ max messages ] [ priority priority ]
```

```
no icap server ip_address [ port port_number ] [ priority priority ]
```

**no**

Removes the specified ICAP server configuration from the current Content Filtering Server Group.

**ip_address**

Specifies the ICAP server’s IP address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

**port port_number**

Specifies the ICAP server’s port number to use for communications as an integer from 1 to 65535. Default: 1344

**max messages**

Specifies the maximum number of unanswered outstanding messages that may be allowed to the ICAP server as an integer from 1 to 4096. Default: 256

**Important:** The maximum outstanding requests per ICAP connection is limited to one. Therefore the value configured using the `max` keyword will be ignored.
priority priority

Specifies priority of the ICAP server in the current Content Filtering Server Group. The priority is used in server selection to determine which standby server becomes active. priority must be an integer from 1 (highest priority) to 65535 (lowest priority). Default: 1

**Important:** The priority keyword is only available in 8.1 and later releases.

**Usage**

This command is used to add an ICAP server configuration to a Content Filtering Server Group with which the system is to communicate for content filtering communication.

In 8.0, the ICAP solution supports only one connection between ACS Manager and ICAP server.

In 8.1, multiple ICAP server connections are supported per manager. At any time only one connection is active with the other connections acting as standby. In case of a connection failure, based on its priority, a standby connection becomes active. Any pending ICAP requests are moved to the new active connection. If a standby connection is unavailable, failure action is taken on all pending ICAP requests. See the failure-action command.

In 8.1 and later releases, a maximum of five ICAP servers can be configured per Content Filtering Server Group with a priority associated with each server. Once configured, an ICAP server’s priority cannot be changed. To change a server’s priority, the server configuration must be removed, and added with the new priority.

**Example**

The following command sets the ICAP server IP address to **10.2.3.4** and port to **1024**:

```
icap server 10.2.3.4 port 1024
```

The following command specifies an ICAP server with IP address **10.6.7.8**, port number **1024**, and priority **3**:

```
icap server 10.6.7.8 port 1024 priority 3
```
origin address

Specifies a bind address for the Content Filtering Server Group (CFSG) endpoint.

Product
CF

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > CFSG Configuration
configure > context context_name > content-filtering server-group server_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-content-filtering)#

Syntax

origin address ip_address

no origin address

no
Disables/releases the binding address for the CFSG endpoint.

ip_address
Specifies the IP address to bind the CFSG endpoint in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

Usage
Use this command to set the bind address for the CFSG endpoint.

Example
The following command sets the origin address of 10.1.1.1:

origin address 10.1.1.1
response-timeout

Sets the response timeout for the ICAP connection between the ICAP server and client.

Product
CF

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > CFSG Configuration
configure > context context_name > content-filtering server-group server_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-content-filtering)#

Syntax

response-timeout duration

{ default | no } response-timeout

  default
  Configures the default setting of 30 seconds.

  no
  Removes the response timeout configuration.

  duration
  Specifies the timeout duration (in seconds) as an integer from 1 to 300. Default: 30

Usage

Use this command to set the ICAP connection response timeout, after which connection will be marked as unsuccessful between ICAP endpoint.

Example

The following command sets the ICAP connection response timeout to 100 seconds:

response-timeout 100
timeout action

This command has been deprecated, and is replaced by the `failure-action` command.
url-extraction

Enables configuration of ICAP URL extraction behavior.

Product
CF

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > CFSG Configuration
configure > context context_name > content-filtering server-group server_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-content-filtering)#

Syntax

url-extraction { after-parsing | raw }

default url-extraction

___

default

Configures the default setting of after-parsing.

___

after-parsing

Specifies sending the parsed URI and host name. Percent-encoded hex characters in URLs sent from the ACF client to the ICAP server will be converted to corresponding ASCII characters before being sent. For example, the URL: http://www.google.co.uk/?this%20is%20a%20test will be sent to the ICAP server as:
http://www.google.co.uk/?this is a test

___

raw

Specifies sending raw URI and host name. The URLs will contain percent-encoded hex characters “as is”. For example, the URL http://www.google.co.uk/?this%20is%20a%20test will be sent to the ICAP server as:
http://www.google.co.uk/?this%20is%20a%20test

Usage

Use this command to configure the ICAP URL extraction behavior. Percent-encoded hex characters—for example, space (%20) and the percent character (%25)—in URLs sent from the ACF client to the ICAP server can be sent either as percent-encoded hex characters or as their corresponding ASCII characters.

Example

The following command configures URLs sent from the ACF client to the ICAP server to contain the escape encoding as is:

url-extraction raw
Chapter 51
Context Configuration Mode Commands A-D

This section includes the commands `aaa accounting` through `domain` service.

**Mode**

Exec > Global Configuration > Context Configuration

`configure > context context_name`

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-ctx)#`

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
aaa accounting

This command enables/disables accounting for subscribers and context-level administrative users for the current context.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration

configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

aaa accounting { administrator radius-diameter | subscriber [ radius-diameter ] }

default aaa accounting { administrator | subscriber }

no aaa accounting { administrator | subscriber } [ radius-diameter ]

default
Configures the default setting.
Default: RADIUS

no
Disables AAA accounting per the options specified.

radius-diameter
Enables AAA accounting for context-level administrative users.

subscriber
Enables AAA accounting for subscribers.

radius-diameter
Enables RADIUS or Diameter accounting for subscribers.

Usage
Use this command to enable/disable accounting for subscribers and context-level administrative users for the current context.
To enable or disable accounting for individual local subscriber configurations refer to the accounting-mode command in the Subscriber Configuration Mode Commands chapter.
**Important:** The accounting parameters in the APN Configuration Mode take precedence over this command for subscriber sessions. Therefore, if accounting is disabled using this command but enabled within the APN configuration, accounting is performed for subscriber sessions.

### Example

The following command disables AAA accounting for context-level administrative users:

```
no aaa accounting administrator
```

The following command enables AAA accounting for context-level administrative users:

```
aaa accounting administrator radius-diameter
```
aaa authentication

This command enables/disables authentication for subscribers and context-level administrative users for the current context.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration
configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

[ no ] aaa authentication { administrator | subscriber } { local | none | radius-diameter }

default aaa authentication { administrator | subscriber }

default

Configures the default setting for the specified parameter.

• administrator: local+RADIUS
• subscriber: RADIUS

no

Disables AAA authentication for administrator(s)/subscribers as specified.

• local: Disables local authentication for current context.
• none: Disables NULL authentication for current context, which enables both local and RADIUS-based authentication.
• radius-diameter: Disables RADIUS or Diameter-based authentication.

administrator | subscriber

• administrator: Enables authentication for administrative users.
• subscriber: Enables authentication for subscribers.

local | none | radius-diameter

Enables AAA authentication for administrator(s)/subscribers as specified.

• local: Enables local authentication for the current context.
• none: Disables authentication for the current context.
• radius-diameter: Enables RADIUS or Diameter-based authentication.
Usage
Use this command to enable/disable AAA authentication during specific maintenance activities or during test periods. The authentication can then be enabled again for the entire context as needed.

Example
The following command disables RADIUS or Diameter-based authentication for subscribers for the current context:

    no aaa authentication subscriber radius-diameter

The following command enables RADIUS or Diameter-based authentication for subscribers for the current context:

    aaa authentication subscriber radius-diameter
aaa constructed-nai

This command configures the password used during authentication for sessions using a Constructed Network Access Identifier (NAI) or an APN-specified user name.

**Product**
- PDSN
- GGSN

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration > Context Configuration
  - `configure > context context_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
aaa constructed-nai authentication [ [ encrypted ] password user_password | use-shared-secret-password ]

no aaa constructed-nai authentication
```

**no**

Disables authentication based upon the constructed NAI.

```
[ encrypted ] password user_password
```

**encrypted:** Specifies that the user password should be encrypted.

**password user_password:** Specifies an authentication password for the NAI-constructed user.

In 12.1 and earlier releases, the `user_password` must be an alphanumeric string of 0 through 63 characters with or without encryption.

In 12.2 and later releases, the `user_password` must be an alphanumeric string of 0 through 63 characters without encryption, or 1 through 132 characters with encryption.

```
use-shared-secret-password
```

Specifies using RADIUS shared secret as the password. Default: No password

**Usage**

This command configures passwords for user sessions that utilize a constructed NAI assigned via a PDSN service or a user name assigned via the APN configuration.

For simple IP sessions facilitated by PDSN services in which the `authentication allow-noauth` and `aaa constructed-nai` commands are configured, this command provides a password used for the duration of the session.

For PDP contexts using an APN in which the outbound user name is configured with no password, this command is used to provide the password. Additionally, this command is also used to provide a password for
situations in which an outbound username and password are configured and the authentication imsi-auth command has been specified.
The encrypted keyword is intended only for use by the system while saving configuration scripts. The system displays the encrypted keyword in the configuration file as a flag that the variable following the password keyword is the encrypted version of the plain text password. Only the encrypted password is saved as part of the configuration file.
If a password is configured with this keyword, then the specified password is used. Otherwise, an empty user-password attribute is sent.
Note that this configuration works in a different way for GGSN services. If a password is configured with this keyword for GGSN service, the specified password is used. Otherwise, if an outbound password is configured, that password is used. If no outbound password is configured, the RADIUS server secret is used as the user-password string to compute the user-password RADIUS attribute.
The NAI-construction consists of the subscriber’s MSID, a separator character, and a domain. The domain that is used is either the domain name supplied as part of the subscriber’s user name or a domain alias.

**Important:** The domain alias can be set with the nai-construction domain command in the PDSN Service Configuration mode, or the aaa default-domain subscriber command in the Global Configuration mode for other core network services.

The domain alias is determined according to the following rules:
- If the domain alias is set by nai-construction domain, that value is always used and the aaa default-domain subscriber value is disregarded, if set. The NAI is of the form <msid><symbol><nai-construction domain>.
- If the domain alias is not set by nai-construction domain, and the domain alias is set by aaa default-domain subscriber, the aaa default-domain subscriber value is used. The NAI is of the form <msid><symbol><aaa default-domain subscriber>.
- If the domain alias is not set by nai-construction domain or aaa default-domain subscriber, the domain name alias is the name of the source context for the PDSN service. The NAI is of the form <msid><symbol><source context of PDSN Service>.

The special separator character can be one of the following six: @, ~, %, \-, /.
The subscriber’s MSID is constructed in one of the formats displayed in the following figure.
The following command configures the authentication password for the NAI-constructed user.

```bash
aaa constructed-nai authentication
```
aaa filter-id rulebase mapping

This command configures the system to use the value of the Filter-Id AVP as the ACS rulebase name.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration
configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

[ no | default ] aaa filter-id rulebase mapping

- no
  Disables the mapping of Filter-Id AVP and ACS rulebase name.

- default
  Configures the default setting. Default: Disabled

Usage
Use this command to enable the mapping of Filter-Id attribute’s value returned during RADIUS authentication as the ACS rulebase name.
This feature provides the flexibility for operator to transact between multi-charging-service support for postpaid and prepaid subscribers through Access Control Lists (ACLs) entered in AAA profiles in RADIUS server to single-charging-service system based on rulebase configuration for postpaid and prepaid subscribers.
This feature internally maps the received ACL in to rulebase name and configures subscriber for postpaid or prepaid services accordingly.
When this feature is enabled and ACS rulebase attribute is not received from RADIUS or not configured in local default subscriber template system copies the filter-id attribute value to ACS rulebase attribute.
This copying happens only if the filter-id is configured and received from RADIUS server and ACS rulebase is not configured in ACS or not received from RADIUS.

Example
The following command enables the mapping value of the Filter-Id attribute to ACS rulebase name:

  aaa filter-id rulebase mapping
aaa group

This command enables/disables the creation, configuration or deletion of AAA server groups in the context.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration

```
configure > context context_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
aaa group group_name [ -noconfirm ]

no aaa group group_name
```

- **no**
  Deletes the specified AAA group.

- **group_name**
  Specifies name of the AAA group.
  If the specified AAA group does not exist, it is created, and the prompt changes to the AAA Server Group Configuration Mode, wherein the AAA group can be configured.
  If the specified AAA group already exists, the prompt changes to the AAA Server Group Configuration Mode, wherein the AAA group can be configured.
  `group_name` must be an alphanumeric string of 1 through 63 characters.

- **-noconfirm**
  Executes the command without any prompt and confirmation from the user.

**Usage**

Use this command to create/configure/delete AAA server groups within the context. Also, refer to the *AAA Server Group Configuration Mode Commands* chapter.

**Example**

The following command enters the AAA Server Group Configuration Mode for a AAA group named `test321`:

```
aaa group test321
```
aaa nai-policy

This command sets policies on how Network Access Identifiers (NAIs) are handled during the authentication process.

**Product**
GGSN
PDSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration
`configure > context context_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
[ default | no ] aaa nai-policy reformat-alg-hex-0-9
```

**default**

Sets the NAI policy back to its default setting which is to remap hexadecimal digits in NAIs and accept calls with embedded 0x00 hexadecimal digits.

**no**

Disable remapping of hexadecimal digits in the NAI and reject calls that have a 0x00 hexadecimal digit embedded in the NAI.

**reformat-alg-hex-0-9**

Default: Enabled
Controls remapping of NAIs that consist only of hex digits 0x00 through 0x09 or if a 0x00 hexadecimal digit is embedded in the NAI.

By default, the system remaps NAIs that consist solely of characters 0x00 through 0x09 to their ASCII equivalent. For example, 0x00 0x01 0x02 0x03 will get remapped to 123.

Also by default the system accepts an NAI containing one or more 0x00 characters within the NAI ignoring all characters after the first 0x00.

When this keyword is disabled NAIs are processed as follows:

- Remapping of hexadecimal digits 0x00 through 0x09 within the user-provided NAI is disabled.
- When the NAI has an embedded 0x00 character anywhere within it (including if there is an extra 0x00 character at the end) the call is rejected.

**Usage**

Use this command to disable or re-enable remapping of hexadecimal digits in the NAI.

**Example**

The following command disables the remapping of hexadecimal digits in the NAI:
no aaa nai-policy reformat-alg-hex-0-9
access-list undefined

Configures the behavior of access control for the current context when an undefined access control list is specified.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration

```bash
configure > context context_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```bash
access-list undefined { deny-all | permit-all }
{ default | no } access-list undefined
```

- **default**
  Configures the default setting.

- **no**
  Disables handling undefined access lists.

- **deny-all**
  Specifies to drop all packets when an undefined ACL is specified.

- **permit-all**
  Specifies to forward all packets when an undefined ACL is specified.

**Usage**

Use this command to specify the default behavior when an ACL specified does not exist. When the security policies require strict access control the `deny-all` handling should be configured.

**Example**

The following command sets the packet handling to ignore (drop) all packets when an undefined ACL is specified.

```bash
access-list undefined deny-all
```
administrator

Configures a user with Security Administrator privileges in the current context.

Product
- All

Privilege
- Security Administrator

Mode
- Exec > Global Configuration > Context Configuration

```console
configure > context context_name
```

Entering the above command sequence results in the following prompt:

```
[context_name] host_name(config-ctx)#
```

Syntax

```
administrator user_name [ encrypted ] password password [ | encrypted ] [ expiry-date date_time ] [ ftp ] [ li-administration ] [ nocli ] [ noecs ] [ timeout-absolute timeout_absolute ] [ timeout-min-absolute timeout_min_absolute ] [ timeout-idle timeout_idle ] [ timeout-min-idle timeout_min_idle ]
```

```
no administrator user_name
```

Removes Security Administrator privileges for the specified user name.

```
user_name
```

Specifies the username for which Security Administrator privileges must be enabled in the current context. `user_name` must be an alphanumeric string of 1 through 32 characters.

```
[ encrypted ] password password
```

Specifies password for the user name. Optionally, the `encrypted` keyword can be used to specify the password uses encryption. `password` must be an alphanumeric string of 1 through 63 characters without encryption, and 1 through 132 characters with encryption.

The `encrypted` keyword is intended only for use by the system while saving configuration scripts. The system displays the `encrypted` keyword in the configuration file as a flag that the variable following the `password` keyword is the encrypted version of the plain text password. Only the encrypted password is saved as part of the configuration file.

```
ecs
```

Permits the user to use ACS-specific configuration commands. Default: Permitted

```
expiry-date date_time
```

Specifies the date and time that this login account expires.
Enter the date and time in the YYYY:MM:DD:HH:mm or YYYY:MM:DD:HH:mm:ss format. Where YYYY is the year, MM is the month, DD is the day of the month, HH is the hour, mm is minutes, and ss is seconds.

**ftp**
Permits the user to use FTP and SFTP. Default: Not permitted

**li-administration**
Refer to the *Lawful Intercept Configuration Guide* for a description of this parameter.

**nocli**
Prevents the user from using the command line interface. Default: Permitted

**noecs**
Prevents the user from accessing ACS-specific commands.

**timeout-absolute timeout_absolute**

**timeout-min-absolute timeout_min_absolute**

**timeout-idle timeout_idle**

**timeout-min-idle timeout_min_idle**
Usage

Use this command to create new Security Administrators or modify existing user’s settings. Security Administrator users have read-write privileges and full access to all contexts and command modes. Refer to the Command Line Interface Overview chapter for more information.

**Important:** A maximum of 128 administrative users and/or subscribers may be locally configured per context.

Example

The following command creates a Security Administrator account named `user1` with access to ACS configuration commands:

```
administrator user1 password secretPassword
```

The following removes the Security Administrator account named `user1`:

```
no administrator user1
```
apn

Creates or deletes Access Point Name (APN) templates and enters the APN Configuration Mode within the current context.

Product

GGSN
P-GW
SAEGW

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > Context Configuration

configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

[ no ] apn apn_name [ -noconfirm ]

no

Deletes a previously configured APN template.

apn_name

Specifies a name for the APN template as an alphanumeric string of 1 through 62 characters that is case insensitive. It may also contain dots (.) and/or dashes (-).

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

⚠️ Caution: If this keyword option is used with the no apn apn_name command, the APN named apn_name will be deleted with all active/inactive subscribers without prompting any warning or confirmation.

Usage

This command creates an APN within the system and causes the CLI to enter the APN Configuration Mode. The APN is a logical name for a packet data network and/or a service to which the system supports access. When a create PDP context request is received by the system, it examines the APN information element within the packet. The system determines if an APN with the identical name is configured. If so, the system uses the configuration parameters associated with that APN as a template for processing the request. If the names do not match, the request is rejected with a cause code of 219 (DBH, Missing or unknown APN).

APN templates should be created/configured within destination contexts on the system.

- Up to 1000 APNs can be configured in the GGSN.
- In StarOS v12.x and earlier, up to 1024 APNs can be configured in the P-GW.
In StarOS v14.0 and later, up to 2048 APNs can be configured in the P-GW (SAEGW).

**Example**

The following command creates an APN template called *isp1*:

```
apn isp1```

asn-qos-descriptor

Creates, deletes or manages the Quality of Service (QoS) descriptor table identifier for Access Service Node Gateway (ASN-GW) service and enters the ASN QoS Descriptor Table Identifier Configuration mode within the source context.

Product
ASN-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration
configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

asn-qos-descriptor id qos_table_id [ default ] dscp [ be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af 43 | ef ] [ -noconfirm ]

no asn-qos-descriptor qos_table_id [ default ] dscp [ be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af 43 | ef ] [ -noconfirm ]

no

Deletes a previously configured ASN QoS descriptor table identifier.

id qos_table_id

Specifies a unique identifier for ASN QoS descriptor table to create/configure. qos_table_id must be an integer from 1 through 65535.

[ default ] dscp

Specifies DSCP marking for this QoS descriptor.

[ be | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af 43 | ef ]

The DSCP marking for this QoS descriptor. Default value is be (best effort).

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

⚠️ Caution: If this keyword option is used with no asn-qos-descriptor id qos_table_id command, the ASN QoS descriptor table with identifier qos_table_id will be deleted with all active/inactive configurations without prompting any warning or confirmation.
Usage

Use this command to configure a QoS description table to manage QoS functionality for an ASN-GW service subscriber. This command creates and allows the configuration of QoS tables with in a context. This command is also used to remove previously configured ASN-GW services QoS descriptor table. A maximum of 16 QoS Descriptor Tables can be configured per system.

Refer to the *ASN QoS Descriptor Configuration Mode Commands* chapter of this reference for additional information.

Example

The following command creates a QoS descriptor table with identifier 1234 for the ASN-GW service subscribers:

```
asn-qos-descriptor id 1234
```
asn-service-profile

Creates, deletes or manages the Service Profiles Identifier for Access Service Node Gateway (ASN-GW) service subscribers and enters the ASN Service Profile Configuration mode within the current context.

Product
ASN-GW

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration
  configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

asn-service-profile id asn_profile_id direction { bi-directional | downlink | uplink } [ activation-trigger { activate | admit | dynamic-reservation | provisioned } [ -noconfirm ]

no asn-service-profile id asn_profile_id [ -noconfirm ]

no
Deletes a previously configured ASN service profile identifier.

id asn-profile_id
Specifies a unique identifier for ASN profile to create/configure.

direction { bi-directional | downlink | uplink }
Specifies the direction of data traffic to apply this service profile.
  bi-directional: Enables this service profile in both direction of uplink and downlink.
  downlink: Enables this service profile in downlink direction, towards the subscriber.
  uplink: Enables this service profile in uplink direction, towards the system.

activation-trigger { activate | admit | dynamic-reservation | provisioned }
Use this option to configure the activation-trigger for the asn-service-profile. Default: provisioned | admit | activate

-noconfirm
Executes the command without any additional prompt and confirmation from the user.

⚠️ Caution: If this keyword option is used with no asn-service-profile id asn_profile_id command, the ASN service profile with identifier asn_profile_id will be deleted with all active/inactive configurations without prompting any warning or confirmation.
Usage

Use this command to configure a service profile to apply the ASN-GW service subscribers. This command creates and allows the configuration of service profiles within a context. This command is also used to remove previously configured ASN-GW services profiles. A maximum of 32 ASN Service Profiles can be configured per context. Refer to the ASN Service Profile Configuration Mode Commands chapter of this reference for additional information.

Example

The following command creates an ASN Service Profile with identifier 1234 for the ASN-GW service subscribers:

```
asn-service-profile id 1234 direction uplink
```
**asngw-service**

Creates, deletes or manages an Access Service Node Gateway (ASN-GW) service and enters the ASN Gateway Service Configuration Mode within the current context.

**Product**
ASN-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration

```
configure > context context_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
asngw-service asngw_name [ -noconfirm ]
```

```
o asngw-service asngw_name
do
```

Deletes a previously configured ASN-GW service.

```
asngw_name
```

Specifies the name of the ASN-GW service to create/configure as an alphanumeric string of 1 through 63 characters that is case sensitive.

---

**Important:** Service names must be unique across all contexts within a chassis.

**-noconfirm**

Executes the command without any additional prompt and confirmation from the user.

**Caution:** If this keyword option is used with `no asngw-service asngw_name` command, the ASN-GW service named `asngw_name` will be deleted with all active/inactive subscribers without prompting any warning or confirmation.

**Usage**

Services are configured within a context and enable certain functionality. This command creates and allows the configuration of services enabling the system to function as an ASN Gateway in a WiMAX network. This command is also used to remove previously configured ASN-GW services.

A maximum of 256 services (regardless of type) can be configured per system.
**Caution:** Large numbers of services greatly increase the complexity of management and may impact overall system performance (i.e. resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Refer to the *ASN Gateway Service Configuration Mode Commands* chapter of this reference for additional information.

**Example**

The following command creates an ASN-GW service name `asn-gw1`:

```
  asngw-service asn-gw1
```
asnpc-service

Creates, deletes or manages an ASN Paging Controller service to manage the ASN paging controller service and enters the ASN Paging Controller Configuration mode within the current context.

Product
ASN-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration
    configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

[ no ] asnpc-service asn_pc_svc_name [ -noconfirm ]

- no
Deletes a previously configured ASN paging controller service.

- asnpc-service asn_pc_svc_name
Specifies the name of the ASN Paging Controller Service to create and enable as an alphanumeric string of 1 through 63 characters that is case sensitive.

Important: Service names must be unique across all contexts within a chassis.

- -noconfirm
Executes the command without any additional prompt and confirmation from the user.

Caution: If this keyword option is used with no asnpc-service asn_pc_svc_name command, the ASN Paging Controller service named asn_pc_svc_name will be deleted and disabled with all active/inactive paging groups and paging agents configured in a context for ASN paging controller service without prompting any warning or confirmation.

Usage
Use this command to create and enable the ASN paging controller services in the system to provide functionality of an ASN Paging Controller service within a context. Additionally this command provides the access to the ASN Paging Controller Service Configuration mode and also used to remove previously configured ASN Paging Controller services.
A maximum of 256 services (regardless of type) can be configured per system.
Caution: Large numbers of services greatly increase the complexity of management and may impact overall system performance (i.e. resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Refer to the *ASN Paging Controller Service Configuration Mode Commands* chapter of this reference for additional information.

Example

The following command creates an ASN paging controller service name *asnpc_1*:

```
asnpc-service asnpc_1
```
atcf

This command enables Access Transfer Control Function (ATCF) functionality for the context. Default is disabled.

Product
SCM: P-CSCF, A-BG

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration
        configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

[ no ] atcf policy name atcf_policy_name [ -noconfirm ]

no
If previously configured, deletes the specified ATCF policy in the context.

atcf_policy_name
Specifies the name of the ATCF policy.
atcf_policy_name must be an alphanumeric string of 1 through 79 characters.

-noconfirm
Executes the command without any prompt and confirmation from the user.

Usage

Use this command to create/configure/delete an ATCF policy.
On entering this command, the CLI prompt changes to:

[context_name]host_name(config-atcf-atgw-policy)#

Refer to the CSCF ATCF-ATGW Policy Configuration Mode Commands chapter for additional information.

Example

The following command creates an ATCF Policy named access and enters the ATCF-ATGW Policy Configuration mode:

        atcf policy name access
**bfd-protocol**

Enables or disables Bidirectional Forwarding Detection (BFD) protocol and enters the BFD Configuration mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

```
[ no ] bfd-protocol
```

**Usage**

Use this command to set configuration parameters for detecting faults in paths established with BFD-enabled routers. Refer to the *BFD Configuration Mode Commands* chapter for additional information.

**Example**

The following command enables BFD Configuration mode:

```
bfd-protocol
```
### bgp extended-asn-cap

Enables or disables the router to send 4-octet ASN capabilities.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

```
[ no ] bgp extended-asn-cap
```

**no**

Disables the ability of the router to send 4-octet ASN capabilities.

**Example**

The following command enables the router to send 4-octet ASN Capabilities:

```
bgp extended-asn-cap
```
bmsc-profile

Creates or deletes Broadcast Multicast Service Center (BM-SC) profiles and enters the BMSC Profile Configuration Mode within the current context.

Product
GGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration
configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

[ no ] bmsc-profile name bmsc_profile_name [ -noconfirm ]

  no
  Deletes a previously configured BM-SC profile.

  name bmsc_profile_name
  Specifies a name for the BM-SC profile as an alphanumeric string of 1 through 62 characters that is case insensitive. It may also contain dots (.) and/or dashes (-).

  -noconfirm
  Executes the command without any additional prompt and confirmation from the user.

⚠️ Caution: If this keyword option is used with no bmsc-profile name bmsc_profile_name command, the BM-SC profile named bmsc_profile_name is deleted with all active/inactive subscribers without prompting any warning or confirmation.

Usage

Use this command to create a BM-SC profile within the context and take the user to enter the BMSC Profile Configuration Mode.
The BM-SC profile is a logical name for a Broadcast Multicast Service Center in Multimedia Broadcast and Multicast service.
BM-SC profile should be created/configured within contexts on the system. Up to four BM-SC profiles can be configured.

Example

The following command creates a BM-SC Profile called mbms_sc_1:

    bmsc-profile name mbms_sc_1
busout ip

Makes addresses from an IPv4 pool in the current context unavailable once they are free.

Product
GGSN
HA
NAT
PDSN
P-GW
SAEGW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration
configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

[ no ] busyout ip pool { all | all-dynamic | all-static | name pool_name } { address-range start_address end_address | lower-percentage percent | upper-percentage percent }

- no
  Disables the busyout command specified.

- ip
  Configure IPv4 busyout information.

- pool
  Configure IPv4 pool busyout information.

- all
  Applies to all IPv4 pools in the current context.

- all-dynamic
  Applies to all dynamic IPv4 pools in the current context.

- all-static
  Applies to all static IPv4 pools in the current context.
name pool_name

Applies the named IP pool or IP pool group in the current context. pool_name must be the name of an existing IP pool or IP pool group in the current context.

address-range start_address end_address

Busyout all addresses from start_address through end_address. start_address: The beginning IP address of the range of addresses to busyout entered in IPv4 dotted-decimal notation.
end_address: The ending IP address of the range of addresses to busyout. This IP address must exist in the pool specified and entered in IPv4 dotted-decimal notation.

lower-percentage percent

Busyout the percentage of IPv4 addresses specified, beginning at the lowest numbered IP address. This is a percentage of all of the IP addresses in the specified IP pool. percent must be an integer from 1 through 100.

upper-percentage percent

Busyout the percentage of IPv4 addresses specified, beginning at the highest numbered IP address. This is a percentage of all of the IPv4 addresses in the specified IP pool. percent must be an integer from 1 through 100.

Usage

Use this command to busyout IPv4 addresses when resizing an IPv4 pool.
Up to 32 instances of this command can be executed per context.
A single instance of this command can busy-out multiple IPv4 address pools in the context through the use of the all, all-static, or all-dynamic keywords.

Example

Assume an IPv4 pool named Pool10 with addresses from 192.168.100.1 through 192.168.100.254. To busy out the addresses from 192.168.100.50 through 192.169.100.100, enter the following command:

    busyout ip pool name Pool10 address-range 192.168.100.50 192.169.100.100

To restore the IPv4 addresses from the previous example and make them accessible again, enter the following command:

    no busyout ip pool name Pool10 address-range 192.168.100.50 192.169.100.100
busyout ipv6

Makes addresses from an IPv6 pool in the current context unavailable once they are free.

Product
GGSN
HA
NAT
PDSN
P-GW
SAEGW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration

configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

[ no ] busyout ipv6 pool { all | all-dynamic | all-static | name pool_name } [ address-range start_address end_address | lower-percentage percent | upper-percentage percent ]

no
Disables the busyout command specified.

ipv6
Configure IPv6 busyout information.

pool
Configure IPv6 pool busyout information.

all
Applies to all IPv6 pools in the current context.

all-dynamic
Applies to all dynamic IPv6 pools in the current context.

all-static
Applies to all static IPv6 pools in the current context.
**name pool_name**

Applies the named IPv6 pool or IPv6 pool group in the current context. *pool_name* must be the name of an existing IPv6 pool or IPv6 pool group in the current context.

**address-range start_address end_address**

Busyout all addresses from *start_address* through *end_address*. *start_address*: The beginning IP address of the range of addresses to busyout entered in IPv6 colon-separated-hexadecimal notation. *end_address*: The ending IP address of the range of addresses to busyout. This IP address must exist in the pool specified and entered in IPv6 colon-separated-hexadecimal notation.

**lower-percentage percent**

Busyout the percentage of IP addresses specified, beginning at the lowest numbered IPv6 address. This is a percentage of all of the IP addresses in the specified IP pool. *percent* must be an integer from 1 through 100.

**upper-percentage percent**

Busyout the percentage of IP addresses specified, beginning at the highest numbered IPv6 address. This is a percentage of all of the IP addresses in the specified IP pool. *percent* must be an integer from 1 through 100.

**Usage**

Use this command to busyout IPv6 addresses when resizing an IPv6 pool. Up to 32 instances of this command can be executed per context. A single instance of this command can busy-out multiple IP address pools in the context through the use of the **all, all-static**, or **all-dynamic** keywords.

**Example**

Assume an IP pool named *Pool12*. To busy out the addresses from *2700:2010:8003::* through *2700:2010:8003::*, enter the following command:

```
busyout ipv6 pool name Pool12 address-range 2700:2010:8003:: 2700:2010:8003::
```

To restore the IPv6 addresses from the previous example and make them accessible again, enter the following command:

```
no busyout ipv6 pool name Pool10 address-range 2700:2010:8003:: 2700:2010:8003::
```
cae-group

Creates a CAE group, which is a CAE server cluster that services TCP video requests from the Mobile Video Gateway. The Mobile Video Gateway uses the configured CAE group for CAE load balancing. The CAE (Content Adaptation Engine) is an optional component of the Mobile Videoscape.

Product
MVG

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration

configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

[ no ] cae-group cae_group_name [ -noconfirm ]

no cae_group_name

Deletes the CAE group if previously configured.

cae_group_name

Creates the specified CAE group and enters the Video Group Configuration Mode. cae_group_name is an alphanumeric string of 1 through 79 characters.

-noconfirm

Executes the command without any prompt and confirmation from the user.

Usage

Use this command to create a CAE group and enter the Video Group Configuration Mode. This command gets issued from the Context Configuration Mode.

Example

The following command creates a CAE group named group_1 and enters the Video Group Configuration Mode:

cae-group group_1
camel-service

Creates an instance of the Customized Applications for Mobile Enhanced Logic (CAMEL) service and enters the CAMEL service configuration mode. This mode configures or edits the configuration for the parameters which control the CAMEL functionality on the SGSN.

**Important:** For details about the commands and parameters, check the *CAMEL Service Configuration Mode* chapter.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration
`configure > context context_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
[ no ] camel-service srvc_name
```

- **no**
  Remove the configuration for the specified SGSN service from the configuration of the current context.

- **srvc_name**
  Creates a CAMEL service instance having a unique name expressed as an alphanumeric string of 1 through 63 characters.

**Important:** Service names must be unique across all contexts within a chassis.

**Usage**
Use this command to create, edit, or remove a CAMEL service

**Example**

The following command creates a CAMEL service named `camel1` in the current context:

```
camel-service camel1
```

The following command removes the CAMEL service named `camel2` from the configuration for the current context:

```
no camel-service camel2
```
cbs-service

Creates a new Cell Broadcasting Service (CBS) or specifies an existing CBS and enters the CBS Configuration Mode.

Product
HNB-GW

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration

\texttt{configure > context context\_name}

Entering the above command sequence results in the following prompt:

\texttt{[context\_name]\_host\_name(config-ctx)#}

Syntax

\[ \text{[ no \ ] cbs-service \ name} \]

<table>
<thead>
<tr>
<th>no</th>
</tr>
</thead>
<tbody>
<tr>
<td>Removes the specified CBS service from the context.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the name of a new or existing CBS service as an alphanumeric string of 1 through 63 characters that must be unique within the same context and across all contexts.</td>
</tr>
</tbody>
</table>

**Important:** Service names must be unique across all contexts within a chassis.

Usage

Use this command to create a new CBS service or modify an existing one.

Example

Following command creates a new CBS service names \texttt{test-cbs} in the context configuration mode:

\texttt{cbs-service test-cbs}

CBS Configuration Mode commands are defined in the \textit{CBS Configuration Mode Commands} chapter of this guide.
**cipher-suite**

Creates a new SSL cipher suite or specifies an existing cipher suite and enters the Cipher Suite Configuration Mode.

**Product**

SCM

**Privilege**

Administrator

**Mode**

Exec > Global Configuration > Context Configuration

```
configure > context context_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
[ no ] cipher-suite name
```

- **no**
  
  Removes the specified SSL cipher suite from the context.

- **name**
  
  Specifies the name of a new or existing SSL cipher suite as an alphanumeric string of 1 through 127 characters that must be unique across all CSCF services within the same context and across all contexts.

**Usage**

Use this command to create a new SSL cipher suite or modify an existing one.

**Important:** One SSL cipher suite can be created per SSL template.

A cipher suite contains the cryptographic algorithms supported by the client, and defines a key exchange and a cipher spec, which specifies the encryption and hash algorithms used during authentication. SSL cipher suites allow operators to select levels of security and to enable communication between devices with different security requirements.

Entering this command results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

Cipher Suite Configuration Mode commands are defined in the **Cipher Suite Configuration Mode Commands** chapter.

**Example**

The following command specifies the SSL cipher suite `cipher_suite_1` and enters the Cipher Suite Configuration Mode:

```
cipher-suite cipher_suite_1
```
class-map

Creates or deletes a class map. If the class-map is newly created, the system enters the Class-Map Configuration Mode within the current destination context to configure the match rules for packet classification to flow-based traffic policing for a subscriber session flow.

Product
ASN-GW
HA
HSGW
PDSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration

configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

[ no ] class-map name class_name [ match-all | match-any ]

---

no
Deletes configured Class-Map within the context.

---

class_name
Specifies the name of Class-Map rule as an alphanumeric string of 1 through 15 characters and is case sensitive.

---

match-all
Default: Enabled.
Enables AND logic for all matching parameters configured in specific Class-Map to classify traffic flow/packets. It indicates to match all classification rules in specific Class-Map to consider the specified Class-Map as a match.

---

match-any
Default: Disabled.
Enables OR logic for matching parameters configured in specific Class-Map to classify traffic flow/packets. It indicates to match any of the classification rule in specific Class-Map to consider the specified Class-Map as a match.
Usage

Use this command to enter in Class-Map Configuration Mode to set classification parameters or filters in traffic policy for a subscriber session flow.

**Important:** In this mode classification rules added sequentially with `match` command to form a Class-Map. To change and/or delete or re-add a particular rule entire Class-Map is required to delete.

Example

Following command configures classification map `class_map1` with option to match any condition in match rule.

```
class-map name class_map1 match-any
```
closedrp-rp handoff

Enables or disables session handoff between Closed-RP and RP connections. Default: Disabled

**Product**
PDSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration
configure > context context_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
closedrp-rp handoff

[ default | no ] closedrp-rp handoff
```

- **default**
  
  Resets the command to its default setting of disabled.

- **no**
  
  Disables Closed-RP to RP session handoff.

**Usage**

Use this command to enable a PDSN service to handoff sessions between Closed-RP and RP connections.

**Example**

To enable Closed-RP to RP handoffs, use the following command:

```
closedrp-rp handoff
```

To disable Closed-RP to RP handoffs, use the following command:

```
no closedrp-rp handoff
```
### config-administrator

Configures a context-level configuration administrator account within the current context.

**Product**
All

**Privilege**
Security Administrator

**Mode**
Exec > Global Configuration > Context Configuration

```
configure > context context_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
config-administrator user_name [ encrypted ] password [ ecs ] [ expiry-date date_time ] [ ftp ] [ li-administration ] [ nocli ] [ noecs ] [ timeout-absolute abs_seconds ] [ timeout-min-absolute abs_minutes ] [ timeout-idle timeout_duration ] [ timeout-min-idle idle_minutes ]
```

```
no config-administrator user_name
```

**no**

Removes a previously configured context-level configuration administrator account.

**user_name**

Specifies the name for the account as an alphanumeric string of 1 through 32 characters.

**[ encrypted ] password password**

Specifies the password to use for the user which is being given context-level administrator privileges within the current context. The encrypted keyword indicates the password specified uses encryption. `password` is an alphanumeric string of 1 through 63 characters without encryption, or 1 through 127 characters with encryption.

The encrypted keyword is intended only for use by the system while saving configuration scripts. The system displays the encrypted keyword in the configuration file as a flag that the variable following the password keyword is the encrypted version of the plain text password. Only the encrypted password is saved as part of the configuration file.

**ecs**

Permits the user access to ACS-specific configuration commands. Default: Enhanced Charging Service (ECS / ACS) specific configuration commands allowed.

**expiry-date date_time**

Specifies the date and time that this account expires in the format YYYY:MM:DD:HH:mm or YYYY:MM:DD:HH:mm:ss.
Where YYYY is the year, MM is the month, DD is the day of the month, HH is the hour, mm is minutes, and ss is seconds.

**ftp**
Indicates the user gains FTP and SFTP access with the administrator privileges. Default: FTP and SFTP are not allowed.

**li-administration**
Refer to the *Lawful Intercept Configuration Guide* for a description of this parameter.

**nocli**
Indicates the user is not allowed to access the command line interface. Default: CLI access allowed.

**noecs**
Prevents the specific user from accessing ACS-specific configuration commands.

**timeout-absolute** abs_seconds

*Important:* This keyword is obsolete. It has been left in place for backward compatibility. If used a warning is issued and the value entered is rounded to the nearest whole minute.

Specifies the maximum amount of time (in seconds) that the administrator may have a session active before the session is forcibly terminated. abs_seconds must be an integer from 0 through 300000000. The value 0 disables the absolute timeout. Default: 0

**timeout-min-absolute** abs_minutes

Specifies the maximum amount of time (in minutes) the context-level administrator may have a session active before the session is forcibly terminated. abs_minutes must be an integer from 0 through 525600 (365 days). The value 0 disables the absolute timeout. Default: 0

**timeout-idle** timeout_duration

*Important:* This keyword is obsolete. It has been left in place for backward compatibility. If used a warning is issued and the value entered is rounded to the nearest whole minute.

Specifies the maximum amount of idle time, in seconds, the context-level administrator may have a session active before the session is terminated. timeout_duration must be a value in the range from 0 through 300000000. The value 0 disables the idle timeout. Default: 0

**timeout-min-idle** idle_minutes

Specifies the maximum amount of idle time, in minutes, the context-level administrator may have a session active before the session is terminated. idle_minutes must be a value in the range from 0 through 525600 (365 days). The value 0 disables the idle timeout. Default: 0
Usage
Create new context-level configuration administrators or modify existing administrator’s options, in particular, the timeout values. Configuration administrator users have read-write privileges and full access to all contexts and command modes except for security functions. Refer to the Command Line Interface Overview chapter of this guide for more information.

Important: A maximum of 128 administrative users and/or subscribers may be locally configured per context.

Example
The following configures a context-level administration named user1 with ACS parameter control:

```
config-administrator user1 password secretPassword ecs
```

The following command removes a context-level administrator named user1:

```
no config-administrator user1
```
**content-filtering**

Enables or disables the creation, configuration or deletion of Content Filtering Server Groups (CFSG).

**Product**
CF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration  
`configure > context context_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
content-filtering server-group cf_server_group_name [ -noconfirm ]

no content-filtering server-group cf_server_group_name  

no

Removes the specified CFSG previously configured in this context.

server-group cf_server_group_name

Specifies the name of the CFSG as an alphanumeric string of 1 through 63 characters.

-noconfirm

Executes the command without any prompt and confirmation from the user.
```

**Usage**

Use this command to create/configure/delete a CFSG.

**Example**

The following command creates a CFSG named `CF_Server1`:

```
content-filtering server-group CF_Server1
```
credit-control-service

Enables or disables the creation, configuration or deletion of credit-control services.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration
configure > context context_name
Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

credit-control-service service_name [ -noconfirm ]
no credit-control-service service_name

no
Deletes the specified credit-control service.

service_name
Specifies name of the credit-control service as an alphanumeric string of 1 through 63 characters.
If the named credit-control service does not exist, it is created, and the CLI mode changes to the Credit Control Service Configuration Mode wherein the service can be configured.
If the named credit-control service already exists, the CLI mode changes to the Credit Control Service Configuration Mode wherein the service can be configured.

Important: Service names must be unique across all contexts within a chassis.

-noconfirm
Executes the command without any additional prompt and confirmation from the user.

Usage
Use this command to create, configure or delete credit-control services.
Entering this command results in the following prompt:

[context_name]host_name(config-credit-control-service)
Credit control Service Configuration commands are described in the Credit Control Service Configuration Mode Commands chapter.

Example
The following command enters the Credit Control Service Configuration Mode for a credit-control service named test159:
credit-control-service test159
crypto dns-nameresolver

Enables or disables the reverse DNS query from a Security Gateway to DNS.

Product
All IPsec security gateway products

Important: This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

Privilege
Security Administrator

Mode
Exec > Global Configuration > Context Configuration

configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

crypto dns-nameresolver

no crypto dns-nameresolver

no

Disables the Reverse DNS query.

Usage

Use this command to enable or disable the reverse DNS query from a WSG to DNS.

Important: You must configure the DNS client prior to enabling the Reverse DNS query.

Example

The following command enables the reverse DNS query:

crypto dns-nameresolver
crypto group

Creates or deletes a crypto group and enters the Crypto Configuration Mode allowing the configuration of crypto group parameters.

**Product**

HA
GGSN
PDIF
PDSN

**Privilege**

Administrator, Config-Administrator

**Mode**

Exec > Global Configuration > Context Configuration

`configure > context context_name`

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-ctx)#`

**Syntax**

```
[ no ] crypto group group_name
```

- **no**
  
  Deletes a previously configured crypto group.

- **group_name**
  
  Specifies the name of the crypto group as an alphanumeric string of 1 through 127 characters that is case sensitive.

**Important:** A maximum of 32 crypto groups per context can be configured.

**Usage**

Use this command to enter the configuration mode allowing the configuration of crypto group parameters. Crypto (tunnel) groups are used to support the Redundant IPSec Tunnel Fail-over feature and consist of two configured ISAKMP crypto maps. Each crypto map defines the IPSec policy for a tunnel. In the crypto group, one tunnel serves as the primary, the other as the secondary (redundant).

**Example**

The following command configures a crypto group called `group1`:

```
crypto group group1
```
crypto ipsec transform-set

Configures transform-sets on the system and enters the Crypto IPSec Transform Set Configuration Mode.

**Product**

PDSN
PDIF
HA
GGSN

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration

```
configure > context context_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```plaintext
```

```plaintext
no crypto ipsec transform-set transform_name
```

**no**

Removes a previously configured transform set

**transform_name**

Specifies the name of the transform set as an alphanumeric string of 1 through 127 characters that is case sensitive.

**ah hmac**

Configures the Authentication Header (AH) hash message authentication codes (HMAC) parameter for the transform set to one of the following:

- **md5-96**: Message Digest 5 truncated to 96 bits
- **sha1-96**: Secure Hash Algorithm-1 truncated to 96 bits

**esp hmac**

Configures the Encapsulating Security Payload (ESP) hash message authentication codes (HMAC) parameter for the transform set to one of the following:

- **md5-96**: Message Digest 5 truncated to 96 bits
- **none**: Disables the use of the AH protocol for the transform set.
- **sha1-96**: Secure Hash Algorithm-1 truncated to 96 bits
cipher

If ESP is enabled, this option must be used to set the encapsulation cipher protocol to one of the following:

- **3des-cbc**: Triple Data Encryption Standard (3DES) in chain block (CBC) mode.
- **aes-cbc-128**: Advanced Encryption Standard (AES) in CBC mode with a 128-bit key.
- **aes-cbc-256**: Advanced Encryption Standard (AES) in CBC mode with a 256-bit key.
- **des-cbc**: DES in CBC mode.

**Usage**

Use this command to create a transform set on the system. Transform Sets are used to define IPSec security associations (SAs). IPSec SAs specify the IPSec protocols to use to protect packets.

Transform sets are used during Phase 2 of IPSec establishment. In this phase, the system and a peer security gateway negotiate one or more transform sets (IPSec SAs) containing the rules for protecting packets. This negotiation ensures that both peers can properly protect and process the packets.

**Example**

Create a transform set that has the name `tset1`, no authentication header, an encapsulating security protocol header hash message authentication code of `md5`, and a bulk payload encryption algorithm of `des-cbc` with the following command:

```
crypto ipsec transform-set tset1 ah hmac none esp hmac md5 cipher des-cbc
```
crypto map

Configures the name of the policy and enters the specified Crypto Map Configuration mode.

Product
- PDSN
- HA
- GGSN
- P-GW
- PDIF
- SAEGW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration

configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

crypto map name [ ikev2-ipv6 | ipsec-dynamic | ipsec-ikev1 | ipsec-manual ]

no crypto map name

no
Removes a previously configured crypto map.

name
Specifies the name of the crypto map as an alphanumeric string of 1 through 127 characters that is case sensitive.

ikev2-ipv6
Refer to the Lawful Intercept Configuration Guide for a description of this parameter.

ipsec-dynamic
Creates a dynamic crypto map and/or enters the Crypto Map Dynamic Configuration Mode.

ipsec-ikev1
Creates an IKEv1 crypto map and/or enters the Crypto Map IKEv1 Configuration Mode.

ipsec-manual
Creates a manual crypto map and/or enters the Crypto Map Manual Configuration Mode.
Usage

Crypto Maps define the policies that determine how IPSec is implemented for subscriber data packets. There are several types of crypto maps supported by the system. They are:

- **Manual crypto maps**: These are static tunnels that use pre-configured information (including security keys) for establishment. Because they rely on statically configured information, once created, the tunnels never expire; they exist until their configuration is deleted.

**Important**: Because manual crypto map configurations require the use of static security keys (associations), they are not as secure as crypto maps that rely on dynamically configured keys. Therefore, it is recommended that they only be configured and used for testing purposes.

- **IKEv1 crypto maps**: These tunnels are similar to manual crypto maps in that they require some statically configured information such as the IP address of a peer security gateway and that they are applied to specific system interfaces. However, IKEv1 crypto maps offer greater security because they rely on dynamically generated security associations through the use of the Internet Key Exchange (IKE) protocol.

- **IKEv2-IPv6 cryptomaps**: Refer to the Lawful Intercept Configuration Guide for a description of this parameter.

- **Dynamic crypto maps**: These tunnels are used for protecting L2TP-encapsulated data between the system and an LNS/security gateway or Mobile IP data between an FA service configured on one system and an HA service configured on another.

**Important**: The crypto map type (dynamic, IKEv1, IKEv2-IPv6, or manual) is specified when the map is first created using this command.

Example

Create a dynamic crypto map named `map1` and enter the Crypto Map Dynamic Configuration Mode by entering the following command:

```
crypto map map1 ipsec-dynamic
```
crypto template

Creates a new or specifies an existing crypto template and enters the Crypto Template Configuration Mode.

Product
- ePDG
- HeNBGW
- PDIF
- SAEGW
- S-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration

\texttt{configure > context context\_name}

Entering the above command sequence results in the following prompt:

\texttt{[context\_name] host_name(config-ctx)#}

Syntax

\texttt{crypto template name ikev2-dynamic}

\texttt{no crypto template name}

\texttt{no}

Deletes a previously configured crypto template.

\texttt{name ikev2-pdif}

Specifies the name of a new or existing crypto template as an alphanumeric string of 1 through 127 characters.

\texttt{ikev2-dynamic}

Configures the Crypto Template to be used for configuring IPSec functionality.

Usage

Use this command to create a new or enter an existing crypto template.

Entering this command results in the following prompt:

\texttt{[context\_name] host_name(config-ctx)#}

Crypto Template Configuration Mode commands are defined in the \textit{Crypto Template Configuration Mode Commands} chapter.

Example

The following command configures a IKEv2 dynamic crypto template called \texttt{crypto1} and enters the Crypto Template Configuration Mode:
crypto template crypto1 ikev2-dynamic
cscf access-profile

Creates a new or enters an existing access profile used to set signaling compression for various network access types.

**Product**
SCM

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration
configure > context context_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
cscf access-profile { default | name profile_name } [ -noconfirm ]
```

- **no**
  Removes the CSCF access profile from the context.

- **default**
  Specifies that the system is to enter the Access Profile Configuration Mode for the default access profile.

- **name profile_name**
  Specifies a name for the access profile as an alphanumeric string of 1 through 79 characters.

- **-noconfirm**
  Executes the command without any additional prompt and confirmation from the user.

**Usage**
Use this command to create an access profile for the CSCF service and cause the system to enter the Access Profile Configuration Mode where parameters are configured for the profile. Entering this command results in the following prompt:

```
[context_name]host_name(config-cscf-access-profile)#
```

Access Profile Configuration Mode commands are defined in the **CSCF Access Profile Configuration Mode Commands** chapter.

**Example**
The following command creates a CSCF Access Profile named *profile2* and enters the Access Profile Configuration Mode:

```
cscf access-profile name profile2
```
cscf acl

Creates an Access Control List (ACL) and enters the ACL Configuration Mode.

Product
SCM

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration
configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

cscf acl { default | name list_name } [ -noconfirm ]

no cscf acl name list_name

Usage
Use this command to create an access control list for the CSCF service and cause the system to enter the ACL Configuration Mode where parameters are configured for the new list.

Entering this command results in the following prompt:

[context_name]host_name(config-cscf-acl)#

ACL Configuration Mode commands are defined in the CSCF ACL Configuration Mode Commands chapter.

Use this command when configuring the following SCM components: P-CSCF, S-CSCF, and SIP Proxy.

Example

The following command creates a CSCF access control list named acl1 and enters the ACL Configuration Mode:

cscf acl name acl1
cscf diameter-selection

Creates a CDF or HSS diameter selection table and enters the CSCF Diameter Selection Configuration Mode.

**Product**
SCM (S-CSCF)

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration

```bash
configure > context context_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]hostname(config-ctx)#
```

**Syntax**

```
[ no ] cscf diameter-selection type { cdf | hss } [ -noconfirm ]
```

- **no**
  Removes the specified CDF or HSS diameter selection table.

- **type { cdf | hss }**
  Specifies the type of diameter selection table.
  - **cdf**: Diameter selection table for selecting CDF server
  - **hss**: Diameter selection table for selecting HSS server

- **-noconfirm**
  Executes the command without any additional prompt and confirmation from the user.

**Usage**

Use this command to cause the system to enter the Diameter Selection Configuration Mode where parameters are configured for the diameter group.

**Important:** When HSS table has entries, this criteria is always applied for HSS server selection. CDF server selection, however, can be enabled or disabled for a given access type.

Entering this command results in the following prompt:

```
[context_name]hostname(config-cscf-diameter-selection)#
```

Diameter Selection Configuration Mode commands are defined in the CSCF Diameter Selection Configuration Mode Commands chapter.

**Example**

Use this command when configuring the S-CSCF.
The following command creates an HSS diameter selection table and enters the Diameter Selection Configuration Mode:

```
cscf diameter-selection type hss
```
cscf ifc-filter-criteria

Creates Initial Filter Criteria (iFC) filter criteria for shared iFC functionality.

Product
SCM (S-CSCF, SIP Proxy)

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration

configure > context context_name

Entering the above command sequence results in the following prompt:

/context_name/host_name(config-ctx)#

Syntax

```
cscf ifc-filter-criteria id fc_id priority priority [ profile-part-indicator { registered | unregistered } ] app-server uri scheme { sip | sips } as as-default-handling { session-continue | session-terminate } [ -noconfirm ] [ include-reg-request ] [ include-reg-response ] [ service-info info ] [ trigger-point tp_id ]
```

```
no cscf ifc-filter-criteria id fc_id
```

Removes the specified CSCF iFC filter criteria from the context.

```
id fc_id
```

Specifies an ID for the iFC filter criteria as an integer from 1 through 200.

```
priority priority
```

Specifies the priority of the filter criteria, which is used to select a particular filter criteria from multiple ones present under an ISC template. `priority` must be an integer from 0 through 1024.

```
profile-part-indicator { registered | unregistered }
```

Indicates whether the iFC is a part of the `registered` or `unregistered` user profile. If a value is not specified, then the configuration will be applied to both registered and unregistered subscribers.

```
app-server uri scheme { sip | sips }
```

Determines the associated application server’s URI scheme.

- `sip`: SIP URI
- `sips`: SIPS URI (TLS)

```
as
```

Specifies an address for the associated application server as an alphanumeric string of 1 through 127 characters.
as-default-handling { session-continue | session-terminate }
Determines whether the dialog should be released (session-terminate) or not (session-continue) when the application server could not be reached or on application server error is returned.

-noconfirm
Executes command without any additional prompt and confirmation from the user.

include-reg-request
Specifies inclusion of UE’s REGISTER to be included in 3rd party REGISTER request.

include-reg-response
Specifies inclusion of UE’s 200OK to be included in 3rd party REGISTER response.

service-info info
Specifies optional service information to be sent to the application server. info is an alphanumeric string of 1 through 63 characters.

trigger-point tp_id
Assigns an iFC trigger point to the filter criteria as an integer from 1 through 200.

Usage
Use this command to create a filter criteria ID and associate an application server address to it. You may also define a trigger point ID to be executed in order to select the application server. If no trigger point is specified, then the application server is selected unconditionally.

Important: Filter criteria is associated with an ISC template in the ISC Template Configuration Mode.

Important: Filter criteria can be assigned to more than one ISC template.

Example
The following command creates a iFC filter criteria 15, which has a priority of 2 and is part of the registered user profile. Filter criteria 15 is assigned to a sip application server named appserver. The dialog will not be released if the application server can not be reached. Filter criteria 15 is also assigned trigger point 12:

cscf ifc-filter-criteria id 15 priority 2 profile-part-indicator registered app-server uri scheme sip appserver as-default-handling session-continue trigger-point 12
cscf ifc-spt-condition

Creates an Initial Filter Criteria (iFC) Service Point Trigger (SPT) condition for shared iFC functionality.

**Product**
SCM (S-CSCF, SIP Proxy)

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration
`configure > context context_name`

Entering the above command sequence results in the following prompt:
`[context_name]host_name(config-ctx)#`

**Syntax**

```
cscf ifc-spt-condition id cond_id { request-uri content uri_content | session-case { originating-registered | originating-unregistered | terminating-registered | terminating-unregistered } | session-description sdp [ content sdp_data ] | sip-header hdr [ content hdr_data ] | sip-method method } [ -noconfirm ] [ condition-negated ]
```

```
no cscf ifc-spt-condition id cond_id
```

**no**
Removes the specified CSCF iFC SPT condition from the context.

**id cond_id**
Specifies an ID for the iFC SPT condition as an integer from 1 through 200.

**request-uri content uri_content**
Specifies request URI content as an alphanumeric string of 1 through 127 characters.

**Important:** Wildcard Extended Regular Expressions (ERE) are supported for this value. For example, \"sip.user[0-9]@192.168.176.150\".

**session-case** { originating-registered | originating-unregistered | terminating-registered | terminating-unregistered }

Determines the type of session:

- **originating-registered**: Session handling an originating end user.
- **originating-unregistered**: Session handling an unregistered originating end user.
- **terminating-registered**: Session handling a terminating registered end user.
- **terminating-unregistered**: Session handling a terminating unregistered end user.
Context Configuration Mode Commands A-D

session-description  

```
session-description sdp [ content sdp_data ]
```

Specifies an SDP line type.

- `sdp` is an alphanumeric string of 1 through 15 characters.
- `content` specifies content on the SDP line.
- `sdp_data` is an alphanumeric string of 1 through 127 characters.

sip-header  

```
sip-header hdr [ content hdr_data ]
```

Specifies a header type.

- `hdr` is an alphanumeric string of 1 through 127 characters.
- `content` specifies content on the header.
- `hdr_data` is an alphanumeric string of 1 through 127 characters.

sip-method  

```
sip-method method
```

Specifies a sip method.

- `method` is an alphanumeric string of 1 through 127 characters.

-noconfirm  

Executes the command without any additional prompt and confirmation from the user.

condition-negated  

Negates the specified condition.

Usage

Use this command to create individual SPT conditions that are later associated with an SPT group in the iFC SPT Group Configuration Mode.

Important: An iFC SPT group maybe associated with multiple SPT conditions.

Example

The following command creates iFC SPT condition 10 which handles an originating end user:

```
cscf ifc-spt-condition id 10 session-case originating-registered
```

The following command negates the condition created above:

```
cscf ifc-spt-condition id 10 session-case originating-registered condition-negated
```
cscf ifc-spt-group

Creates an Initial Filter Criteria (iFC) Service Point Trigger (SPT) group for shared iFC functionality.

**Product**
SCM (S-CSCF, SIP Proxy)

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration
configure > context context_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
cscf ifc-spt-group id group_id [ [ -noconfirm ] | reg-type { de-registration | initial-registration | re-registration } [ -noconfirm ] ]
```

```
no cscf ifc-spt-group id group_id
```

- `no`
  Removes the specified CSCF iFC SPT group from the context.

- `id group_id`
  Specifies an ID for the iFC SPT group as an integer from 1 through 200.

- `-noconfirm`
  Executes the command without any additional prompt and confirmation from the user.

- `reg-type { de-registration | initial-registration | re-registration }`
  Defines whether the SPT condition matches to REGISTER messages that are related to:
  - `de-registration`
  - `initial-registration`
  - `re-registration`

**Usage**

Use this command to create an iFC SPT group ID and bind different SPT conditions under it.

**Important:** An iFC SPT group may be associated with multiple SPT conditions.

The SPT group can also specify the registration type that defines whether the SPT condition matches to REGISTER messages that are related to initial registrations, re-registrations, or de-registrations.

Entering this command results in the following prompt:
iFC SPT Group Configuration Mode commands are defined in the *CSCF IFC SPT Group Configuration Mode Commands* chapter.

**Example**

The following command creates iFC SPT group 21:

```
cscf ifc-spt-group id 21
```
cscf ifc-trigger-point

Creates an Initial Filter Criteria (iFC) trigger point for shared iFC functionality.

Product
SCM (S-CSCF, SIP Proxy)

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration
configure > context context_name

Entering the above command sequence results in the following prompt:
[context_name]host_name(config-ctx)#

Syntax

cscf ifc-trigger-point id tp_id condition-type { cnf | dnf } [ -noconfirm ]

no cscf ifc-trigger-point id tp_id

no
Removes the specified CSCF iFC trigger point from the context.

id tp_id
Specifies an ID for the iFC trigger point as an integer from 1 through 200.

condition-type { cnf | dnf }
Defines the condition type of the iFC trigger point:
cnf: conjunctive normal form
dnf: disjunctive normal form

-noconfirm
Executes the command without any additional prompt and confirmation from the user.

Usage
Use this command to create a trigger point ID and bind different SPT groups under it.

Important: An iFC SPT group can be assigned to more than one iFC trigger point.

Entering this command results in the following prompt:
[context_name]host_name(config-cscf-ifc-trigger-point)#

IFC Trigger Point Configuration Mode commands are defined in the CSCF IFC Trigger Point Configuration Mode Commands chapter.
Example

The following command creates IF trigger point 11 with a cnf condition type:

```
cscf ifc-trigger-point id 11 condition-type cnf
```
cscf isc-template

Creates an IMS Service Control (ISC) template and enters the ISC Template Configuration Mode.

**Product**
SCM (S-CSCF)

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration
`configure > context context_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
[ no ] cscf isc-template id template_id
```

- **no**
  Removes the CSCF ISC template from the context.

```
cscf isc-template id template_id
```

Speceifies an ID for the ISC template as an integer from 1 through 200.

**Usage**

Use this command to create an ISC template for the CSCF service and cause the system to enter the ISC Template Configuration Mode where parameters are configured for the new template. Entering this command results in the following prompt:

```
[context_name]hostname(config-cscf-isc-tmpl)#
```

ISC Template Configuration Mode commands are defined in the *CSCF ISC Template Configuration Mode Commands* chapter.

Use this command when configuring the following SCM component: S-CSCF.

**Example**

The following command creates ISC template 10 and enters the ISC Template Configuration Mode:

```
cscf isc-template id 10
```
cscf last-route-profile

Creates a last route profile, which will be specified on peer server configuration to select the Last Routing Option (LRO) number while forwarding an emergency call packet to a particular peering server, and enters the Last Route Profile Criteria Configuration Mode.

Product
SCM

Privilege
Administrator

Syntax

```
cscf last-route-profile name profile_name criteria { county-name | round-robin } [ -noconfirm ]
no cscf last-route-profile name profile_name
```

- `no`
  Removes the specified CSCF last route profile from the context.

- `name profile_name`
  Specifies the name of the last route profile as an alphanumeric string of 1 through 79 characters.

- `criteria { county-name | round-robin }`
  - `county-name`
    Profile specific to the county-name criteria.
  Entering this command results in the following prompt:
  ```
  [context_name]hostname(config-county-name-lro-profile)#
  ```
  Last Route Profile Criteria Configuration Mode commands are defined in the **CSCF Last Route Profile Criteria Configuration Mode Commands** chapter.
  - `round-robin`
    Profile specific to the round-robin criteria.
  Entering this command results in the following prompt:
  ```
  [context_name]hostname(config-round-robin-lro-profile)#
  ```
  Last Route Profile Criteria Configuration Mode commands are defined in the **CSCF Last Route Profile Criteria Configuration Mode Commands** chapter.

- `-noconfirm`
  Executes the command without any additional prompt and confirmation from the user.

Usage

Use this command to create a last route profile and enter the Last Route Profile Criteria Configuration Mode.
**Important:** Last route profiles are associated with peer servers in the CSCF Peer Server Monitoring Configuration Mode.

Use this command when configuring the following SCM components: S-CSCF and SIP Proxy.

The following command creates a last route profile named `lro1` and enters the CSCF Last Route Profile Criteria Configuration Mode to specify county name criteria:

```
cscf last-route-profile name lro1 criteria county-name
```

The following command creates a last route profile named `lro2` and enters the CSCF Last Route Profile Criteria Configuration Mode to specify round robin criteria:

```
cscf last-route-profile name lro2 criteria round-robin
```
cscf peer-servers

Creates a peer server type for next-hop session routing and enters the Peer Servers Configuration Mode.

Product
SCM

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration

configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

```
cscf peer-servers server_name type { type } [ -noconfirm ]
```

```
no cscf peer-servers server_name
```

```
no
```

Removes the specified CSCF peer server from the context.

```
server_name
```

Specifies the name of the peer server as an alphanumeric string of 1 through 79 characters.

```
type { type }
```

Specifies the type of peer server to configure:

- **bgcf**: Border Gateway Control Function
- **ecscf**: Emergency Call/Session Control Function
- **ibcf**: Interconnect Border Control Function
- **icscf**: Interrogating Call/Session Control Function
- **mgcf**: Media Gateway Control Function
- **mrfc**: Media Resource Function Controller
- **other**: Other Function
- **pcscf**: Proxy Call/Session Control Function
- **scscf**: Serving Call/Session Control Function
- **sip-as**: Session Initiation Protocol-Application Server

```
-noconfirm
```

Executes the command without any additional prompt and confirmation from the user.
Usage
Use this command to create a specific peer server and enter the Peer Servers Configuration Mode where connectivity parameters can be entered.
Entering this command results in the following prompt:

```
[context_name]hostname(config-cscf-peer-servers)#
```

Peer Servers Configuration Mode commands are defined in the *CSCF Peer Servers Configuration Mode Commands* chapter.
Use this command when configuring the following SCM components: E-CSCF, P-CSCF, S-CSCF, and SIP Proxy.

Example
The following command creates an I-CSCF server type called *icscf_peer1* and enters the Peer Servers Configuration Mode:

```
cscf peer-servers icscf_peer1 type icscf
```
cscf peer-servers-group

Creates a peer servers group and enters the Peer Servers Group Configuration Mode.

Product
SCM

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration
configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

cscf peer-servers-group group_name type { bgcf | ecscf | ibcf | icscf | mgcf | mrfc | other | pcscf | scscf | sip-as } [ -noconfirm ]

no cscf peer-servers-group group_name

no
Removes the specified CSCF peer servers group from the context.

group_name
Specifies the name of the peer servers group as an alphanumeric string of 1 through 79 characters.

type { bgcf | ecscf | ibcf | icscf | mgcf | mrfc | other | pcscf | scscf | sip-as }

Specifies the type of peer servers group to configure.
bacf: Border Gateway Control Function
cescf: Emergency Call/Session Control Function
ibcf: Interconnect Border Control Function
icscf: Interrogating Call/Session Control Function
mgcf: Media Gateway Control Function
mrfc: Media Resource Function Controller
other: Other Function
pcscf: Proxy Call/Session Control Function
scscf: Serving Call/Session Control Function
sip-as: Session Initiation Protocol-Application Server

-noconfirm
Executes the command without any additional prompt and confirmation from the user.
Usage

Use this command to create a specific peer servers group and enter the Peer Servers Group Configuration Mode where peer servers lists can be managed. Entering this command results in the following prompt:

```
[context_name]hostname(config-cscf-peer-servers-group)#
```

Peer Servers Group Configuration Mode commands are defined in the CSCF Peer Servers Group Configuration Mode Commands chapter.

Example

The following command creates a peer servers group called `group1` and enters the Peer Servers Group Configuration Mode:

```
cscf peer-servers-group group1 type sip-as
```
cscf policy

Creates a policy group for specific AoR profiles and enters the Policy Configuration Mode.

**Product**
SCM

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration
`configure > context context_name`

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-ctx)#`

**Syntax**

```
cscf policy { default | name policy_name [-noconfirm] }
```

no cscf policy name policy_name

```
no
```

Removes the specified CSCF policy group from the context.

```
default
```

Specifies that the system is to enter the AoR Policy Rules Configuration Mode for the default policy. The default policy uses AoR policy rules. Entering this command results in the following prompt:

`[context_name]hostname(config-aor-policy)#`

Default (AoR) Policy Configuration Mode commands are defined in the *CSCF AoR Policy Rules Configuration Mode Commands* chapter.

```
name policy_name
```

Specifies the name of the policy group as an alphanumeric string of 1 through 79 characters. Entering this command results in the following prompt:

`[context_name]hostname(config-cscf-policy)#`

Policy Configuration Mode commands are defined in the *CSCF Policy Configuration Mode Commands* chapter.

```
-noconfirm
```

Executes the command without any additional prompt and confirmation from the user.

**Usage**

Use this command to create a policy group and enter either the AoR Policy Rules Configuration Mode (**default**) or Policy Configuration Mode (**name policy_name**). Use this command when configuring the following SCM components: P-CSCF, S-CSCF, and SIP Proxy.

**Example**
The following command creates a policy group named `group2` and enters the CSCF Policy Configuration Mode:

```
cscf policy name group2
```
cscf prefix-table

Creates a CSCF prefix table and enters the CSCF Prefix Table Configuration Mode.

**Product**
SCM

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration

`configure > context context_name`

Entering the above command sequence results in the following prompt:

`[context_name]hostname(config-ctx)#`

**Syntax**

```
[ no ] cscf prefix-table
```

- **no**
  Removes the prefix table.

**Usage**

Use this command to create a CSCF prefix table and cause the system to enter the Prefix Table Configuration Mode. The prefix table is used to configure for each number (or number prefix) whether it is ported and the SIP routing domain.

Entering this command results in the following prompt:

`[context_name]hostname(config-cscf-prefix-table)#`

Prefix Table Configuration Mode commands are defined in the *CSCF Prefix Table Configuration Mode Commands* chapter.

**Example**

The following command creates a CSCF prefix table and enters the Prefix Table Configuration Mode:

```
cscf prefix-table
```
cscf routes

Creates a route group for specifying routing information and enters the Routes Configuration Mode.

Product
SCM

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration

configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

cscf routes { default | name route_name [ -noconfirm ] }

no cscf routes name route_name

no
Removes the specified CSCF route group from the context.

default
Specifies that the system is to enter the Routes Configuration Mode for the default route group.

name route_name
Specifies the name of the route group as an alphanumeric string of 1 through 79 characters.

-noconfirm
Executes the command without any additional prompt and confirmation from the user.

Usage

Use this command to create a route group and enter the Routes Configuration Mode.

Entering this command results in the following prompt:

[context_name]host_name(config-cscf-route)#

Routes Configuration Mode commands are defined in the CSCF Routes Configuration Mode Commands chapter.

Use this command when configuring the following SCM components: P-CSCF, S-CSCF, SIP Proxy.

Example

The following command creates a route group named route_group5 and enters the Route Group Configuration Mode:

cscf routes name route_group5
cscf service

Creates a CSCF service or specifies an existing CSCF service and enters the CSCF Service Configuration Mode for the current context.

**Product**
SCM

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration

`configure > context context_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
[ no ] cscf service service_name [ -noconfirm ]
```

- **no**
  Removes the specified CSCF service from the context.

- **service_name**
  Specifies the name of the CSCF service. If `service_name` does not refer to an existing service, the new service is created if resources allow.
  `service_name` is an alphanumeric string of 1 through 63 characters.

**Important:** Service names must be unique across all contexts within a chassis.

- **-noconfirm**
  Executes the command without any additional prompt and confirmation from the user.

**Usage**

Enter the CSCF Service Configuration Mode for an existing service or for a newly defined service. This command is also used to remove an existing service.

A maximum of 256 services (regardless of type) can be configured per system.

**Caution:** Large numbers of services greatly increase the complexity of management and may impact overall system performance (for example, resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Entering this command results in the following prompt:
CSCF Service Configuration Mode commands are defined in the *CSCF Service Configuration Mode Commands* chapter. Use this command when configuring the following SCM components: P-CSCF, S-CSCF, SIP Proxy.

**Example**

The following command enters the existing CSCF Service Configuration Mode (or creates it if it does not already exist) for the service named `cscf-service1`:

```
cscf service cscf-service1
```

The following command will remove `cscf-service1` from the system:

```
no cscf service cscf-service1
```
cscf session-template

Creates a session template and/or enters the Session Template Configuration Mode.

**Product**

SCM

**Privilege**

Administrator

**Mode**

Exec > Global Configuration > Context Configuration

```bash
configure > context context_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```bash
cscf session-template { default | name template_name [ -noconfirm ] }
```

```bash
no cscf session-template name template_name
```

- **no**
  - Removes the specified CSCF session template from the context.

- **default**
  - Specifies that the system is to enter the Session Template Configuration Mode for the default session template.

- **name template_name**
  - Specifies a name for the template as an alphanumeric string of 1 through 79 characters.

- **-noconfirm**
  - Executes the command without any additional prompt and confirmation from the user.

**Usage**

Use this command to create a new session template and enter the Session Template Configuration Mode or enter the mode for an existing template.

Entering this command results in the following prompt:

```
[context_name]host_name(config-cscf-session-template)#
```

Session Template Configuration Mode commands are defined in the **CSCF Session Template Configuration Mode Commands** chapter.

Use this command when configuring the following SCM components: P-CSCF, S-CSCF, SIP Proxy.

**Example**

The following command enters the Session Template Configuration Mode for a template named `sess_temp4`:

```bash
```
cscf session-template name sess_temp4
cscf subdomain-routes

Creates subdomain-route list and enters the Subdomain-route List Configuration Mode.

Product
SCM (I-CSCF)

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration
configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

[ no ] cscf subdomain-routes

no
Removes the CSCF subdomain-route list from the context.

Usage
Use this command to create a subdomain-route list and enter the Subdomain-route List Configuration Mode. I-CSCF, upon receiving the terminating request, checks the subdomain-route list for matches. If a match is found, the routing will happen based on it. Otherwise, I-CSCF performs a User Location Query (Location-Information-Request) before proceeding.

Entering this command results in the following prompt:

[context_name]host_name(config-cscf-subdomain-route)#

Subdomain-route List Configuration Mode commands are defined in the CSCF Subdomain-route List Configuration Mode Commands chapter.

Example
The following command enters the Subdomain-route List Configuration Mode:

cscf subdomain-routes
cscf translation

Creates a translation list and enters the Translation Configuration Mode.

Product
SCM

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration

configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

```
cscf translation { default | name list_name [ -noconfirm ] }
no cscf translation name list_name
```

Usage

Use this command to create a new translation list and enter the Translation Configuration Mode or enter the mode for an existing list.
Translation lists are used to modify or replace a request-URI such as an E.164 number. For example, a translation list can be configured to append digits to the end of a number or replace a domain name with another.

Entering this command results in the following prompt:

```
[context_name]host_name(config-cscf-translation)#
```

Translation Configuration Mode commands are defined in the CSCF Translation Configuration Mode Commands chapter.

Example

Use this command when configuring the following SCM components: P-CSCF, S-CSCF, SIP Proxy.
The following command enters the Translation Configuration Mode for a translation list named `trans_list3`:

```
cscf translation name trans_list3
```
cscf urn-service-list

Creates a URN service list and enters the URN List Configuration Mode.

Product
SCM

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration

configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

cscf urn-service-list { default | name list_name [ -noconfirm ] }

no cscf urn-service-list name list_name

no

Removes the specified CSCF URN service list from the context.

default

Specifies that the system is to enter the URN List Configuration Mode for the default URN service list.

name list_name

Specifies a name for the URN service list as an alphanumeric string of 1 through 79 characters.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage

Use this command to create a URN service list name and enter the URN List Configuration Mode. URN lists contain URN to URI mappings used for emergency and location-based services. A URN service list is selected by a CSCF session template.

Entering this command results in the following prompt:

[context_name]host_name(config-cscf-service-urn)#

URN List Configuration Mode commands are defined in the CSCF URN List Configuration Mode Commands chapter.

Use this command when configuring the following SCM components: P-CSCF.

Example

The following command enters the URN List Configuration Mode for a URN list named urn_list1:
cscf urn-service-list name urn_list1
css server

In StarOS 9.0 and later releases, this command is obsolete. And, in earlier releases, this command is restricted.
**dhcp-client-profile**

Adds a specified Dynamic Host Control Protocol (DHCP) client profile name to allow configuration of DHCP client profile to the current context and enters the configuration mode for that profile.

**Product**

GGSN
P-GW
SAEGW

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration

```
configure > context context_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
[ no ] dhcp-client-profile clnt_profile_name [ -noconfirm ]
```

- `no`
  
  Removes a previously configured DHCP client profile from the current context.

- `clnt_profile_name`
  
  Specifies the name of the DHCP client profile as an alphanumeric string of 1 through 63 characters that is case sensitive.

- `noconfirm`
  
  Executes the command without any additional prompt and confirmation from the user.

⚠️ **Caution:** If this keyword option is used with `no dhcp-client-profile clnt_profile_name` command the DHCP client profile named `clnt_profile_name` is deleted with all active/inactive subscribers without prompting any warning or confirmation.

**Usage**

Use this command to add a DHCP client profile to a context configured on the system and enter the DHCP Client Profile Configuration Mode. Entering this command results in the following prompt:

```
[context_name]host_name(config-dhcp-client-profile)#
```

DHCP Client Profile Configuration Mode commands are defined in the *DHCP Client Profile Configuration Mode Commands* chapter.
The following command creates a DHCP client profile called `test_profile`:

```
dhcp-client-profile test_profile
```
dhcp-server-profile

Adds a specified Dynamic Host Control Protocol (DHCP) server profile name to allow configuration of DHCP server profile to the current context and enters the configuration mode for that profile.

**Product**
GGSN
P-GW
SAEGW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration
configure > context context_name
Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
[ no ]dhcp-server-profile srvr_profile_name [ -noconfirm ]
```

- **no**
  Removes a previously configured DHCP server profile from the current context.

- **srvr_profile_name**
  Specifies the name of the DHCP server profile as an alphanumeric string of 1 through 63 characters that is case sensitive.

- **-noconfirm**
  Executes the command without any additional prompt and confirmation from the user.

**Caution:** If this keyword option is used with `no dhcp-server-profile srvr_profile_name` command the DHCP server profile named `srvr_profile_name` is deleted with all active/inactive subscribers without prompting any warning or confirmation.

**Usage**

Use this command to add a DHCP server profile to a context configured on the system and enter the DHCP Server Profile Configuration Mode.

Entering this command results in the following prompt:

```
[context_name]host_name(config-dhcp-server-profile)#
```

DHCP Server Profile Configuration Mode commands are defined in the *DHCP Server Profile Configuration Mode Commands* chapter.

**Example**
The following command creates a DHCP server profile called `test_server_profile`:

```
dhcp-server-profile test_server_profile
```
dhcp-service

Adds a Dynamic Host Control Protocol (DHCP) service instance to the current context and enters the configuration mode for that service.

Product
ASN-GW
eWAG
GGSN
HA
P-GW
SAEGW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration
  configure > context context_name
  Entering the above command sequence results in the following prompt:
  [context_name]host_name(config-ctx)#

Syntax

dhcp-service service_name [ no ] allow dhcp-relay-agent-auth-suboption[ -noconfirm ]

no dhcp-service service_name

<table>
<thead>
<tr>
<th>no</th>
</tr>
</thead>
<tbody>
<tr>
<td>Removes a previously configured DHCP service from the current context.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>service_name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the name of the DHCP service as an alphanumeric string of 1 through 63 characters that is case sensitive.</td>
</tr>
</tbody>
</table>

Important: Service names must be unique across all contexts within a chassis.

allow dhcp-relay-agent-auth-suboption
The DHCP Relay Agent Information Option conveys information between a DHCP Relay Agent and a DHCP server. This specification defines an authentication suboption for that option, containing a keyed hash in its payload. The suboption supports data integrity and replay protection for relayed DHCP messages.

-noconfirm
Executes the command without any additional prompt and confirmation from the user.
Caution: If this keyword option is used with `no dhcp-service service_name` command the DHCP service named `service_name` is deleted with all active/inactive subscribers without prompting any warning or confirmation.

Usage

Use this command to add a DHCP service to a context configured on the system and enter the DHCP Service Configuration Mode. A DHCP service is a logical grouping of external DHCP servers. The DHCP Configuration Mode provides parameters that dictate the system’s communication with one or more of these DHCP servers. A maximum of 256 services (regardless of type) can be configured per system.

Caution: Large numbers of services greatly increase the complexity of management and may impact overall system performance (i.e. resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Example

Refer to the `DHCP Service Configuration Mode` chapter of this reference for additional information.

The following command creates a DHCP service called `dhcp1` and enter the DHCP Service Configuration Mode:

```
dhcp-service dhcp1
```
dhcpv6-service

Creates a specified DHCPv6 service name to allow configuration of DHCPv6 service to the current context and enters the configuration mode for that service.

Product
GGSN
P-GW
SAEGW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration
configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

[ no ]dhcpv6-service service_name [ -noconfirm ]

no
Removes a previously configured DHCPv6 service from the current context.

service_name
Specifies the name of the DHCPv6 service as an alphanumeric string of 1 through 63 characters that is case sensitive.

Important: Service names must be unique across all contexts within a chassis.

-noconfirm
Executes the command without any additional prompt and confirmation from the user.

Caution: If this keyword option is used with no dhcpv6-service service_name command the DHCPv6 service named service_name is deleted with all active/inactive subscribers without prompting any warning or confirmation.

Usage
Use this command to add a DHCPv6 service to a context configured on the system and enter the DHCPv6 Service Configuration Mode.
The DHCPv6 Service Configuration Mode provides parameters that dictate the system’s communication with one or more of these DHCPv6 servers.
Entering this command results in the following prompt:
DHCPv6 Service Configuration Mode commands are defined in the *DHCPv6 Service Configuration Mode Commands* chapter.

**Important:** A maximum of 3 DHCPv6 services can be configured per system.

### Example

The following command creates a DHCPv6 service called `dhcpv6` and enter the DHCPv6 Service Configuration Mode:

```
dhcpv6-service dhcpv6
```
diameter accounting

This command configures Diameter accounting related settings.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration
configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

diameter accounting { dictionary { aaa-custom1 | aaa-custom10 | aaa-custom2 | aaa-custom3 | aaa-custom4 | aaa-custom5 | aaa-custom6 | aaa-custom7 | aaa-custom8 | aaa-custom9 | dynamic-load | nasreq | rf-plus } | endpoint endpoint_name | hd-mode fall-back-to-local | hd-storage-policy hd_policy | max-retries max_retries | max-transmissions transmissions | request-timeout duration | server host_name priority priority }

default diameter accounting { dictionary | hd-mode | max-retries | max-transmissions | request-timeout }

no diameter accounting { endpoint | hd-mode | hd-storage-policy | max-retries | max-transmissions | server host_name }

endpoint: Removes the currently configured accounting endpoint. The default accounting server configured in the default AAA group will be used.
hd-mode: Sends records to the Diameter server, if all Diameter servers are down or unreachable, then copies records to the local HDD and periodically retries the Diameter server.
hd-storage-policy: Disables use of the specified HD storage policy.
max-retries: Disables the retry attempts for Diameter accounting in this AAA group.
max-transmissions: Disables the maximum number of transmission attempts for Diameter accounting in this AAA group.
server host_name: Removes the Diameter host host_name from this AAA server group for Diameter accounting.

default diameter accounting { dictionary | hd-mode | max-retries | max-transmissions | request-timeout }

dictionary: Sets the context’s dictionary to the default.
hd-mode: Sends records to the Diameter server, if all Diameter servers are down or unreachable, then copies records to the local HDD and periodically retries the Diameter server.
max-retries:0 (disabled)
max-transmissions:0 (disabled)
request-timeout: 20 seconds

dictionary { aaa-custom1 | aaa-custom10 | aaa-custom2 | aaa-custom3 | aaa-custom4
| aaa-custom5 | aaa-custom6 | aaa-custom7 | aaa-custom8 | aaa-custom9 | dynamic-load | nasreq | rf-plus }

Specifies the Diameter accounting dictionary.

aaa-custom1 ... aaa-custom10: Configures the custom dictionaries. Even though the CLI syntax supports several custom dictionaries, not necessarily all of them have been defined. If a custom dictionary that has not been implemented is selected, the default dictionary will be used.

dynamic-load: Configures the dynamically loaded Diameter dictionary. The dictionary name must be an alphanumeric string of 1 through 15 characters. For more information on dynamic loading of Diameter dictionaries, see the diameter dynamic-dictionary in the Global Configuration Mode Commands chapter of this guide.

nasreq: nasreq dictionary—the dictionary defined by RFC 3588.

rf-plus: RF Plus dictionary.

endpoint endpoint_name

Enables Diameter to be used for accounting, and specifies which Diameter endpoint to use. endpoint_name is an alphanumeric string of 1 through 63 characters.

hd-mode fall-back-to-local

Specifies that records be copied to the local HDD if the Diameter server is down or unreachable. CDF/CGF will pull the records through SFTP.

hd-storage-policy hd_policy

Specifies the HD Storage policy name. hd_policy must be the name of a configured HD Storage policy, expressed as an alphanumeric string of 1 through 63 characters.

HD storage policies are configured through the Global Configuration Mode. This and the hd-mode command are used to enable the storage of Rf Diameter Messages to HDD incase all Diameter Servers are down or unreachable.

max-retries max_retries

Specifies how many times a Diameter request should be retried with the same server, if the server fails to respond to a request. max_retries specifies the maximum number of retry attempts. The value must be an integer from 1 through 1000.

Default: 0

max-transmissions transmissions

Specifies the maximum number of transmission attempts for a Diameter request. Use this in conjunction with the “max-retries max_retries” option to control how many servers will be attempted to communicate with.

transmissions specifies the maximum number of transmission attempts for a Diameter request. The value must be an integer from 1 through 1000. Default: 0
request-timeout duration

Specifies how long the system will wait for a response from a Diameter server before re-transmitting the request.
duration specifies the number of seconds the system will wait for a response from a Diameter server before re-transmitting the request. This value must be an integer from 1 through 3600. Default: 20

server host_name priority priority

Specifies the current context Diameter accounting server’s host name and priority.
host_name specifies the Diameter host name, expressed as an alphanumeric string of 1 through 63 characters.
priority specifies the relative priority of this Diameter host. The priority is used in server selection. The priority must be an integer from 1 through 1000.

Usage

Use this command to manage the Diameter accounting options according to the Diameter server used for the context.

Example

The following command configures the Diameter accounting dictionary as aaa-custom4:

diameter accounting dictionary aaa-custom4

The following command configures the Diameter endpoint named aaaa_test:

diameter accounting endpoint aaaa_test
diameter authentication

This command configures Diameter authentication related settings.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration

```
configure > context context_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
diameter authentication { dictionary { aaa-custom1 | aaa-custom10 | aaa-custom11 | aaa-
custom12 | aaa-custom13 | aaa-custom14 | aaa-custom15 | aaa-custom16 | aaa-custom17 | 
    aaa-custom18 | aaa-custom19 | aaa-custom2 | aaa-custom20 | aaa-custom3 | aaa-custom4 | 
    aaa-custom5 | aaa-custom6 | aaa-custom7 | aaa-custom8 | aaa-custom9 | dynamic-load | 
    nasreq } | endpoint endpoint_name | max-retries max_retries | max-transmissions 
    transmissions | redirect-host-avp { just-primary | primary-then-secondary } | request-timeout duration | server host_name priority priority }

default diameter authentication { dictionary | max-retries | max-transmissions | 
    redirect-host-avp | request-timeout }

no diameter authentication { endpoint | max-retries | max-transmissions | server 
    host_name }
```

- **endpoint**: Removes the authentication endpoint. The default server configured in default AAA group will be used.
- **max-retries**: Disables the retry attempts for Diameter authentication in this AAA group.
- **max-transmissions**: Disables the maximum transmission attempts for Diameter authentication in this AAA group.
- **server host_name**: Removes the Diameter host host_name from this AAA server group for Diameter authentication.

```
default diameter authentication { dictionary | max-retries | max-transmissions | 
    redirect-host-avp | request-timeout }

Configures default setting for specified parameter.
- **dictionary**: Sets the context’s dictionary to the default.
- **max-retries**: Sets the retry attempts for Diameter authentication requests in this AAA group to default 0 (disable).
• **max-transmissions**: Sets the configured maximum transmission attempts for Diameter authentication in this AAA group to default 0 (disable).

• **redirect-host-avp**: Sets the redirect choice to default (just-primary).

• **request-timeout**: Sets the timeout duration, in seconds, for Diameter authentication requests in this AAA group to default (20).

```plaintext
```

Specifies the Diameter authentication dictionary.

aaa-custom1 ... aaa-custom8, aaa-custom10 ... aaa-custom20: Configures the custom dictionaries. Even though the CLI syntax supports several custom dictionaries, not necessarily all of them have been defined. If a custom dictionary that has not been implemented is selected, the default dictionary will be used.

**Important:** aaa-custom1 dictionary is only available in Release 8.1 and later. aaa-custom2 to aaa-custom20 dictionaries are only available in Release 9.0 and later releases.

aaa-custom9: Configures the STa standard dictionary.

dynamic-load: Configures the dynamically loaded Diameter dictionary. The dictionary name must be an alphanumeric string of 1 through 15 characters. For more information on dynamic loading of Diameter dictionaries, see the [diameter dynamic-dictionary](#) in the Global Configuration Mode Commands chapter of this guide.

nasreq: nasreq dictionary—the dictionary defined by RFC 3588.

```plaintext
endpoint  endpoint_name
```

Enables Diameter to be used for authentication, and specifies which Diameter endpoint to use. `endpoint_name` is an alphanumeric string of 1 through 63 characters.

```plaintext
max-retries  max_retries
```

Specifies how many times a Diameter authentication request should be retried with the same server, if the server fails to respond to a request. `max_retries` specifies the maximum number of retry attempts, and must be an integer from 1 through 1000. Default: 0

```plaintext
max-transmissions  transmissions
```

Specifies the maximum number of transmission attempts for a Diameter authentication request. Use this in conjunction with the "max-retries max_retries" option to control how many servers will be attempted to communicate with. `transmissions` specifies the maximum number of transmission attempts, and must be an integer from 1 through 1000. Default: 0

```plaintext
diameter authentication redirect-host-avp { just-primary | primary-then-secondary }
```

Specifies whether to use just one returned AVP, or use the first returned AVP as selecting the primary host and the second returned AVP as selecting the secondary host.
just-primary: Redirect only to primary host.
primary-then-secondary: Redirect to primary host, if fails then redirect to the secondary host.
Default: just-primary

request-timeout duration
Specifies how long the system will wait for a response from a Diameter server before re-transmitting the request.
duration specifies the number of seconds the system will wait for a response from a Diameter server before re-transmitting the request, and must be an integer from 1 through 3600. Default: 20

server host_name priority priority
Specifies the current context Diameter authentication server’s host name and priority.
host_name specifies the Diameter host name, expressed as an alphanumeric string of 1 through 63 characters.
priority specifies the relative priority of this Diameter host, and must be an integer from 1 through 1000. The priority is used in server selection.

Usage
Use this command to manage the Diameter authentication configurations according to the Diameter server used for the context.

Example
The following command configures the Diameter authentication dictionary aaa-custom14:

diameter authentication dictionary aaa-custom14

The following command configures the Diameter endpoint named aaaul:

diameter authentication endpoint aaaul
diameter authentication failure-handling

This command configures error handling for Diameter EAP requests.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration

configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

diameter authentication failure-handling { authorization-request | eap-request | eap-termination-request } { request-timeout action { continue | retry-and-terminate | terminate } | result-code result_code { [ to end_result_code ] action { continue | retry-and-terminate | terminate } } }

no diameter authentication failure-handling { authorization-request | eap-request | eap-termination-request } result-code result_code [ to end_result_code ]

default diameter authentication failure-handling { authorization-request | eap-request | eap-termination-request } request-timeout action

no
Disables Diameter authentication failure handling.

default
Configures the default Diameter authentication failure handling setting.

authorization-request
Specifies that failure handling is to be performed on Diameter authorization request messages (AAR/AAA).

eap-request
Specifies configuring failure handling for EAP requests.

eap-termination-request
Specifies configuring failure handling for EAP termination requests.

request-timeout action { continue | retry-and-terminate | terminate }
Specifies the action to be taken for failures:
  *continue:Continues the session
- **retry-and-terminate**: First retries, if it fails then terminates the session
- **terminate**: Terminates the session

```plaintext
result-code result_code { [ to end_result_code ] action { continue | retry-and-terminate | terminate } }
```

*result-code*: Specifies the result code, must be an integer from 1 through 65535.
*to end_result_code*: Specifies the upper limit of a range of result codes. *end_result_code* must be greater than *result_code*.
*action { continue | retry-and-terminate | terminate }*: Specifies action to be taken for failures:
  - **continue**: Continues the session
  - **retry-and-terminate**: First retries, if it fails then terminates the session
  - **terminate**: Terminates the session

---

**Usage**

Use this command to configure error handling for Diameter EAP, EAP-termination, and authorization requests. Specific actions (continue, retry-and-terminate, or terminate) can be associated with each possible result-code. Ranges of result codes can be defined with the same action, or actions can be specific on a per-result code basis.

**Example**

The following commands configure result codes 5001, 5002, 5004, and 5005 to use *action continue* and result code 5003 to use *action terminate*:

```plaintext
diameter authentication failure-handling eap-request result-code 5002 to 5005 action continue

diameter authentication failure-handling eap-request result-code 5003 action terminate
```
diameter dictionary

This command is deprecated and is replaced by the diameter accounting dictionary and diameter authentication dictionary commands. See diameter accounting and diameter authentication commands respectively.
diameter endpoint

This command enables the creation, configuration or deletion of a Diameter endpoint.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration
`configure > context context_name`

Entering the above command sequence results in the following prompt:
`[context_name]host_name(config-ctx)#`

**Syntax**

```
[ no ] diameter endpoint endpoint_name [ -noconfirm ]
```

- **no**
  Removes the specified Diameter endpoint.

- **endpoint_name**
  Specifies name of the Diameter endpoint as an alphanumeric string of 1 through 63 characters that should be unique within the system.
  If the named endpoint does not exist, it is created, and the CLI mode changes to the Diameter Endpoint Configuration Mode wherein the endpoint can be configured.
  If the named endpoint already exists, the CLI mode changes to the Diameter Endpoint Configuration Mode wherein the endpoint can be reconfigured.

- **-noconfirm**
  Executes the command without any additional prompt and confirmation from the user.

**Usage**

Use this command to create/configure/delete a Diameter origin endpoint.

Entering this command results in the following prompt:
`[context_name]host_name(config-ctx)#`

Diameter origin endpoint configuration commands are described in the *Diameter Endpoint Configuration Mode Commands* chapter.

**Example**

The following command changes to the Diameter Endpoint Configuration CLI mode for Diameter origin endpoint named `test13`:

```
diameter endpoint test13
```
diameter sctp

This command configures Diameter SCTP parameters for all Diameter endpoints within the context. In 12.2 and later releases, this command is obsolete and replaced with `associate sctp-parameters-template` command in the Diameter Endpoint Configuration Mode.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration

`configure > context context_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

Syntax

```
diameter sctp { hearbeat-interval interval | path max-retransmissions retransmissions }
default diameter sctp { hearbeat-interval | path max-retransmissions }
```

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Configures this command with the default settings.</td>
</tr>
<tr>
<td><em>heartbeat-interval</em></td>
<td>Sets the heartbeat interval to the default value.</td>
</tr>
<tr>
<td><em>path max-retransmissions</em></td>
<td>Sets the SCTP path maximum retransmissions to the default value.</td>
</tr>
</tbody>
</table>

```
heartbeat-interval interval
```

Specifies the time interval between heartbeat chunks sent to a destination transport address in seconds. `interval` must be an integer from 1 through 255.

Default: 30 seconds

```
path max-retransmissions retransmissions
```

Specifies the maximum number of consecutive retransmissions over a destination transport address of a peer endpoint before it is marked as inactive.

`retransmissions` must be an integer from 1 through 10.

Default: 10

Usage

Use this command to configure Diameter SCTP parameters for all Diameter endpoints within the context.

Example

The following command configures the heartbeat interval to 60 seconds:

```
diameter sctp hearbeat-interval 60
```
The following command configures the maximum number of consecutive retransmissions to 6, after which the endpoint is marked as inactive:

```
diameter sctp path max-retransmissions 6
```
**diameter origin**

This command is deprecated and is replaced by the `diameter endpoint` command.
**dns-client**

Creates a DNS client and/or enters the DNS Client Configuration Mode.

**Product**
- ePDG
- MME
- P-GW
- SAEGW
- SCM
- SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration

```
configure > context context_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]hostname(config-dns-client)#
```

**Syntax**

```
[ no ] dns-client name [ -noconfirm ]
```

- **no**
  Removes the specified DNS client from the context.

- **dns-client name**
  Specifies a name for the DNS client as an alphanumeric string of 1 through 63 characters.

**Usage**

Use this command to create a new DNS client and enter the DNS Client Configuration Mode or enter the mode for an existing client.

Entering this command results in the following prompt:

```
[context_name]hostname(config-dns-client)#
```

DNS Client Configuration Mode commands are defined in the *DNS Client Configuration Mode Commands* chapter.

**Example**

The following command enters the DNS Client Configuration Mode for a DNS client named *dns1*:

```
dns-client dns1
```
domain

Configures a domain alias for the current context.

Product
HA
PDSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration
configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

domain [ * ]domain_name [ default subscriber subscriber_template_name ]

no domain [ * ]domain_name

Indicates the domain specified is to be removed as an alias to the current context.

[ * ]domain_name

domain_name specifies the domain alias to create/remove from the current context. If the domain portion of a subscribers user name matches this value, the current context is used for that subscriber.
domain_name must be an alphanumeric string of 1 through 79 characters. The domain name can contain all special characters, however note that the character * (wildcard character) is only allowed at the beginning of the domain name.
If the domain name is prefixed with * (wildcard character), and an exact match is not found for the domain portion of a subscribers username, subdomains of the domain name are matched. For example, if the domain portion of a subscriber’s user name is abc.xyz.com and you use the domain command domain *xyz.com it matches. But if you do not use the wildcard (domain xyz.com) it does not match.

Important: The domain alias specified must not conflict with the name of any existing context or domain names.

default subscriber subscriber_template_name

Specifies the name of the subscriber template to apply to subscribers using this domain alias.
subscriber_template_name must be an alphanumeric string of 1 through 127 characters. If this keyword is not specified the default subscriber configuration in the current context is used.
Usage
Use this command to configure a domain alias when a single context may be used to support multiple domains via aliasing.

Example

    domain sampleDomain.net

    no domain sampleDomain.net
Chapter 52
Context Configuration Mode Commands E-H

This section includes the commands `edr-module active-charging-service` through `hss-peer-service`.

Mode

Exec > Global Configuration > Context Configuration

`configure > context context_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

---

**Important**: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
**eap-profile**

Creates a new, or specifies an existing, Extensible Authentication Protocol (EAP) profile and enters the EAP Configuration Mode.

**Product**

- ASN-GW
- ePDG
- PDIF

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration

```
configure > context context_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
[ no ] eap-profile name
```

`name`

Specifies the name of a new or existing EAP profile as an alphanumeric string of 1 through 256 characters.

**Usage**

Use this command to create a new or enter an existing EAP profile. Entering this command results in the following prompt:

```
[context_name]host_name(config-ctx-eap-profile)#
```

EAP Configuration Mode commands are defined in the *EAP Configuration Mode Commands* chapter.

**Example**

The following command configures an EAP profile called *eap1* and enters the EAP Configuration Mode:

```
eap-profile eap1
```
**edr-module active-charging-service**

Enables the creation, configuration, or deletion of the Event Data Record (EDR) module for this context. In releases prior to 15.0, the SGSN re-used the existing “EDR” module for generating event logs which is primarily used for charging records. But from release 15.0 onwards, the session-event module is used by SGSN for event logging. For more information see the `session-event-module` command.

**Product**
- ACS
- GGSN
- HA
- LNS
- PDSN
- SGSN

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration > Context Configuration
- `configure > context context_name`

Entering the above command sequence results in the following prompt:

```
[context_name]hostname(config-ctx)#
```

**Usage**

Use this command to create the EDR module for the context, and configure the EDR module for active charging service records. You must be in a non-local context when specifying this command, and you must use the same context when specifying the UDR module command.

If this CLI command is configured without the `charging` or `reporting` keywords, by default the EDR module is enabled for charging EDRs.

On entering the command with the `charging` keyword or without any keywords, the CLI prompt changes to:

```
[context_name]hostname(config-edr)#
```

On entering the command with the `reporting` keyword, the CLI prompt changes to:
Example

The following command creates the EDR module for the context for charging EDRs, and enters the EDR Module Configuration Mode:

```
edr-module active-charging-service
```
egtp-service

Creates an eGTP service or specifies an existing eGTP service and enters the eGTP Service Configuration Mode for the current context. On an S4-SGSN, creating and configuring the eGTP service is required for the S4-SGSN to communicate with the S-GW via the S4 interface.

Product
MME
P-GW
SAEGW
SGSN
S-GW

Important: Currently the SGSN is not supported on the ASR 5500 platform.

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration
configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

[ no ] egtp-service service_name [ -noconfirm ]

egtp-service service_name

Specifies the name of the eGTP service as an alphanumeric string of 1 through 63 characters. If service_name does not refer to an existing service, the new service is created if resources allow.

Important: Service names must be unique across all contexts within a chassis.

-noconfirm
Executes the command without any additional prompt and confirmation from the user.

no egtp-service service_name
Removes the specified eGTP service from the context.

Usage
Enter the eGTP Service Configuration Mode for an existing service or for a newly defined service. This command is also used to remove an existing service. A maximum of 256 services (regardless of type) can be configured per system.
Caution: Large numbers of services greatly increase the complexity of management and may impact overall system performance (for example, resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Entering this command results in the following prompt:

```
[context_name]hostname(config-egtp-service)#
```

eGTP Service Configuration Mode commands are defined in the eGTP Service Configuration Mode Commands chapter.

Use this command when configuring the following GTP SAE components: MME, P-GW, and S-GW. Also use this command when configuring an S4-SGSN. Once the eGTP service has been created on the S4-SGSN, the eGTP service must be configured using the `gtpc, validation-mode` and `interface-type` commands in eGTP Service Configuration Mode. Once the service is created and configured, it then must be associated with the 2G and/or 3G services configured on the S4-SGSN using the `associate` command in Call Control Profile Configuration Mode.

Example

The following command enters the existing eGTP Service Configuration Mode (or creates it if it does not already exist) for the service named `egtp-service1`:

```
egtp-service egtp-service1
```

The following command will remove `egtp-service1` from the system:

```
no egtp-service egtp-service1
```
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
epdg-service

Creates Evolved Packet Data GateWay service and enters EPDG service configuration mode.

Product
ACS
ePDG
GGSN
HA
LNS
PDSN
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration
configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

[ no ] epdg-service name [ -noconfirm ]

no
Indicates the evolved packet data gateway service specified is to be removed.

name
Specifies the name of the ePDG service to configure as an alphanumeric string of 1 through 63 characters. If name does not refer to an existing service, the new service is created if resources allow.

**Important:** Service names must be unique across all contexts within a chassis.

-noconfirm
Executes the command without any additional prompt and confirmation from the user.

Usage
Enter the ePDG Service Configuration Mode for an existing service or for a newly defined service. This command is also used to remove an existing service.

Example
The following command will enter the ePDG Service Configuration Mode creating the service
sampleService, if necessary.

```
epdg-service sampleService
```

The following command will remove sampleService as being a defined ePDG service.

```
no epdg-service sampleService
```
event-notif-endpoint

Enables creation, configuration or deletion of an Event Notification collection server endpoint.

Product
IPCF

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration
configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

[ no ] event-notif-endpoint en_node_name

no

Removes the specified Event Notification collection server endpoint.

en_node_name

Specifies name of the Event Notification collection server endpoint as an alphanumeric string of 1 through 31 characters.
If the named endpoint does not exist, it is created, and the CLI mode changes to the Event Notification Interface Endpoint Configuration Mode wherein the endpoint can be configured.
If the named endpoint already exists, the CLI mode changes to the Event Notification Interface Endpoint Configuration Mode wherein the endpoint can be reconfigured.

Usage

Use this command to create/configure/delete an Event Notification collection server endpoint.
Only 1 Event Notification interface across a chassis can be configured on a system.
Entering this command results in the following prompt:

[context_name]host_name(config-ntfyntf-endpoint)#

The commands configured in this mode are defined in the Event Notification Interface Endpoint Configuration Mode Commands chapter of Command Line Interface Reference.

Caution: This is a critical configuration. The PCC Event notification can not be collected on a server without this configuration. Any change to this configuration would lead to the loss of event notifications from PCC service on IPCF node.

Example

The following command creates an Event Notification Interface Endpoint named event_intfc_3:
event-notif-endpoint event_intfc_3
**exit**

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Use this command to return to the parent configuration mode.
external-inline-server

This is a restricted command.
fa-service

Creates or deletes a foreign agent (FA) service or specifies an existing FA service for which to enter the FA Service Configuration Mode for the current context.

**Product**
- ASN-GW
- PDSN
- FA

**Privilege**
- Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration

```
configure > context context_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
[ no ] fa-service name [ -noconfirm ]
```

- `no`
  Indicates the foreign agent service specified is to be removed.

- `name`
  Specifies the name of the FA service to configure as an alphanumeric string of 1 through 63 characters. If `name` does not refer to an existing service, the new service is created if resources allow.

<table>
<thead>
<tr>
<th>Important:</th>
<th>Service names must be unique across all contexts within a chassis.</th>
</tr>
</thead>
</table>

- `-noconfirm`
  Executes the command without any additional prompt and confirmation from the user.

**Usage**
Enter the FA Service Configuration Mode for an existing service or for a newly defined service. This command is also used to remove an existing service. A maximum of 256 services (regardless of type) can be configured per system.

| Caution: | Large numbers of services greatly increase the complexity of management and may impact overall system performance (i.e. resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information. |
Example

The following command will enter the FA Service Configuration Mode creating the service `sampleService`, if necessary.

```
fa-service sampleService
```

The following command will remove `sampleService` as being a defined FA service.

```
no fa-service sampleService
```
firewall max-associations

This command is obsolete.
fng-service

Creates a new, or specifies an existing FNG service and enters the FNG Service Configuration Mode. A maximum of 16 FNG services can be created. This limit applies per ASR 5000 chassis and per context.

Product
FNG

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration
configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

fng-service name [ -noconfirm ]

no fng-service name

fng-service name

Specifies the name of a new or existing FNG service as an alphanumeric string of 1 through 63 characters that must be unique across all FNG services within the same context and across all contexts.

Important: Service names must be unique across all contexts within a chassis.

no fng-service name

Deletes the specified FNG service.

Usage
Use this command in Context Configuration Mode to create a new FNG service or modify an existing one. Executing this command enters the FNG Service Configuration Mode.

Example
The following command configures an FNG service named fmg1 and enters the FNG Service Configuration Mode:

fng-service fmg1


**ggsn-service**

Creates or deletes a Gateway GPRS Support Node (GGSN) service and enters the GGSN Service Configuration Mode within the current context to configure it.

**Product**

GGSN

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration

```
configure > context context_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
ggsn-service svc_name [ -noconfirm ]
```

```
o ggsn-service svc_name
```

`no`

Deletes a previously configured GGSN service.

```
svc_name
```

Specifies the name of the GGSN service to create/configure as an alphanumeric string of 1 through 63 characters that is case sensitive.

**Important:** Service names must be unique across all contexts within a chassis.

```
-noconfirm
```

Executes the command without any additional prompt and confirmation from the user.

**Usage**

Services are configured within a context and enable certain functionality. This command creates and allows the configuration of services enabling the system to function as a GGSN in a GPRS or UMTS network. This command is also used to remove previously configured GGSN services.

A maximum of 256 services (regardless of type) can be configured per system.

**Caution:** Large numbers of services greatly increase the complexity of management and may impact overall system performance (i.e. resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

**Example**

`Cisco ASR 5x00 Command Line Interface Reference`
The following command creates a GGSN service named \textit{ggsn1}:

\texttt{ggsn-service ggsn1}
gprs-service

Creates a GPRS service instance and enters the GPRS Service Configuration Mode. This mode configures all of the parameters specific to the operation of an SGSN in a GPRS network.

Important: For details about the commands and parameters for this mode, check the GPRS Service Configuration Mode chapter.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration

configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

\texttt{gprs-service srvc\_name \ [\ -noconfirm \]}

\texttt{no gprs-service srvc\_name}

\texttt{no}

Removes the configuration for the specified GPRS service from the configuration for the current context.

\texttt{srvc\_name}

Specifies the name of the GPRS service as a unique alphanumeric string of 1 through 63 characters.

Important: Service names must be unique across all contexts within a chassis.

\texttt{-noconfirm}

Executes the command without any additional prompt and confirmation from the user.

Usage

Use this command to create or remove a GPRS service. Entering this command will move the system to the GPRS Service Configuration Mode and change the prompt to:

[context_name]host_name(config-gprs-service)#

Example

The following command creates an GPRS service named \textit{gprs1}:
gprs-service gprsl

The following command removes the GPRS service named gprsl:

   no gprs-service gprsl
gs-service

Creates a Gs service instance and enters the Gs Service Configuration Mode. This mode configures the parameters specific to the Gs interface between the SGSN and the MSC/VLR.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration
configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

gs-service svc_name [ -noconfirm ]

no gs-service svc_name

- Remove the configured Gs service from the current context.

svc_name

Specifies the Gs service as a unique alphanumeric string of 1 through 63 characters.

**Important:** Service names must be unique across all contexts within a chassis.

- **noconfirm**

  Executes the command without any additional prompt and confirmation from the user.

Usage

Use this command to create, edit, or remove a Gs service.

A maximum of 32 Gs service can be configured in one context/system. This limit is subject to maximum of 256 services (regardless of type) can be configured per system.

**Important:** For details about the commands and parameters for this mode, refer Gs Service Configuration Mode chapter.

Example

The following command creates an Gs service named gsl:

```
gs-service gsl
```
The following command removes the Gs service named \textit{gs1}:

\begin{verbatim}
no gs-service gs1
\end{verbatim}
**gtpc overload-protection egress**

Configures the over-load protection of GGSN/PGW by throttling outgoing GTPv1 and GTPv2 control messages over Gn/Gp(GTPv1) or S5/S8 (GTPv2) interface using rate-limiting-function (RLF) template for services configured in a context.

**Product**
GGSN
P-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration
configure > context context_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cxt)#
```

**Syntax**

```
gtpc overload-protection egress [ rlf-template rlf_template_name | throttling-override-policy throttling_override_policy_name ]

[no] gtpc overload-protection egress
```

- **no**
  Disables the GTP Outgoing Control Message Throttling for GGSN/PGW services in this context.

- **rlf-template rlf_template_name**
  It associates the preconfigured Rate-Limiting-Function (RLF) template \texttt{rlf\_template\_name} in Global Configuration mode for throttling the GTP outgoing control messages for the GGSN/PGW services in this context. This is a mandatory parameter to enable throttling.

- **throttling-override-policy throttling_override_policy_name**
  INSERT TEXT HERE.

**Usage**

Use this command to enable the GTP Outgoing Control Message Throttling for GGSN/PGW services configured in the same context. The RLF template associated with this command controls the throttling parameters.

**Example**

The following command enables the outgoing GTP control messages in a context using rlf-template \texttt{gtpc\_1}:

```
gtpc overload-protection egress rlf-template gtpc_1
```
gtpc overload-protection ingress

Configures the over-load protection of GGSN/PGW by throttling incoming GTPv1 and GTPv2 control messages over Gn/Gp(GTPv1) or S5/S8 (GTPv2) interface with other parameters for services configured in a context.

Product
GGSN
P-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration
configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax


gtpc overload-protection ingress {msg-rate msg_rate} [delay-tolerance dur] [queue-size size]

[no] gtpc overload-protection ingress

no
Disables the GTP incoming control message throttling for GGSN/PGW services in this context.

msg-rate msg_rate
Defines the number of GTP incoming messages that can be processed per second.
msg_rate is an integer between 100 through 12000.

delay-tolerance dur
Defines the maximum number of seconds a incoming GTP message can be queued before it is processed. After exceeding this, the message is dropped.
dur is an integer between 1 through 10.

queue-size size
Defines the maximum size of the queue to be maintained for incoming GTPC messages. If the queue exceeds the defined size size, any new incoming messages will be dropped.
size is an integer between 100 through 10000.

Usage
Use this command to enable the GTP incoming control message throttling for GGSN/PGW services configured in the same context.

Example
The following command enables the incoming GTP control messages in a context using message rate 1000 per second with message queue size 10000 and delay of 1 second:

```
gtpc overload-protection ingress msg-rate 1000 delay-tolerance 1 queue-size 10000
```


**gtpp algorithm**

Configures GTPP routing algorithms for the current context. This command is deprecated but available for backward compatibility.

**Product**

GGSN

P-GW

SAEGW

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration

`configure > context context_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
gtpp algorithm { first-server | round-robin | first-n count }
```

- **first-server**
  
  Specifies that accounting data is sent to the first available charging gateway function (CGF) based upon the relative priority of each configured CGF. Default: Enabled

- **round-robin**
  
  Specifies that accounting data is transmitted in a circular queue fashion such that data is sent to the highest priority CGF first, then to the next available CGF of the highest priority, and so on. Ultimately, the queue returns to the CGF with the highest configured priority. Default: Disabled

- **first-n count**
  
  Specifies that the AGW must send accounting data to `count` (more than one) CGFs based on their priority. Response from any one of the `count` CGFs would suffice to proceed with the call. The full set of accounting data is sent to each of the `count` CGFs.
  
  `count` is the number of CGFs to which accounting data will be sent, and must be an integer from 2 through 65535. Default: 1 (Disabled)

**Usage**

Use this command to control how G-CDR/P-CDR accounting data is routed among the configured CGFs.

**Example**

The following command configures the system to use the round-robin algorithm when transmitting G-CDR/P-CDR accounting data:

```
gtpp algorithm round-robin
```


**gtpp attribute**

Allows the specification of the optional attributes to be present in the Call Detail Records (CDRs) that the GPRS/PDN/UMTS access gateway generates. It also defines that how the information is presented in CDRs by encoding the attribute field values.

**Product**

GGSN
SGSN
P-GW
SAEGW

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration

```bash
configure > context context_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```bash
gtpp attribute [ apn-ambr [ include-for-all-bearers | include-for-default-bearer | include-for-non-gbr-bearers ] | apn-ni | apn-selection-mode | charging-characteristic-selection-mode | camel-info | cell-plmn-id | diagnostics | duration-ms | dynamic-flag | dynamic-flag-extension | furnish-charging-information | imei | imsi-unauthenticated-flag | local-record-sequence-number | losdv | ms-timezone | misdn | node-id | node-id-suffix STRING | pdn-connection-id | pdp-address | pdp-type | pgw-plmn-id | plmn-id | rat | recordextension | record-extensions rat | served-mna | served-pdp-pdn-address-extension | served-pdp-pdn-address-prefix-length | sgsn-change | sms { destination-number | recording-entity | service-centre } | start-time | stop-time | uli | user-csg-information } +

default gtpp attribute [ apn-ambr [ include-for-all-bearers | include-for-default-bearer | include-for-non-gbr-bearers ] | apn-ni | apn-selection-mode | charging-characteristic-selection-mode | cell-plmn-id | diagnostics | duration-ms | dynamic-flag | dynamic-flag-extension | furnish-charging-information | imei | imsi-unauthenticated-flag | local-record-sequence-number | losdv | ms-timezone | misdn | node-id | pdn-connection-id | pdp-address | pdp-type | pgw-plmn-id | plmn-id | rat | recordextension | record-extensions rat | served-mna | served-pdp-pdn-address-extension | served-pdp-pdn-address-prefix-length | sgsn-change | sms { destination-number | recording-entity | service-centre } | start-time | stop-time | uli | user-csg-information }

no gtpp attribute [ apn-ambr [ include-for-all-bearers | include-for-default-bearer | include-for-non-gbr-bearers ] | apn-ni | apn-selection-mode | charging-characteristic-selection-mode | cell-plmn-id | diagnostics | duration-ms | dynamic-flag | dynamic-flag-extension | furnish-charging-information | imei | imsi-unauthenticated-flag | local-record-sequence-number | losdv | ms-timezone | misdn | node-id | pdn-connection-id | pdp-address | pdp-type | pgw-plmn-id | plmn-id | rat | recordextension | record-
```
extensions rat | served-mnai | served-pdp-pdn-address-extension | served-pdp-pdn-address-prefix-length | sgsn-change | served-mnai | sms { destination-number | recording-entity | service-centre } | start-time | stop-time | uli | user-csg-information |

default
Sets the default GTPP attributes in the generated CDRs. It also sets the default presentation of attribute values in generated CDRs.

no
Removes the configured GTPP attributes from the CDRs.

apn-ambr [ include-for-all-bearers | include-for-default-bearer | include-for-non-gbr-bearers ]
Default: Disabled
This keyword controls the inclusion of the optional field “apn-ambr” in the PGW-CDRs in the custom24 GTPP dictionary.

**Important:** This keyword option will be available only if a valid license is installed. For more information, contact your Cisco account representative.

The APN Aggregate Maximum Bit Rate (AMBR) is a subscription parameter stored per APN. It limits the aggregate bit rate that can be expected to be provided across all non-GBR bearers and across all PDN connections of the same APN. Each of these non-GBR bearers potentially utilize the entire APN AMBR, e.g. when the other non-GBR bearers do not carry any traffic. The APN AMBR is present as part of QoS information.

In 15.0 and later releases, this CLI command should be configured along with the following additional options to support APN-AMBR reporting in SGW-CDRs in all GTPP dictionaries.

- **include-for-all-bearers:** Includes the APN-AMBR information in SGW-CDRs for all bearers (GBR and NON-GBR)
- **include-for-default-bearer:** Includes APN-AMBR information in SGW-CDRs only for default bearer.
- **include-for-non-gbr-bearers:** Includes APN-AMBR information for non-gbr-bearers.

This feature is required to enable post-processing of CDRs to verify MVNO subscribers actual QoS against invoicing systems.

**Important:** This CLI command and the associated options are not available for products other than S-GW and P-GW. The option “non-gbr-bearers-only” is available in S-GW and P-GW but the other options are available in S-GW only.

In the P-GW implementation, if the CLI command “gtpp attribute apn-ambr” is configured, it will be treated as “gtpp attribute apn-ambr non-gbr-bearers-only”. In case of S-GW/P-GW combo if any of the options is configured, it will be considered that the attribute is available.

apn-ni
Default: Enabled
This keyword controls the inclusion of the optional field “APN” in the x-CDRs.
**apn-selection-mode**

Default: Enabled
This keyword controls the inclusion of the optional field “APN Selection Mode” in the x-CDRs.

**camel-info**

SGSN only
Enter this keyword to include CAMEL-specific fields in SGSN CDRs. Default: Disabled

**cell-plmn-id**

SGSN only
Enter this keyword to enable the system to include the Cell PLMN ID field in the M-CDR. Default: Disabled

**charging-characteristic-selection-mode**

Default: Enabled
This keyword controls the inclusion of the optional field “Charging Characteristic Selection Mode” in the x-CDRs.

**diagnostics**

Default: Disabled
Enables the system to include the Diagnostic field in the CDR that is created when PDP contexts are released. The field will include one of the following values:

- **26** - For GGSN: if the GGSN sends “delete PDP context request” for any other reason (e.g., the operator types “clear subscribers” on the GGSN). For SGSN: The SGSN includes this cause code in the S-CDR to indicate that a secondary PDP context activation request or a PDP context modification request has been rejected due to insufficient resources.

- **36** - For GGSN: this cause code is sent in the G-CDR to indicate the PDP context has been deactivated in the GGSN due to the SGSN having sent a “delete PDP context request” to the GGSN. For SGSN, this cause code is used to indicate a regular MS or network-initiated PDP context deactivation.

- **37** - When the network initiates a QoS modification, the SGSN sends in the S-CDR to indicate that the MS initiation deactivate request message has been rejected with QoS not accepted as the cause.

- **38** - If the GGSN sends “delete PDP context request” due to GTP-C/GTP-U echo timeout with SGSN. If the SGSN sends this cause code, it indicates PDP context has been deactivated due to path failure, specifically GTP-C/GTP-U echo timeout.

- **39** - SGSN only - this code indicates the network (GGSN) has requested a PDP context reactivation after a GGSN restart.

- **40** - If the GGSN sends “delete PDP context request” due to receiving a RADIUS Disconnect-Request message.

**duration-ms**

Specifies that the information contained in the mandatory Duration field be reported in milliseconds instead of seconds (as the standards require). Default: Disabled

**dynamic-flag**

Default: Enabled
This keyword controls the inclusion of the optional field “Dynamic Flag” in the x-CDRs.
**dynamic-flag-extension**

Default: Enabled  
This keyword controls the inclusion of the optional field “Dynamic Address Flag Extension” in the x-CDRs.  
This field is seen in the CDR when the IPv4 address is dynamically assigned for a dual PDP context. This extension field is required in the 3GPP Release 10 compliant CDRs so that the Dual Stack Bearer support is available.

**furnish-charging-information**

Default: Disabled  
This keyword controls the inclusion of the optional field “pSFurnishChargingInformation” in the eG-CDRs and PGW-CDRs.

---

**Important:** The Furnish Charging Information (FCI) feature is applicable to all GTPP dictionaries compliant to 3GPP Rel.7 and 3GPP Rel.8 except custom43 dictionary. This keyword option will be available only if a valid license is installed. For more information, contact your Cisco account representative.

PGW-CDR and eG-CDR will contain FCI only if it is enabled at command level, i.e. using the `gtpp attribute furnish-charging-information` command in GTPP Server Group Configuration mode. 
Whenever FCI changes, a new Free-Format-Data (FFD) value is either appended to existing FFD or overwritten on the existing FDD depending on Append-Free-Format-Data (AFFD) flag. CDR is not generated upon FCI change. 
FCI is supported in main CDR as well as in LOSDV. Whenever a trigger (volume, time, RAT, etc.) happens current available FFD at command level is added to the main body of the CDR. The same FFD at command level is added to the main body of the next CDRs until it is not appended or overwritten by next Credit-Control-Answer message at command level. 
In the case of custom43 dictionary, the FCI implementation will be as follows:

- Whenever FCI changes PGW-CDR will generate CDR i.e close old bucket and will have old FCI details in the generated CDR.
- Translation for the PS-Free-Format-Data in CDR will be conversion of hexadecimal values in ASCII format (for numbers 0 to 9) to decimal values as integers.
- PS-Append-Free-Format-Data always OVERWRITE.

---

**imei**

Default: Disabled  
For SGSN: includes the IMEI value in the S-CDR.  
For GGSN: includes the IMEISV value in the G-CDR.

**imsi-unauthenticated-flag**

Default: Enabled  
This keyword controls the inclusion of the optional field “IMSI Unauthenticated Flag” in the x-CDRs.  
When the served IMSI is not authenticated, this field “IMSI Unauthenticated Flag” if configured, will be present in the P-GW CDR record for custom35 dictionary. This field is added per 3GPP TS 32.298 v10.7.

**local-record-sequence-number**

Default: Disabled  
This keyword provides both the local record sequence number and the Node ID. In the x-CDRs, this field indicates the number of CDRs generated by the node and is unique within the session manager.
The Node ID field is included in the x-CDR for any of several reasons, such as when PDP contexts are released or if partial-CDR is generated based on configuration. The field will consist of a AAA Manager identifier automatically appended to the name of the SGSN or GGSN service.

The name of the SGSN or GGSN service may be truncated, because the maximum length of the Node ID field is 20 bytes. Since each AAA Manager generates CDRs independently, this allows the Local Record Sequence Number and Node ID fields to uniquely identify a CDR.

**Important:** If this keyword is enabled and the `gtpp centralized-lrsn-creation` option is enabled with the `gtpp single-source centralized-lrsn` command, then the Node ID format changes as follows: `<1-byte-AAAproxy-restart-counter> <3-byte AAAproxy instance number> <node-id-suffix>`. If `gtpp centralized-lrsn-creation` is not enabled, the node-id format for CDRs generated by Sessmgr is as follows: `<1-byte Sessmgr restart-value> <3-byte Sessmgr instance number> <node-id-suffix>`. If `gtpp centralized-lrsn-creation` is not enabled, the node-id format for CDRs generated by ACSMGRR is as follows: `<1-byte ACSmgr restart-value> <3-byte ACSmgr instance number> <Active charging service-name>`.

---

**losdv**

Default: Enabled

This keyword controls the inclusion of the optional field “List of Service Data” in the x-CDRs.

**ms-timezone**

Default: Enabled

This keyword controls the inclusion of the optional field “MS-Timezone” in the x-CDRs.

**msisdn**

Default: Enabled

This keyword controls the inclusion of the optional field “MSISDN” in the x-CDRs.

**node-id**

Default: Enabled

This keyword controls the inclusion of the optional field “Node ID” in the x-CDRs.

**node-id-suffix**  STRING

Default: Disabled

Specifies the configured Node-ID-Suffix to use in the NodeId field of GTPP CDRs as an alphanumeric string of 1 through 16 characters. Each Session Manager task generates a unique NodeID string per GTPP context.

**Important:** The NodeID field is a printable string of the `ndddSTRING` format: `n`: The first digit is the Sessmgr restart counter having a value between 0 and 7. `ddd`: The number of sessmgr instances. Uses the specified NodeID-suffix in all CDRs. The “Node-ID” field consists of sessMgr Recovery counter (1 digit) `n` + AAA Manager identifier (3 digits) `ddd` + the configured NodeId-suffix (1 to 16 characters) `STRING`. If the centralized LRSN feature is enabled, the “Node-ID” field will consist of only the specified NodeId-suffix (NodeID-prefix is not included). If this option is not configured, then GTPP group name will be used instead (For default GTPP groups, context-name will be used).

**Important:** If this `node-id-suffix` is not configured, the GGSN uses the GTPP context name as the Node-id-suffix (truncated to 16 characters) and the SGSN uses the GTPP group named as the `node-id-suffix`.
pdn-connection-id
Default: Enabled
This keyword controls the inclusion of the optional field “PDN Connection ID” in the x-CDRs.

pdp-address
Default: Enabled
This keyword controls the inclusion of the optional field “PDP Address” in the x-CDRs.

pdp-type
Default: Enabled
This keyword controls the inclusion of the optional field “PDP Type” in the x-CDRs.

pgw-plmn-id
Default: Enabled
This keyword controls the inclusion of the optional field “PGW PLMN-ID” in the x-CDRs.

plmn-id [ unknown-use ]
Default: Enabled
For SGSN, reports the SGSN PLMN Identifier value (the RAI) in the S-CDR provided if the dictionary supports it.
For GGSN, reports the SGSN PLMN Identifier value (the RAI) in the G-CDR if it was originally provided by the SGSN in the GTP create PDP context request. It is omitted if the SGSN does not supply one.
Normally when SGSN PLMN-id information is not available, the attribute sgsnPLMNIdentifier is not included in the CDR. This keyword enables the inclusion of the sgsnPLMNIdentifier with a specific value when the SGSN PLMN-id is not available.
unknown-use hex_num: is a hexadecimal number from 0x0 through 0xFFFFFFFF that identifies a foreign SGSN that has not provided a PLMN-id. For GGSN only.

rat
Default: Enabled
For SGSN: includes the RAT (identifies the radio access technology type) value in the S-CDR.
For GGSN: includes the RAT (identifies the radio access technology type) value in the G-CDR.

recordextension
Default: Disabled
This keyword controls the inclusion of the optional field “RecordExtension” in the x-CDRs.

record-extensions rat
Default: Disabled
Enables network operators and/or manufacturers to add their own recommended extensions to the CDRs according to the standard record definitions from 3GPP TS 32.298 Release 7 or higher.

served-mnai
Default: Disabled
This keyword controls the inclusion of the optional field “Served MNAI” in the x-CDRs.
**served-pdp-pdn-address-extension**

Default: Disabled
In support of IPv4v6 dual-stack PDP address types, this keyword causes the service to include IPv4v6 address information in the CDR. The IPv4 address goes in the Served PDP PDN Address Extension field and the IPv6 address goes in the Served PDP Address or Served PDP PDN Address field.

**Important:** This attribute will not be displayed if the GTPP dictionary is set to custom34.

**served-pdp-pdn-address-prefix-length**

Default: Enabled
In support of IPv6 prefix delegation, this keyword causes the service to include this field “Served PDP PDN Address” in the x-CDRs.
If this field is configured, the servedPDPPDNAddress field will support reporting the IPv6 prefix length as outlined in 3GPP 32.298. The prefix length will only be reported if:
- it is configured
- it is not the default length of 64
- it is an IPv6 or IPv4v6 call

**sgsn-change**

Default: Enabled
This keyword is specific to SGSN and is license restricted.
This keyword controls the inclusion of the S-CDR attribute “SGSN Change” in the S-CDRs. It is enabled by default and the attribute “SGSN Change” is included in the S-CDRs by default.

**sms { destination-number | recording-entity | service-centre }**

This keyword is specific to the SGSN.
Entering this keyword causes the inclusion of an SMS-related field in the SMS-MO-CDR or SMS-MT-CDR.
**destination-number:** Includes the “destinationNumber” field in the SMS-MO-CDR or SMS-MT-CDR.
**recording-entity:** Includes the “recordingEntity” field in the SMS-MO-CDR or SMS-MT-CDR.
**service-centre:** Includes the “serviceCentre” field in the SMS-MO-CDR or SMS-MT-CDR.

**start-time**

Default: Enabled
This keyword controls the inclusion of the optional field “Start-Time” in the x-CDRs.

**stop-time**

Default: Enabled
This keyword controls the inclusion of the optional field “Stop-Time” in the x-CDRs.

**uli**

Default: Enabled
This keyword controls the inclusion of the optional field “User Location Information” in the x-CDRs.

**user-csg-information**

Default: Disabled
This keyword controls the inclusion of the optional field “User CSG Information” in the x-CDRs.

**Important:** Currently, UCI values are only supported for SGW-CDRs. This attribute will not be displayed if the GTPP dictionary is set to custom11, custom34, or custom35.

+ Indicates that this command can be entered multiple times to configure multiple attributes.

**Usage**

Use this command to configure the type of optional information fields to include in generated CDRs (M-CDRs, S-CDRs, S-SMO-CDR, S-SMT-CDR from SGSN and G-CDRs, eG-CDRs from GGSN) by the AGW (SGSN/GGSN/P-GW/SAEGW). In addition, it controls how the information for some of the mandatory fields are reported.

Fields described as optional by the standards but not listed above will always be present in the CDRs, except for Record Extensions (which will never be present).

**Important:** This command can be repeated multiple times with different keywords to configure multiple GTPP attributes.

**Example**

The following command configures the system to present the time provided in the Duration field of the CDR is reported in milliseconds:

```
gtpp attribute duration-ms
```
**gtpp charging-agent**

Configures the IP address and port of the system interface within the current context used to communicate with the Charging Gateway Function (CGF).

**Product**
GGSN
SGSN
P-GW
SAEGW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration

```bash
configure > context context_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```bash
gtpp charging-agent address ip_address [ port port ]
```

```bash
no gtpp charging-agent
```

**no**

Removes a previously configured charging agent address.

```bash
address ip_address
```

Specifies the IP address of the interface configured within the current context that is used to transmit CDR records (G-CDR/eG-CDR/M-CDR/S-CDR) to the CGF. `ip_address` must be entered using IPV4 dotted-decimal notation.

```bash
port port
```

Specifies the Charging Agent UDP port. as an integer from 1 through 65535. If `port` is not defined, IP will take the default port number 49999.

**Important:** Configuring `gtpp charging-agent` on port 3386 may interfere with a `ggsn-service` configured with the same `ip address`.

**Usage**

This command establishes a Ga interface for the system. For GTPP accounting, one or more Ga interfaces must be specified for communication with the CGF. These interfaces must exist in the same context in which GTPP functionality is configured (refer to the `gtpp` commands in this chapter).
This command instructs the system as to what interface to use. The IP address supplied is also the address by which the GSN is known to the CGF. Therefore, the IP address used for the Ga interface could be identical to one bound to a GSN service (a Gn interface).
If no GSN service is configured in the same context as the Ga interface, the address configured by this command is used to receive unsolicited GTPP packets.

Example

The following command configures the system to use the interface with an IP address of 192.168.13.10 as the accounting interface with port 20000 to the CGF:

```bash
gtpp charging-agent address 192.168.13.10 port 20000
```
gtpp data-request sequence-numbers

Configures the range of sequence numbers to be used in the GTPP data record transfer record (DRT). Use this command to set the start value for the sequence number.

Product
GGSN
SGSN
P-GW
SAEGW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration

Syntax
```
gtpp data-request sequence-numbers start { 0 | 1 }
default gtpp data-request sequence-numbers start
```

Usage
When the GGSN/P-GW (SAEGW)/SGSN is configured to send GTPP echo request packets, the SGSN always uses 0 as the sequence number in those packets. Re-using 0 as a sequence number in the DRT packets is allowed by the 3GPP standards; however, this CLI command ensures the possibility of inter-operating with CGFs that can not properly handle the re-use of sequence number0 in the echo request packets.

Example
The following command sets the sequence to start at 1.
```
gtpp data-request sequence-numbers start 1
```
gtpp dead-server suppress-cdrs

Enables or disables CDR archiving when a dead server is detected.

**Important:** This command is customer specific. For more information please contact your local Cisco service representative.

**Product**
- GGSN
- P-GW
- SAEGW

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration > Context Configuration
- `configure > context context_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
[ default | no ] gtpp dead-server suppress-cdrs
```

**default**
Configures the default setting.
Default: Disabled

**no**
Re-enables CDR archiving.

**Usage**

Use this command to enable/disable CDR archiving when a dead server is detected. With this CLI, once a server is detected as down, requests are purged. Also the requests generated for the period when the server is down are purged.
gtpp deadtime

Configures the amount of time to wait before attempting to communicate with a Charging Gateway Function (CGF) that was previously marked as unreachable.

Product

GGSN
P-GW
SAEGW

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > Context Configuration
configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

gtpp deadtime time

default gtpp deadtime

default

Configures this command with the default setting.
Default: 120 seconds

time

Specifies the amount of time (in seconds) that must elapse before the system attempts to communicate with a CGF that was previously unreachable. time is an integer from 1 through 65535.

Usage

If the system is unable to communicate with a configured CGF, after a pre-configured number of failures the system marks the CGF as being down. This command specifies the amount of time that the system waits prior to attempting to communicate with the downed CGF.
Refer to the gtpp detect-dead-server and gtpp max-retries commands for additional information on the process the system uses to mark a CGF as down.

Example

The following command configures the system to wait 60 seconds before attempting to re-communicate with a CGF that was marked as down:

gtpp deadtime 60
**gtpp detect-dead-server**

Configures the number of consecutive communication failures that could occur before the system marks a Charging Gateway Function (CGF) as down.

**Product**
- GGSN
- P-GW
- SAEGW

**Privilege**
- Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration
configure > context context_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
gtpp detect-dead-server consecutive-failures max_number
```

```
default gtpp detect-dead-server consecutive-failures
```

<table>
<thead>
<tr>
<th><strong>default</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Configures this command with the default setting.</td>
</tr>
<tr>
<td>Default: 0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>consecutive-failures max_number</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the number of failures that could occur before marking a CGF as down. max_number is an integer from 0 through 1000.</td>
</tr>
</tbody>
</table>

**Usage**

This command works in conjunction with the **gtpp max-retries** parameter to set a limit to the number of communication failures that can occur with a configured CGF.

The gtpp max-retries parameter limits the number of attempts to communicate with a CGF. Once that limit is reached, the system treats it as a single failure. The gtpp detect-dead-server parameter limits the number of consecutive failures that can occur before the system marks the CGF as down and communicate with the CGF of next highest priority.

If all of the configured CGFs are down, the system ignores the detect-dead-server configuration and attempt to communicate with the highest priority CGF again.

If the system receives a GTPP Node Alive Request, Echo Request, or Echo Response message from a CGF that was previously marked as down, the system immediately treats it as being active.

Refer to the **gtpp max-retries** command for additional information.

**Example**

The following command configures the system to allow 8 consecutive communication failures with a CGF before it marks it as down:
gtpp detect-dead-server consecutive-failures 8
gtpp dictionary

Designates a dictionary used by GTPP for a specific context.

**Product**
- GGSN
- SGSN
- PDG/TTG
- P-GW
- SAEGW
- S-GW

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration > Context Configuration

```
configure > context context_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
gtpp dictionary { custom1 | custom10 | custom11 | custom12 | custom13 | custom14 |
custom15 | custom16 | custom17 | custom18 | custom19 | custom2 | custom20 | custom21 |
custom22 | custom23 | custom24 | custom25 | custom26 | custom27 | custom28 | custom29 |
custom3 | custom30 | custom31 | custom32 | custom33 | custom34 | custom35 | custom36 |
custom37 | custom38 | custom39 | custom4 | custom40 | custom41 | custom42 | custom43 |
custom44 | custom45 | custom46 | custom47 | custom48 | custom49 | custom5 | custom50 |
custom51 | custom52 | custom53 | custom54 | custom55 | custom56 | custom57 | custom58 |
custom59 | custom6 | custom60 | custom7 | custom8 | custom9 | standard }
```

**default gtpp dictionary**

```
default
```

Configures the default dictionary.

```
custom1
```

This is a custom-defined dictionary that conforms to TS 32.015 v 3.6.0 for R99. It supports the encoding of IP addresses in text format for G-CDRs.

```
custom2
```

Custom-defined dictionary.

```
custom3
```

This is a custom-defined dictionary that conforms to TS 32.015 v 3.6.0 for R99 except that it supports the encoding of IP addresses in binary format for G-CDRs.
context4

This is a custom-defined dictionary that conforms to TS 32.015 v 3.6.0 for R99 except that:
- IP addresses are encoded in binary format.
- The Data Record Format Version information element contains 0x1307 instead of 0x1308.
- QoS Requested is not present in the LoTV containers.
- QoS negotiated is added only for the first container and the container after a QoS change.

custom5

Custom-defined dictionary.

custom6

This is a custom-defined dictionary for eG-CDR encoding.

custom7 ... custom30

These custom-defined dictionary have default behavior or “standard” dictionary.

custom31

This is a custom-defined dictionary for S-CDR encoding that is based on 3GPP TS 32.298 v6.4.1 with a special field appended for the PLMN-ID.

custom33

This is a custom-defined dictionary for S-CDR encoding that is based on the 3GPP TS 32.298v6.4.1 with the following exceptions:
- Proprietary PLMN-ID field is present.
- It is a SEQUENCE and not a SET.
- Diagnostics and SGSN-Change fields are not supported.
- Indefinite length encoding is used.
- Booleans are encoded as 0x01 (3GPP it is 0xff).
- IMEISV shall be sent if available else IMEI should be sent.
- Record Sequence Number is Mandatory.
- APN OI and NI part is length encoded.
- Cause for Record closure should be “RAT Change” instead of “intra-SGSNinter-system”.

standard

Default: Enabled
This dictionary conforms to TS 32.215 v 4.6.0 for R4 (and also R5 - extended QoS format).

Usage

Use this command to designate specific dictionary used by GTPP for specific context.
**Important:** Note that the following warning message will be displayed whenever an existing GTPP dictionary is being changed or a new GTPP dictionary is configured irrespective of whether or not the calls are active on the system.

Warning: It is not recommended to change the dictionary when the system has active calls. Are you sure? [Yes|No]: n

**Important:** This change will require user's input on the CLI console for GTPP dictionary configuration / change.

**Example**

The following command configures the system to use *custom3* dictionary to encode IP address in Binary format in G-CDRs:

```
gtp dictionary custom3
```
**gtpp duplicate-hold-time**

Configures the number of minutes to hold on to CDRs that are possibly duplicates while waiting for the primary Charging Gateway Function (CGF) to come back up.

**Product**
- GGSN
- SGSN
- P-GW
- SAEGW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration

```
configure > context context_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
gtpp duplicate-hold-time minutes
```

default gtpp duplicate-hold-time

```
default
Configures this command with the default setting.
Default: 60 minutes
```

```
minutes
Specifies the number of minutes to hold on to CDRs that may be duplicates whenever the primary CGF is down, minutes must be an integer from 1 through 10080.
```

**Usage**

Use this command to configure how long to hold on to CDRs that are possibly duplicates while waiting for the primary CGF to come back up. If the GGSN/P-GW (SAEGW) determines that the primary CGF is down, CDRs that were sent to the primary CGF but not acknowledged are sent by the GSN to the secondary CGF as “possibly duplicates”. When the primary CGF comes back up, the GSN uses GTPP to determine whether the possibly duplicate CDRs were received by the primary CGF. Then the secondary CGF is told whether to release or cancel those CDRs. This command configures how long the system should wait for the primary CGF to come back up. As soon as the configured time expires, the secondary CGF is told to release all of the possibly duplicate CDRs.

**Example**

Use the following command to set the amount of time to hold on to CDRs to 2 hours (120 minutes);

```
gtpp duplicate-hold-time 120
```
gtpp echo-interval

Configures the frequency at which the system sends GTPP echo packets to configured CGFs.

**Product**
- GGSN
- SGSN
- P-GW
- SAEGW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration
```
configure > context context_name
```
Entering the above command sequence results in the following prompt:
```
[context_name]host_name(config-ctx)#
```

**Syntax**
```
gtpp echo-interval time
{ default | no } gtpp echo-interval
```

- **default**
  Configures the default setting for this command,
  Default: 60 seconds

- **no**
  Disables the use of the echo protocol except for the scenarios described in the Usage section for this command.

- **time**
  Specifies the time interval (in seconds) for sending GTPP echo packets as an integer from 60 through 2147483647. Default: 60

**Usage**
The GTPP echo protocol is used by the system to ensure that it can communicate with configured CGFs. The system initiates this protocol for each of the following scenarios:
- Upon system boot
- Upon the configuration of a new CGF server on the system using the `gtpp server` command as described in this chapter
- Upon the execution of the `gtpp test accounting` command as described in the Exec Mode Commands chapter of this reference
Upon the execution of the `gtpp sequence-numbers private-extensions` command as described in this chapter.

The echo-interval command is used in conjunction with the `gtpp max-retries` and `gtpp timeout` commands as described in this chapter.

In addition to receiving an echo response for this echo protocol, if we receive a GTPP Node Alive Request message or a GTPP Echo Request message from a presumed dead CGF server, we will immediately assume the server is active again.

The alive/dead status of the CGFs is used by the AAA Managers to affect the sending of CDRs to the CGFs. If all CGFs are dead, the AAA Managers will still send CDRs, (refer to the `gtpp deadtime` command), albeit at a slower rate than if a CGF were alive. Also, AAA Managers independently determine if CGFs are alive/dead.

**Example**

The following command configures an echo interval of 120 seconds:

```
gtp echo-interval 120
```
gtpp egcdr

Configures the eG-CDR and P-CDR (P-GW CDR) parameters and triggers.

Product
GGSN
P-GW
SAEGW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration

configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax


default gtpp egcdr { closure-reason admin-disconnect | final-record include-content-ids only-with-traffic closing-cause same-in-allpartials | losdv-max-containers | lotdv-max-containers | service-idle-timeout 0 }

no gtpp egcdr { rulebase-max-length | service-data-flow threshold { interval | volume { downlink [ uplink ] | total | uplink [ downlink ] } } }

closure-reason admin-disconnect [ management-intervention | normal-release ]

Controls the configuration of “causeForRecordClosing” in PGW-CDR when a call is cleared from the chassis.
Releases prior to 14.1, when a call is cleared from the chassis the field “causeForRecordClosing” in a PGW-CDR shows “Normal Release”. In 15.0 and later releases, the behavior has changed to comply with the 3GPP specifications. That is, the default “causeForRecordClosing” in PGW-CDR will be “Management Intervention”.

Important: This behavioral change is limited to PGW-CDR Release 8 dictionaries only.

Closing-reason: Configures the record closing reason for PGW-CDR.

management-intervention: Specifies to send Management-Intervention as causeForRecordClosing in PGW-CDRs. By default, Management-Intervention will be sent as the record closure reason for PGW-CDRs.
• **normal-release**: Specifies to send Normal Release as causeForRecordClosing in PGW-CDRs.

```plaintext
final-record [ [ include-content-ids { all | only-with-traffic } ] [ closing-cause { same-in-allpartials | unique } ] ]
```

Enables configuration of the final eG-CDR/P-CDR.
Default: Restores the GTTP eG-CDR/P-CDR final record to the default setting to include content IDs with some data to report are included. Also, sets the closing cause to the default of using the same closing cause for multiple final eG-CDR/P-CDRs.

• **include-content-ids**: Controls which content IDs are being included in the final eG-CDR/P-CDR.
  - **all**: Specifies that all content IDs be included in the final eG-CDR/P-CDR.
  - **only-with-traffic**: Specifies that only content-IDs with traffic be included in the final eG-CDR/P-CDRs.

• **closing-cause**: Configures closing cause for the final eG-CDR/P-CDR.
  - **same-in-all-partials**: Specifies that the same closing cause is to be included for multiple final eG-CDR/P-CDRs
  - **unique**: Specifies that the closing cause for final eG-CDR/P-CDRs is to be unique.

---

`losdv-max-containers max_losdv_containers`

The maximum number of List of Service Data Volume (LoSDV) containers in one eG-CDR/P-CDR.

`max_losdv_containers` must be an integer from 1 through 255.
Default: 10

`lotdv-max-containers max_lotdv_containers`

The maximum number of List of Traffic Data Volume (LoTDV) containers in one eG-CDR/P-CDR.

`max_lotdv_containers` must be an integer from 1 through 8.
Default: 8

`rulebase-max-length rulebase_name_max_length`

Specifies the maximum character length of charging rulebase name in LOSDVs of eG-CDR/P-CDR.

`rulebase_name_max_length` must be an integer from 0 through 63. Zero (0) means the rulebase name is added as-is.
Default: None. That is, full (un-truncated) charging rulebase name will go in LOSDVs of eG-CDR/P-CDR.

---

`service-data-flow threshold { interval interval | volume { downlink bytes [ uplink bytes ] | total bytes | uplink bytes [ downlink bytes ] } }`

Configures the thresholds for closing a service data flow container within an eG-CDR/P-CDR.

• **interval interval**: Specifies the time interval, in seconds, to close the eG-CDR/P-CDR if the minimum time duration thresholds for service data flow containers satisfied in flow-based charging.

  `interval` must be an integer from 60 through 40000000.
Default: Disabled

• **volume { downlink bytes [ uplink bytes ] | total bytes | uplink bytes [ downlink bytes ] }**: Specifies the volume octet counts for the generation of the interim G-CDR/P-CDRs to service data flow container in FBC.

  • **downlink bytes**: specifies the limit for the number of downlink octets after which the eG-CDR/P-CDR is closed.
**Usage**

Use this command to configure individual triggers for eG-CDR/P-CDR generation.

Use the `service-data-flow threshold` option to configure the thresholds for closing a service data flow container within an eG-CDR (eG-CDRs for GGSN and P-CDRs for PGW) during flow-based charging (FBC). A service data flow container has statistics regarding an individual content ID.

Thresholds can be specified for time interval and for data volume, by entering the command twice (once with interval and once with volume). When either configured threshold is reached, the service data flow container will be closed. The volume trigger can be specified for uplink or downlink or the combined total (uplink + downlink) byte thresholds.

When the PDP context is terminated, all service data flow containers will be closed regardless of whether the thresholds have been reached.

An eG-CDR/P-CDR will have at most ten service data flow containers. Multiple eG-CDR/P-CDRs will be created when there are more than ten.

**Example**

Use the following command to set the maximum number of LoSDV containers to 7:

```
gtp egcdr losdv-max-containers 7
```

The following command sets an eG-CDR threshold interval of 6000 seconds:

```
gtp egcdr service-data-flow threshold interval 6000
```
**gtpp error-response**

Configures the response when the system receives an error response after transmitting a DRT (data record transfer) request.

**Product**
- GGSN
- SGSN
- P-GW
- SAEGW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration

```
configure > context context_name
```

Entering the above command sequence results in the following prompt:
```
[context_name]host_name(config-ctx)#
```

**Syntax**
```
gtpp error-response { discard-cdr | retry-request }
default gtpp error-response
```

- **default**
  Configures this command with the default setting.
  Default: *retry-request*

- **discard-cdr**
  Instructs the system to purge the request upon receipt of an error response and not to retry.

- **retry-request**
  Instructs the system to retry sending a DRT after receiving an error response. This is the default behavior.

**Usage**
This command configures the system’s response to receiving an error message after sending a DRT request.

**Example**
```
gtpp error-response discard-cdr
```
gtpp group

Configures GTPP server group in a context for the Charging Gateway Function (CGF) accounting server(s) that the system is to communicate with.

Product

GGSN
SGSN
P-GW
SAEGW

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > Context Configuration
configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

[ no ] gtpp group group_name [ -noconfirm ]

group_name

Specifies the name of GTPP server group that is used for charging and/or accounting in a specific context. group_name must be an alphanumeric string of 1 through 63 character. A maximum of eight GTPP server groups (excluding system created default GTPP server group “default”) can be configured with this command in a context.

no

Removes the previously configured GTPP group within a context. When a GTPP group is removed accounting information is not generated for all calls using that group and all calls associated with that group are dropped. A warning message displays indicating the number of calls that will be dropped.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage

This feature provides the charging gateway function (CGF) accounting server configurable for a group of servers. Instead of having a single list of CGF accounting servers per context, this feature configures multiple GTPP accounting server groups in a context and each server group is consist of list of CGF accounting servers. In case no GTPP server group is configured in a context, a server group named “default” is available and all the CGF servers configured in a specific context for CGF accounting functionality will be part of this “default” server group.
Example

The following command configures a GTPP server group named *star1* for CGF accounting functionality. This server group is available for all subscribers within that context.

```
gtp group star1
```
gtpp max-cdr

Configures the maximum number of charging data records (CDRs) included per packet.

Product

GGSN
P-GW
SAEGW
SGSN

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > Context Configuration

configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

```
gtpp max-cdr max_cdr [ wait-time wait_time ]
default gtpp max-cdr
```

default

Configures this command with the default setting.
Default: One CDR per packet; disables wait-time

max_cdr

Specifies the maximum number of CDRs to be inserted in a single packet as an integer from 1 through 255.
Default: 1

wait-time wait_time

Specifies the number of seconds the system waits for CDRs to be inserted into the packet before sending it.
wait_time must be an integer from 1 through 300. Default: Disabled

Important: If the wait-time expires, the packet is sent as this keyword over-rides max_cdr.

Usage

CDRs are placed into a GTPP packet as the CDRs close. The system stops placing CDRs into a packet when either the maximum max_cdr is met, or the wait-time expires, or the value for the gtpp max-pdu-size command is met.

Example

The following command configures the system to place a maximum of 10 CDRs in a single GTPP packet before transmitting the packet:
gtpp max-cdrrs 10


**gtpp max-pdu-size**

Configures the maximum payload size of a single GTPP packet that could be sent by the system.

**Product**

- GGSN
- P-GW
- SAEGW
- SGSN

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration

```text
configure > context context_name
```

Entering the above command sequence results in the following prompt:

```text
[context_name]host_name(config-ctx)#
```

**Syntax**

```text
  gtpp max-pdu-size pdu_size
  default gtpp max-pdu-size
```

- **default**
  - Configures this command with the default setting.
  - Default: 65400 bytes

- **pdu_size**
  - Specifies the maximum payload size (in octets) of the GTPP packet as an integer from 1024 to 65400. The payload includes the CDR and the GTPP header.

**Caution:** This command is effective only when GTPP single-source is configured, otherwise this command has no effect.

**Usage**

The GTPP packet contains headers (layer 2, IP, UDP, and GTPP) followed by the CDR. Each CDR contains one or more volume containers. If a packet containing one CDR exceeds the configured maximum payload size, the system creates and send the packet containing the one CDR regardless.

The larger the packet data unit (PDU) size allowed, the more volume containers that can be fit into the CDR.

The system performs standard IP fragmentation for packets that exceed the system’s maximum transmission unit (MTU).

**Important:** The maximum size of an IPv4 PDU (including the IPv4 and subsequent headers) is 65,535. However, a slightly smaller limit is imposed by this command because the system’s max-pdu-size doesn't include the IPv4 and...
UDP headers, and because the system may need to encapsulate GTPP packets in a different/larger IP packet (for sending to a backup device).

Example

The following command configures a maximum PDU size of 2048 octets:

```
gtp max-pdu-size 2048
```
**gtpp max-retries**

Configures the maximum number of times the system attempts to communicate with an unresponsive Charging Gateway Function (CGF).

**Product**

- GGSN
- P-GW
- SAEGW
- SGSN

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration

`configure > context context_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
gtpp max-retries max_attempts

default gtpp max-retries
```

---

**default**

Configures this command with the default setting.

Default: 4

---

**max_attempts**

Specifies the number of times the system attempts to communicate with a CGF that is not responding.

`max_attempts` is an integer from 1 through 15.

---

**Usage**

This command works in conjunction with the `gtpp detect-dead-server` and `gtpp timeout` parameters to set a limit to the number of communication failures that can occur with a configured CGF.

When the value specified by this parameter is met, a failure is logged. The `gtpp detect-dead-server` parameter specifies the number of consecutive failures that could occur before the server is marked as down.

In addition, the `gtpp timeout` command controls the amount of time between re-tries.

If the value for the max-retries is met, the system begins storing CDRs in Random Access Memory (RAM). The system allocates memory as a buffer, enough to store one million CDRs for a fully loaded chassis (a maximum of one outstanding CDR per PDP context). Archived CDRs are re-transmitted to the CGF until they are acknowledged or the system’s memory buffer is exceeded.

Refer to the `gtpp detect-dead-server` and `gtpp timeout` commands for additional information.

**Example**

The following command configures the maximum number of re-tries to be 8:

```
gtpp max-retries 8
```
gtpp max-retries 8
gtpp node-id

Configures the GTPP Node ID for all CDRs.

Product
GGSN
P-GW
SAEGW
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration
configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

```
gtpp node-id node_id
no gtpp node-id
```

Usage

Use this command to configure the GTPP Node ID for all CDRs.

Example

The following command configures the GTPP Node ID as test123:

```
gtpp node-id test123
```
gtpp redirection-allowed

Configures the system to allow or disallow the redirection of CDRs when the primary Charging Gateway Function (CGF) is unavailable.

Product

GGSN
P-GW
SAEGW
SGSN

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > Context Configuration

configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

gtpp redirection-allowed

{ default | no } gtpp redirection-allowed

default

Configures this command with the default setting. Default: Enabled

no

Deletes the command from the configuration.

Usage

This command allows operators to better handle erratic network links, without having to remove the configuration of the backup server(s) via the no gtpp server command. This functionality is enabled by default.

If the no gtpp redirection-allowed command is executed, the system only sends CDRs to the primary CGF. If that CGF goes down, we will buffer the CDRs in memory until the CGF comes back or until the system runs out of buffer memory. In addition, if the primary CGF announces its intent to go down (with a GTPP Redirection Request message), the system responds to that request with an error response.
gtpp redirection-disallowed

This command has been obsoleted and is replaced by the `gtpp redirection-allowed` command.
**gtpp server**

Configures the Charging Gateway Function (CGF) accounting server(s) with which the system will communicate.

**Product**
- GGSN
- P-GW
- SAEGW
- SGSN

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration > Context Configuration
- `configure > context context_name`

Entering the above command sequence results in the following prompt:

```
[context_name] host_name(config-ctx) #
```

**Syntax**

```
gtpp server ip_address [ max max_messages ] [ priority priority ] [ port port ] [ node-alive { enable | disable } ] [ -noconfirm ]
```

```
no gtpp server ip_address
```

- **no**
  - Deletes a previously configured CGF.

- **ip_address**
  - Specifies the IP address of the CGF in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

- **max max_messages**
  - Default: 256
  - Specifies the maximum number of outstanding or unacknowledged GTPP packets (from any one AAA Manager task) allowed for this CGF before the system begins buffering the packets.
  - `max_messages` can be configured as an integer from 1 through 256.

- **priority priority**
  - Default: 1000
  - Specifies the relative priority of this CGF. When multiple CGFs are configured, the priority is used to determine which CGF server to send accounting data to.
  - `priority` can be configured as an integer from 1 through 1000. When configuring two or more servers with the same priority you will be asked to confirm that you want to do this. If you use the `-noconfirm` option, you are not asked for confirmation and multiple servers could be assigned the same priority.
**port** *port*
Default: 3386
Specifies the port the CGF is using. *port* can be configured as an integer from 1 through 65535. Default value for port is 3286.

**Important:** The *port* keyword option has been modified from *udp-port* to make it a generic command. The *udp-port* keyword can still be used, however, it will be in concealed mode and will not be shown in auto-complete or help for the command.

**node-alive** { enable | disable }
Default: Disable.
This optional keyword allows operator to enable/disable GSN to send Node Alive Request to GTPP Server (i.e. CGF). This configuration can be done per GTPP Server basis.

**-noconfirm**
Executes the command without any additional prompt and confirmation from the user.

**Usage**
Use this command to configure the CGF(s) that the system sends CDR accounting data to. Multiple CGFs can be configured using multiple instances of this command. Up to 12 CGF scan be configured per system context. Each configured CGF can be assigned a priority. The priority is used to determine which server to use for any given subscriber based on the routing algorithm that has been implemented. A CGF with a priority of “1” has the highest priority.

**Important:** The configuration of multiple CGFs with the same IP address but different port numbers is not supported.

Each CGF can also be configured with the maximum allowable number of unacknowledged GTPP packets. Since multiple AAA Manager tasks could be communicating with the same CGF, the maximum is based on any one AAA Manager instance. If the maximum is reached, the system buffers the packets Random Access Memory (RAM). The system allocates memory as a buffer, enough to store one million CDRs for a fully loaded chassis (a maximum of one outstanding CDR per PDP context).

**Example**
The following command configures a CGF with an IP address of 192.168.2.2 and a priority of 5.

```
gtpp server 192.168.2.2 priority 5
```

The following command deletes a previously configured CGF with an IP address of 100.10.35.7:

```
no gtpp server 100.10.35.7
```
gtpp source-port-validation

Toggles port checking for node alive/echo/redirection requests from the CGF.

**Product**

GGSN
P-GW
SAEGW

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration

`configure > context context_name`

Entering the above command sequence results in the following prompt:

```
[context_name] host_name(config-ctx)#
```

**Syntax**

```
[ default | no ] gtpp source-port-validation
```

- **default**
  
  Configures this command with the default setting.
  
  Default: Enabled

- **no**
  
  Disables CGF port checking. Only the IP address will be used to verify CGF requests.

**Usage**

This command is for enabling or disabling port checking on node alive/echo/redirection requests from the CGF. If the CGF sends messages on a non-standard port, it may be necessary to disable port checking in order to receive CGF requests. On the default setting, both IP and port are checked.

**Example**

The following command disables port checking for CGF requests:

```
no gtpp source-port-validation
```
**gtpp storage-server**

Configures information for the GTPP back-up storage server.

**Product**
GGSN
P-GW
SAEGW
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration
configure > context context_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
[ no ] gtpp storage-server ip-address port port-num
```

- **no**
  Removes a previously configured back-up storage server.

- **ip-address**
  Specifies the IP address of the back-up storage server expressed in IPv4 dotted-decimal notation.

- **port port-num**
  Specifies the UDP port number over which the GSN communicates with the back-up storage server. Default: 3386

**Usage**

This command configures the information for the server to which GTPP packets are to be backed up to if all the CGFs are unreachable.
One backup storage server can be configured per system context.

**Important:** This command only takes affect if `gtpp single-source` in the Global Configuration Mode is also configured. Additionally, this command is customer specific. Please contact your local sales representative for additional information.

**Example**

The following command configures a back-up server with an IP address of 192.168.1.2:

```
gtpp storage-server 192.168.1.2
```
gtpp storage-server local file

Configures the parameters for GTPP files stored locally on the GTPP storage server. This command is available for the ASR 5000 platform only.

Product
GGSN
P-GW
SAEGW
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration

configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

gtpp storage-server local file { compression { gzip | none } | format { custom1 | custom2 | custom3 | custom4 | custom5 | custom6 | custom7 | custom8 } | name { format string [ max-file-seq-num seq_number ] | prefix prefix } | purge-processed-files { file-name-pattern file_pattern | purge-interval purge_dur } | push { encrypted-url url | url url } [ encrypted-secondary-url url | secondary-url url ] [ via-local-context ] | rotation { cdr-count count | time-interval time [ force-file-rotation ] | volume mb size } | start-file-seq-num seq_num { recover-file-seq-num }

default gtpp storage-server local file { compression | format | name { format | prefix } | purge-processed-files | rotation { cdr-count | time-interval | volume } | start-file-seq-num }

no gtpp storage-server local file { purge-processed-files | push | rotation { cdr-count | time-interval } }

default

Configures default setting for the specified parameter.

no

Removes a previously configured parameters for local storage of CDR files on HDD on SMC card.

compression { gzip | none }

Configures the type of compression to be used on the files stored locally.

• gzip: Enables Gzip file compression.
• none: Disables Gzip file compression -this is the default value.
Default: Disabled

format { custom-n }

Configures the file format to be used to format files to be stored locally.

- custom1: File format custom1—this is the default value.
- custom2: File format custom2.
- custom3: File format custom3.
- custom5: File format custom5.
- custom6: File format custom6 with a block size of 8K for CDR files.
- custom7: File format custom7 is a customer specific CDR file format.
- custom8: File format custom8 is a customer specific CDR file format. It uses node-id-
  suffix_date_time_fixed-length-seq-num format for file naming.

Default: custom1

name { format | prefix prefix }

Allows the format of the CDR filenames to be configured independently from the file format so that the name format contains the file name with conversion specifications.

prefix—Enter an alphanumeric string of 1 through 127 characters. The string must begin with the % (percent sign).

- %y: = year as a decimal number without century (range 00 to 99).
- %Y: year as a decimal number with century.
- %m: month as a decimal number (range 01 to 12).
- %d: day of the month as a decimal number (range 01 to 31).
- %H: hour as a decimal number 24-hour format (range 00 to 23).
- %h: hour as a decimal number 12-hour format (range 01 to 12).
- %M: minute as a decimal number (range 00 to 59).
- %S: second as a decimal number (range 00 to 60). (The range is up to 60 to allow occasional leap seconds.)
- %Q: File sequence number. Field width may be specified between the % and the Q. If the natural size of the field is smaller than this width, then the result string is padded (on the left) to the specified width with 0s
- %N: No of CDRs in the file. Field width may be specified between the % and the N. If the natural size of the field is smaller than this width, then the result string is padded (on the left) to the specified width with 0s
- max-file-seq-no: This can be configured optionally. It indicates the maximum value of sequence number in file name (starts from 1). Once the configured max-file-seq-no limit is reached, the sequence number will restart from 1. If no max-file-seq-no is specified then file sequence number ranges from 1 – 4294967295.

By default the above keyword is not configured (default gtp storage-server local filename format). In which case the CDR filenames are generated based on the file format as before (maintains backward compatibility).

purge-processed-files [ file-name-pattern file_pattern | purge-interval purge_dur ]

Enables the GSN to periodically (every 4 minutes) delete locally processed (*.p) CDR files from the HDD on the SMC card. Default: Disabled
This keyword also deletes the processed push files (tx.*, under $CDR_PATH/TX/tx.*) a well when purging is enabled instead of "*.p:*.P".

**Important:** This option is available only when GTPP server storage mode is configured for local storage of CDRs with the `gtpp storage-server mode local` command.

Optional keyword `file-name-pattern file_pattern` provides an option for user to control the pattern of files. *file_pattern* must be mentioned in "*.p:*.P:tx.*" format in a string of size 1 through 127, which is also the default format. Wildcards * and: (synonymous to |) are allowed.

Optional keyword `purge-interval purge_dur` provides an option for user to control the purge interval duration (in minutes). *purge_dur* must be an integer from 1 through 259200. Default value 60.

```
push { encrypted-url encrypted_url | url url } [ encrypted-secondary-url encrypted_url | secondary-url url ] [ via-local-context ]
```

Enables push method to transfer local CDR files to remote system.

- `encrypted-url`: Defines use of an encrypted url.
  - *encrypted_url* must be an alphanumeric string of 1 through 8192 characters in SFTP format.
- `url`: Location where the CDR files are to be transferred.
  - *url* must be an alphanumeric string of 1 through 1024 characters in the format: `scheme://user:password@host`
  - *encrypted_url* must be an alphanumeric string of 1 through 8192 characters in SFTP format.
- `secondary-url`: Secondary location where the CDR files are to be transferred, in case primary is unreachable.
  - *url* must be an alphanumeric string of 1 through 1024 characters in the format: `scheme://user:password@host`

**Important:** When a file transfer to primary fails four times, the transfer of files will automatically be failed over to the secondary server. The transfer will switch back to the original primary after 30 minutes, or if there are four transfer failures to the secondary server.

- `via-local-context`: Pushes the CDR files via SPIO in the local context.
  - Default: Pushes via the group's context.

**Important:** If the push is done through gtpp context, then the push rate is lesser compared to via local context as the HDD is attached to the local context.

```
rotation { cdr-count count | time-interval time | volume mb size }
```

Specifies rotation related configuration for GTPP files stored locally.

- `cdr-count count`: Configures the CDR count for the file rotation as an integer from 1000 through 65000. Default value 10000.
- `time-interval time`: Configures the time interval (in seconds) for file rotation as an integer from 30 through 86400. Default value 3600 (1 hour).
- `volume mb size`: Configure the file volume (in MB) for file rotation. Enter an integer from 2 to 40. This trigger cannot be disabled. Default value is 4MB.
gtpp storage-server local file rotation time-interval 5400 start-file-seq-num 20 recover-file-seq-num

Usage
This command configures the parameters for storage of GTPP packets as files on the local server—meaning the hard disk.

Example
The following command configures rotation for every 1.5 hours (5400 seconds) for locally stored files.

```
gtpp storage-server local file rotation time-interval 5400 start-file-seq-num 20 recover-file-seq-num
```
**gtpp storage-server max-retries**

Configures the maximum number of times the system attempts to communicate with an unresponsive GTPP back-up storage server.

**Product**
- GGSN
- P-GW
- SAEGW

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration > Context Configuration
  ```
  configure > context context_name
  ```
  Entering the above command sequence results in the following prompt:
  ```
  [context_name] host_name(config-ctx)#
  ```

**Syntax**

```
gtpp storage-server max-retries max_attempts

default gtpp storage-server max-retries
```

**default gtpp storage-server max-retries**

```
default
```

Configures this command with the default setting.
Default: 2

```
max_attempts
```

Specifies the number of times the system attempts to communicate with a GTPP back-up storage server that is not responding. `max_attempts` enter an integer from 1 through 15.

**Usage**

This command works in conjunction with the `gtpp storage-server timeout` parameters to set a limit to the number of communication failures that can occur with a configured GTPP back-up storage server. The `gtpp storage-server timeout` command controls the amount of time between re-tries.

**Example**

The following command configures the maximum number of re-tries to be 8:

```
gtpp storage-server max-retries 8
```
gtpp storage-server mode

Configures storage mode, local or remote, for CDRs. Local storage mode is available with ASR 5000 platforms only.

Product
GGSN
P-GW
SAEGW
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration
configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

gtpp storage-server mode { local | remote | streaming }

default gtpp storage-server mode

default
Configures this command with the default setting.
Default: remote

local
Default: Disabled
Specifies the use of the hard disk on the SMC for storing CDRs

remote
Specifies the use of an external server for storing CDRs. This is the default value.

streaming
Default: Disabled
Allows the operator to configure “streaming” mode of operation for GTPP group. When this keyword is supplied the CDRs will be stored in following fashion:

- When GTPP link is active with CGF, CDRs are sent to a CGF via GTPP and local hard disk is NOT used as long as every record is acknowledged in time.
- If the GTPP connection is considered to be down, all streaming CDRs will be saved temporarily on the local hard disk and once the connection is restored, unacknowledged records will be retrieved from the hard disk and sent to the CGF.
Usage
This command configures whether the CDRs should be stored on the hard disk of the SMC or remotely, on an external server.

Example
The following command configures use of a hard disk for storing CDRs:

```
gtpp storage-server mode local
```
**gtpp storage-server timeout**

Configures the amount of time that must pass with no response before the system re-attempts to communicate with the GTPP back-up storage server.

**Product**

GGSN
P-GW
SAEGW

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration

`configure > context context_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
gtpp storage-server timeout duration

default gtpp storage-server timeout
```

**default gtpp storage-server timeout**

- `default`

  Configures this command with the default setting.
  Default: 30 seconds

- `duration`

  Specifies the maximum amount of time (in seconds) the system waits for a response from the GTPP back-up storage server before assuming the packet is lost. `duration` is an integer from 30 through 120.

**Usage**

This command works in conjunction with the `gtpp storage-server max-retries` command to establish a limit on the number of times that communication with a GTPP back-up storage server is attempted before a failure is logged. This parameter specifies the time between retries.

**Example**

The following command configures a retry timeout of 60 seconds:

```
gtpp storage-server timeout 60
```
**gtpp suppress-cdrs zero-volume**

This command suppresses the CDRs with zero byte data count. The CDRs can be classified as Final-cdrs, Internal-trigger-cdrs, and External-trigger-cdrs. This command allows the selection of CDRs to be suppressed and it is disabled by default.

**Important:** This command is license dependent. For more information, contact your Cisco account representative.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration

`configure > context context_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
gtpp suppress-cdrs zero-volume { external-trigger-cdr | final-cdr | internal-trigger-cdr }

default gtpp suppress-cdrs zero-volume

no gtpp suppress-cdrs zero-volume
```

*default*

Configures this command with the default setting.

*no*

Disables suppression of the CDRs with zero byte data count.

**Usage**

This command suppresses the CDRs with zero byte data count. This command provides an option to select the CDRs to be suppressed.

**Example**

To suppress only final zero volume CDRs use:

```
gtpp suppress-cdrs zero-volume final-cdr
```

To suppress final zero Volume CDRs and interim zero volume CDRs due to internal triggers use:

```
gtpp suppress-cdrs zero-volume final-cdr internal-trigger-cdr
```
To suppress final zero volume CDRs and interim zero volume CDRs due to internal and external triggers use:

`gtpp suppress-cdrs zero-volume final-cdr internal-trigger-cdr external-trigger-cdr`

To suppress interim zero volume CDRs due to internal and external triggers use:

`gtpp suppress-cdrs zero-volume internal-trigger-cdr external-trigger-cdr`

To suppress interim zero volume CDRs due to external triggers use:

`gtpp suppress-cdrs zero-volume external-trigger-cdr`
gtpp suppress-cdrs zero-volume-and-duration

Suppresses the CDRs created by sessions having zero duration and/or zero volume. By default this mode is disabled.

**Product**
- GGSN
- P-GW
- SAEGW
- SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration
```
configure > context context_name
```
Entering the above command sequence results in the following prompt:
```
[context_name]host_name(config-ctx)#
```

**Syntax**
```
gtpp suppress-cdrs zero-volume-and-duration { gcdrs [ egcdrs ] | egcdrs [ gcdrs ] }

default gtpp suppress-cdrs zero-volume-and-duration
```

**Usage**
Use this command to suppress the CDRs (G-CDRs and eG-CDRs) which were created when zero-duration sessions and zero-volume sessions are encountered due to any reason. By default this command is disabled and system will not suppress any CDR.

**Example**
The following command configures the system to suppress the eG-CDRs created for a zero duration session or zero volume session:
```
gtpp suppress-cdrs zero-volume-and-duration egcdrs gcdrs
```
**gtpp timeout**

Configures the amount of time that must pass with no response before the system re-attempts to communicate with the Charging Gateway Function (CGF).

**Product**
- GGSN
- SGSN
- P-GW
- SAEGW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration
```bash
configure > context context_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
gtpp timeout time

default gtpp timeout
```

- **default**
  Configures this command with the default setting. Default: 20 seconds

- **time**
  Specifies the maximum amount of time (in seconds) the system waits for a response from the CGF before assuming the packet is lost. `time` is an integer from 1 through 60.

**Usage**
This command works in conjunction with the `gtpp max-retries` command to establish a limit on the number of times that communication with a CGF is attempted before a failure is logged. This parameter specifies the time between retries.

**Example**

The following command configures a retry timeout of 30 seconds:

```
gtpp timeout 30
```
gtpp trigger

This command is left in place for backward compatibility. To disable and enable GTPP triggers you should use the `gtpp trigger` command in GTPP Server Group Configuration Mode.
gtpp transport-layer

Selects the transport layer protocol for the Ga interface for communication between the access gateways (GSNs) and GTPP servers.

Product

GGSN
P-GW
SAEGW
SGSN

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > Context Configuration
configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

```
gtpp transport-layer { tcp | udp }

default gtpp transport-layer
```

default

Configures this command with the default setting.
Default: udp

tcp

Default: Disabled
Enables the system to implement TCP as transport layer protocol for communication with GTPP server.

udp

Default: Enabled
Enables the system to implement UDP as transport layer protocol for communication with GTPP server.

Usage

Use this command to select the TCP or UDP as the transport layer protocol for Ga interface communication between GTPP servers and AGWs (GSNs).

Example

The following command enables TCP as the transport layer protocol for the GSN’s Ga interface.

```
  gtpp transport-layer tcp
```
**gtpu-service**

Creates a GTP-U service or specifies an existing GTP-U service and enters the GTP-U Service Configuration Mode for the current context.

**Product**
- GGSN
- P-GW
- SAEGW
- S-GW

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration
```
configure > context context_name
```
Entering the above command sequence results in the following prompt:
```
[context_name]host_name(config-ctx)#
```

**Syntax**
```
gtpu-service service_name [ -noconfirm ]
no gtpu-service service_name
```
- `gtpu-service service_name` Specifies the name of the GTP-U service. If `service_name` does not refer to an existing service, a new service is created if resources allow. `service_name` is an alphanumeric string of 1 through 63 characters.

- `-noconfirm` Executes the command without any additional prompt and confirmation from the user.

- `no gtpu-service service_name` Removes the specified GTP-U service from the context.

**Usage**
Enter the GTP-U Service Configuration Mode for an existing service or for a newly defined service. This command is also used to remove an existing service. A maximum of 256 services (regardless of type) can be configured per system.

**Caution:** Large numbers of services greatly increase the complexity of management and may impact overall system performance (for example, resulting from such things as system handoffs). Therefore, it is recommended that a
large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Entering this command results in the following prompt:

```
[context_name] hostname(config-gtpu-service)#
```

GTP-U Service Configuration Mode commands are defined in the *GTP-U Service Configuration Mode Commands* chapter.

**Example**

The following command enters the existing GTP-U Service Configuration Mode (or creates it if it does not already exist) for the service named `gtpu-service1`:

```
gtpu-service gtpu-service1
```

The following command will remove `gtpu-service1` from the system:

```
no gtpu-service gtpu-service1
```
ha-service

Creates/deletes a home agent service or specifies an existing HA service for which to enter the Home Agent Service Configuration Mode for the current context.

Product
HA

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration
configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

ha-service name [ -noconfirm ]

no ha-service name

no
Indicates the home agent service specified is to be removed.

name
Specifies the name of the HA service to configure. If name does not refer to an existing service, the new service is created if resources allow. name is an alphanumeric string of 1 through 63 characters.

Important: Service names must be unique across all contexts within a chassis.

- noconfirm
Executes the command without any additional prompt and confirmation from the user.

Usage
Enter the HA Service Configuration Mode for an existing service or for a newly defined service. This command is also used to remove an existing service.
A maximum of 256 services (regardless of type) can be configured per system.

Caution: Large numbers of services greatly increase the complexity of management and may impact overall system performance (i.e. resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Example
The following command will enter, or create and enter, the HA service sampleService:
ha-service sampleService

The following command will remove sampleService as being a defined HA service:

no ha-service sampleService
hnbgw-service

Creates or removes an Home Node B Gateway (HNB-GW) service or configures an existing HNB-GW service and enters the HNB-GW Service Configuration Mode for Femto UMTS access networks configuration in the current context.

Product
HNB-GW

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration
```
configure > context context_name
```
Entering the above command sequence results in the following prompt:
```
[context_name]host_name(config-ctx)#
```

Syntax
```
hnbgw-service hnbgw_svc_name [ -noconfirm ]
```
```
no hnbgw-service hnbgw_svc_name
```

-hnbgw_svc_name
Specifies the name of the HNB-GW service. If service_name does not refer to an existing service, the new service is created if resources allow. hnbgw_svc_name is an alphanumeric string of 1 through 63 characters.

-noconfirm
Executes the command without any additional prompt and confirmation from the user.

Usage
Use this command to enter the HNB-GW Service Configuration Mode for an existing service or for a newly defined service. This command is also used to remove an existing service.
A maximum of one HNB-GW service which is further limited to a maximum of 256 services (regardless of type) can be configured per system.

Caution: Large numbers of services greatly increase the complexity of management and may impact overall system performance (for example, resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Important: Service names must be unique across all contexts within a chassis.
Entering this command results in the following prompt:

```
[context_name]hostname(config-hnbgw-service)#
```

The commands available in this mode are defined in the *HNB-GW Service Configuration Mode Commands* chapter of *Command Line Interface Reference*.

⚠️ **Caution:** This is a critical configuration. The HNB-GW service can not be configured without this configuration. Any change to this configuration would lead to restarting the HNB-GW service and removing or disabling this configuration will stop the HNB-GW service.

**Example**

The following command enters the existing HNB-GW Service Configuration Mode (or creates it if it does not already exist) for the service named `hnb-service1`:

```
hnbgw-service hnb-service1
```

The following command will remove `hnb-service1` from the system:

```
no hnbgw-service hnb-service1
```
**hsgw-service**

Creates an HSGW service or specifies an existing HSGW service and enters the HSGW Service Configuration Mode for the current context.

**Product**
HSGW

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration

`configure > context context_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
hsgw-service service_name [ -noconfirm ]

no hsgw-service service_name
```

- **no**
  Removes the specified HSGW service from the context.

- **service_name**
  Specifies the name of the HSGW service. If `service_name` does not refer to an existing service, the new service is created if resources allow. `service_name` is an alphanumeric string of 1 through 63 characters.

**Important:** Service names must be unique across all contexts within a chassis.

```
-noconfirm
```

Executes the command without any additional prompt and confirmation from the user.

**Usage**

Enter the HSGW Service Configuration Mode for an existing service or for a newly defined service. This command is also used to remove an existing service.

A maximum of 256 services (regardless of type) can be configured per system.

**Caution:** Large numbers of services greatly increase the complexity of management and may impact overall system performance (for example, resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Entering this command results in the following prompt:
HSGW Service Configuration Mode commands are defined in the *HSGW Service Configuration Mode Commands* chapter.

Use this command when configuring the following eHRPD components: HSGW.

**Example**

The following command enters the existing HSGW Service Configuration Mode (or creates it if it does not already exist) for the service named `hsgw-service1`:

```
no hsgw-service hsgw-service1
```
hss-peer-service

Creates a Home Subscriber Service (HSS) peer service or configures an existing HSS peer service and enters the HSS Peer Service Configuration Mode.

Product
MME
SGSN

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration
```
configure > context context_name
```
Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

Syntax

```
hss-peer-service service_name [ -noconfirm ]

no hss-peer-service service_name
```

- **no**
  Removes the specified HSS peer service from the context.

- **service_name**
  Specifies the name of the HSS peer service. If `service_name` does not refer to an existing service, a new service is created if resources allow. `service_name` is an alphanumeric string of 1 through 63 characters.

**Important:** Service names must be unique across all contexts within a chassis.

- **-noconfirm**
  Executes the command without any additional prompt and confirmation from the user.

Usage

Enter the HSS Peer Service Configuration Mode for an existing service or for a newly defined service. This command is also used to remove an existing service. A maximum of 256 services (regardless of type) can be configured per system.

**Caution:** Large numbers of services greatly increase the complexity of management and may impact overall system performance (for example, resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.
Entering this command results in the following prompt:

```
[context_name]hostname(config-hss-peer-service)#
```

HSS Peer Service Configuration Mode commands are defined in the *HSS Peer Service Configuration Mode Commands* chapter.

**Example**

The following command enters the existing HSS Peer Service Configuration Mode (or creates it if it does not already exist) for the service named `hss-peer1`:

```
hss-peer-service hss-peer1
```

The following command will remove `hss-peer1` from the system:

```
no hss-peer-service hss-peer1
```
This section includes the commands `ikev1 disable-initial-contact` through `multicast-proxy` service.

**Mode**

Exec > Global Configuration > Context Configuration

`configure > context context_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Important**: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
ikev1 disable-initial-contact

Disables the sending of the INITIAL-CONTACT message in the IKEv1 protocol after the node creates a new Phase1 SA, caused either by Dead Peer Detection or by a rekey.

Product
GGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration

configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

[ no ] ikev1 disable-initial-contact

no
Disables this command, which re-enables the sending of the INITIAL-CONTACT message.

Usage

Use this command to disable the sending of the INITIAL-CONTACT message in the IKE v1 protocol.

Example

The following command disables the sending of the INITIAL-CONTACT message:

   ikev1 disable-initial-contact
ikev1 disable-phase1-rekey

Configures the rekeying of Phase1 SA when the Internet Security Association and Key Management Protocol (ISAKMP) lifetime expires in Internet Key Exchange (IKE) v1 protocol.

Product
PDSN
HA
GGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration
configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax
[ no ] ikev1 disable-phase1-rekey

Syntax

no

Re-enables Phase 1 SAs when the ISAKMP lifetime expires.

Usage
Use this command to disable the rekeying of Phase 1 SAs when the ISAKMP lifetime expires in IKE v1 protocol.

Example
The following command disables rekeying of Phase1 SAs when the lifetime expires:

ikev1 disable-phase1-rekey
ikev1 keepalive dpd

Configures the ISAKMP IPSec Dead Peer Detection (DPD) message parameters for IKE v1 protocol.

Product
PDSN
HA
GGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration
configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

[ no ] ikev1 keepalive dpd interval interval timeout time num-retry retries

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Deletes previously configured IPSec DPD Protocol settings.</td>
</tr>
<tr>
<td>dpd interval</td>
<td>Specifies the time interval (in seconds) at which IPSec DPD Protocol messages are sent. interval is an integer from 10 through 3600.</td>
</tr>
<tr>
<td>timeout time</td>
<td>Specifies the amount of time (in seconds) allowed for receiving a response from the peer security gateway prior to re-sending the message. time is an integer from 10 through 3600.</td>
</tr>
<tr>
<td>num-retry retries</td>
<td>Specifies the maximum number of times that the system should attempt to reach the peer security gateway prior to considering it unreachable. retries is an integer from 1 through 100.</td>
</tr>
</tbody>
</table>

Usage

Use this command to configure the ISAKMP dead peer detection parameters in IKE v1 protocol. Tunnels belonging to crypto groups are perpetually kept “up” through the use of the IPSec Dead Peer Detection (DPD) packets exchanged with the peer security gateway.

Important: The peer security gateway must support RFC 3706 in order for this functionality to function properly.
This functionality is for use with the Redundant IPSec Tunnel Fail-over feature and to prevent IPSec tunnel state mismatches between the FA and HA when used in conjunction with Mobile IP applications. Regardless of the application, DPD must be supported/configured on both security peers. If the system is configured with DPD but it is communicating with a peer that does not have DPD configured, IPSec tunnels still come up. However, the only indication that the remote peer does not support DPD exists in the output of the `show crypto isakmp security associations summary dpd` command.

**Important:** If DPD is enabled while IPSec tunnels are up, it will not take affect until all of the tunnels are cleared.

**Example**

The following command configures IPSec DPD Protocol parameters to have an interval of 15, a timeout of 10, to retry each attempt 5 times:

```
ikev1 keepalive dpd interval 15 timeout 10 num-retry 5
```
ikev1 policy

Configures or creates an ISAKMP policy with the specified priority and enters ISAKMP Configuration Mode for IKE v1 protocol.

**Product**
- PDSN
- HA
- GGSN

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration > Context Configuration
- `configure > context context_name`

Entering the above command sequence results in the following prompt:

```
[context_name] host_name(config-ctx)#
```

**Syntax**

```
[ no ] ikev1 policy priority
```

- **no**
  - Removes a previously configured ISAKMP policy for IKE v1 protocol.

- **priority**
  - Specifies the priority of an ISAKMP policy as an integer from 0 through 100. ISAKMP policies for IKE v1 protocol with lower priority numbers take precedence over policies with higher priorities. “0” is the highest priority. Default: 0

**Usage**

Use this command to create ISAKMP policies to regulate how IPSec key negotiation is performed for IKE v1 protocol.

Internet Security Association Key Management Protocol (ISAKMP) policies are used to define Internet Key Exchange (IKE) SAs. The IKE SAs dictate the shared security parameters (i.e. which encryption parameters to use, how to authenticate the remote peer, etc.) between the system and a peer security gateway.

During Phase 1 of IPSec establishment, the system and a peer security gateway negotiate IKESAs. These SAs are used to protect subsequent communications between the peers including the IPSec SA negotiation process.

Multiple ISAKMP policies can be configured in the same context and are used in an order determined by their priority number.

**Example**

Use the following command to create an ISAKMP policy with the priority 1 and enter the ISAKMP Configuration Mode:

```
ikev1 policy 1
```
ikev2-ikesa

Creates a new, or specifies an existing, IKEv2 security association parameters and enters the IKEv2 Security Association Configuration Mode.

**Product**
ePDG
HeNBGW
PDIF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration

```
configure > context context_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
[ no ] ikev2-ikesa { auth-method-set auth_method_set_name | transform-set transform_set_name }
```

- **no**

  Removes the entered IKEv2 security association authentication method set or transform set from the system.

- **auth-method-set auth_method_set_name**

  Configure an IKEv2 IKE Security Association Auth-Method Set. Applicable for IKEv2 subscriber-mode based products. This object encapsulates various Authentication methods. **auth_method_set_name** is the context level name to be used for the IKEv2 IKE Security Association Authentication methods Set, which is a string of size 1 to 127.

- **transform-set transform_set_name**

  Configure an IKEv2 IKE Security Association Transform Set. This object encapsulates various IKEv2 IKE algorithm configurations which are required for establishing and IKEv2 IKE Security Association with a remote peer. **transform_set_name** is the context level name to be used for the IKEv2 IKE Security Association Transform Set, which is a string of size 1 to 127.

**Usage**

Use this command to create a new or enter an existing IKEv2 security association parameters set. A list of up to four separate transform-sets and three separate authentication method sets can be created. Entering the command **transform-set transform_set_name** results in the following prompt:

```
[context_name]hostname(cfg-ctx-ikev2ikesa-tran-set)#
```
IKEv2 Security Association Configuration Mode commands are defined in the *IKEv2 Security Association Configuration Mode Commands* chapter.

**Example**

The following command configures an IKEv2 security association transform set called `ikesa3` and enters the IKEv2 Security Association Configuration Mode:

```
ikev2-ikesa transform-set ikesa3
```
**ims-auth-service**

This command enables the creation, configuration or deletion of an IMS authorization service in the current context.

**Product**
GGSN  
HA  
IPSG  
PDSN  
P-GW  
SAEGW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration

```
configure > context context_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
ims-auth-service auth_svc_name [ -noconfirm ]
```

{ no | default } ims-auth-service auth_svc_name

- **no**
  Deletes the specified IMS authorization service within the current context.

- **default**
  Restores default state of IMS authorization service, disabled for a specific context.

- **auth_svc_name**
  Specifies name of the IMS authorization service as a unique alphanumeric string of 1 through 63 characters. In releases prior to 18, a maximum of 16 authorization services can be configured globally in the system. There is also a system limit for the maximum number of total configured services. In 18 and later releases, up to a maximum of 30 IMS authorization service profiles can be configured within the system.

**Important:** Service names must be unique across all contexts within the system.

- **-noconfirm**
  Executes the command without any additional prompt and confirmation from the user.
Usage

Use this command to create/configure/delete an IMS authorization service for Gx interface support in the current context.

Entering this command results in the following prompt:

```
[context_name]hostname(config-imsa-service)
```

IMS authorization Service Configuration commands are described in the *IMS Authorization Service Configuration Mode Commands* chapter.

**Important:** Whenever a new ims-auth-serv is configured using an endpoint that is used by another ims-auth-serv, then the diabase callbacks are overwritten with values of the new IMSA service. This is a limitation on the system to register only one application per endpoint. So, multiple IMSA services registering with same endpoint may not work properly. If such scenario occurs, configure a different endpoint name for the IMSA service being used and then remove and re-configure the IMSA service used.

Example

The following command configures an IMS authorization service named *ims_interface1* within the current context:

```
ims-auth-service ims_interface1
```
**ims-sh-service**

Creates the specified IP Multimedia Subsystem (IMS) Sh service name to allow configuration of an Sh service.

**Product**
- PDIF
- SCM

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration
`configure > context context_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
ims-sh-service name

no ims-sh-service name
```

**Important**: Service names must be unique across all contexts within a chassis.

**Usage**

The IMS-Sh-service is named in the pdif-service and/or csf-service. Use this command to enter the IMS Sh Service Configuration Mode.

Entering this command results in the following prompt:
```
[context_name]host_name(config-ims-sh-service)#
```

IMS Sh Service Configuration Mode commands are defined in the *IMS Sh Service Configuration Mode Commands* chapter in this guide.

**Example**

The following example creates or enters an IMS Sh service named *ims-1*:

```
ims-sh-service ims-1
```
inspector

Configures a context-level inspector account within the current context.

**Product**
All

**Privilege**
Security Administrator

**Mode**
Exec > Global Configuration > Context Configuration

`configure > context context_name`

Entering the above command sequence results in the following prompt:

```
[context_name] host_name(config-ctx)#
```

**Syntax**

```
inspector user_name [ encrypted ] password password [ ecs | noecs ] [ expiry-date date_time ] [ li-administration ] [ noecs ] [ timeout-absolute abs_seconds ] [ timeout-min-absolute abs_minutes ] [ timeout-idle timeout_duration ] [ timeout-min-idle idle_minutes ]
```

```
no inspector user_name
```

*no*

Removes a previously configured inspector account.

**user_name**

Specifies a name for the context-level inspector account as an alphanumeric string of 1 through 32 characters.

```
[ encrypted ] password password
```

Specifies the password to use for the user which is being given context-level inspector privileges within the current context. The encrypted keyword indicates the password specified uses encryption.

`password` is an alphanumeric string of 1 through 63 characters without encryption, or 1 through 127 characters with encryption.

The encrypted keyword is intended only for use by the system while saving configuration scripts. The system displays the encrypted keyword in the configuration file as a flag that the variable following the password keyword is the encrypted version of the plain text password. Only the encrypted password is saved as part of the configuration file.

**ecs | noecs**

Default: `noecs`

`ecs`: Permits the specific user to access ACS-specific configuration commands.

`noecs`: Prevents the specific user to access ACS-specific configuration commands.
expiry-date date_time
Specifies the date and time that this account expires. Enter the date and time in the format YYYY:MM:DD:HH:mm or YYYY:MM:DD:HH:mm:ss. Where YYYY is the year, MM is the month, DD is the day of the month, HH is the hour, mm is minutes, and ss is seconds.

li-administration
Refer to the Lawful Intercept Configuration Guide for a description of this parameter.

timeout-absolute abs_seconds
This keyword is obsolete. It has been left in place for backward compatibility. If used a warning is issued and the value entered is rounded to the nearest whole minute.
Specifies the maximum amount of time (in seconds) the context-level inspector may have a session active before the session is forcibly terminated. abs_seconds must be an integer from 0 through 30000000. The value 0 disables the absolute timeout. Default: 0

timeout-min-absolute abs_minutes
Specifies the maximum amount of time (in minutes) the context-level inspector may have a session active before the session is forcibly terminated. abs_minutes must be an integer from 0 through 525600 (365 days). The value 0 disables the absolute timeout. Default: 0

timeout-idle timeout_duration
This keyword is obsolete. It has been left in place for backward compatibility. If used a warning is issued and the value entered is rounded to the nearest whole minute.
Specifies the maximum amount of idle time (in seconds) the context-level inspector may have a session active before the session is terminated. timeout_duration must be an integer from 0 through 30000000. The value 0 disables the idle timeout. Default: 0

timeout-min-idle idle_minutes
Specifies the maximum amount of idle time (in minutes) the context-level inspector may have a session active before the session is terminated. idle_minutes must be an integer from 0 through 525600 (365 days). The value 0 disables the idle timeout. Default: 0

Usage
Create new context-level inspector or modify existing inspector's options, in particular, the timeout values. Inspector users have minimal read-only privileges. Refer to the Command Line Interface Overview chapter for more information.

Important: A maximum of 128 administrative users and/or subscribers may be locally configured per context.

Example
The following command creates a context-level inspector account named user1:

```
inspector user1 password secretPassword
```

The following command removes a context-level inspector account named user1:
no inspector user1
interface

Creates or deletes an interface or specifies an existing interface. By identifying an interface, the mode changes to configure this interface in the current context.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration
configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

interface name [ broadcast | loopback | point-to-point | tunnel ]

no interface name

no
Indicates the interface specified is to be removed.

name
Specifies the name of the interface to configure. If name does not refer to an existing interface, the new interface is created if resources allow. name is an alphanumeric string of 1 through 79 characters.

broadcast
Creates an Ethernet broadcast (IP) interface and enters the Ethernet Configuration Mode. Default: Enabled

Important: Refer to the Ethernet Interface Configuration Mode Command chapter for more information.

loopback

Creates an internal IP address that is always UP, is not bound to any physical card/port, and can be reached by any interface configured in the current context. As a loopback interface uses all available physical ports, this type of interface is particularly useful for load-balancing. The interface must be configured for loopback when configuring Interchassis Session Recovery (ICSR). A total of 256 loopback interfaces can be configured. Default: Disabled

This loopback option is not used to setup a diagnostic test port so it should not be confused with the loopback option used in the various card/port configuration modes.

Important: Refer to the Loopback Interface Configuration Mode Command chapter for more information.
point-to-point

Creates a permanent virtual connection (PVC) in the current context and enters the PVC Configuration Mode. Currently, this type of interface is only used with an optical (ATM) line card.

Important: Refer to the PVC Interface Configuration Mode Command chapter for more information.

tunnel

Creates a tunnel interface to support the various tunnel interfaces. Currently only IPv6-over-IPv4 and GRE tunnel interfaces are supported.

Important: Refer to the Tunnel Interface Configuration Mode Commands chapter for more information.

Usage

Use this command to enter or create the interface configuration mode for an existing interface or for a newly defined interface. This command is also used to remove an existing interface when it longer is needed.

Important: If no keyword is specified, broadcast is assumed and the interface is Ethernet by default.

Example

For IPv6-over-IPv4 or GRE tunneling, you need to specify the interface type as tunnel.

The following command enters the Ethernet Interface Configuration Mode creating the interface sampleService, if necessary:

```
interface sampleInterface
```

The following command removes sampleService as being a defined interface:

```
no interface sampleInterface
```

The following command enters the Tunnel Interface Configuration Mode creating the interface GRE_tunnel1, if necessary:

```
interface GRE_tunnel1 tunnel
```
**ip access-group**

Configures an access group with an Access Control List (ACL) for IP traffic for the current context. The Context-level ACL is applied only to outgoing packets.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration

`configure > context context_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
ip access-group name [ in | out ] [ priority_value ]

no ip access-group name [ in | out ]
```

- **name**
  Indicates the specified ACL rule is to be removed from the group.

- **priority_value**
  Specifies the priority of the access group. 0 is the highest priority. If `priority_value` is not specified, the priority is set to 0. `priority_value` must be an integer from 0 through 4294967295. Default: 0.

- If access groups in the list have the same priority, the last one entered is used first.

**Usage**

Use this command to add IP access lists (refer to the `ip access-list` command) configured with in the same context to an ACL group.

---

**Important:** Up to eight ACLs can be applied to a group provided that the number of rules configured within the ACL(s) does not exceed the 256-rule limit for the context.
Refer to the *Access Control Lists* appendix of the *System Administration Guide* for more information on ACLs.

**Example**

The following commands add `sampleGroup` to the context-level ACL with a priority of `0`:

```
ip access-group sampleGroup 0
```
**ip access-list**

Enables creation, configuration or deletion of an IP Access List in the current context.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration

`configure > context context_name`

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-ctx)#w`

**Syntax**

```plaintext
ip access-list name

{ default | no } ip access-list name
```

- **default**
  Sets the context’s default access control list to that specified by `name`.

- **no**
  Removes the specified access list.

- **name**
  Specifies the access list name.
  In Release 8.0, `name` is an alphanumeric string of 1 through 79 characters.
  In Release 8.1 and later, `name` is an alphanumeric string of 1 through 47 characters.
  If the named access list does not exist, it is created, and the CLI mode changes to the ACL Configuration Mode, wherein the access list can be configured.
  If the named access list already exists, the CLI mode changes to the ACL Configuration Mode, wherein the access list can be reconfigured.

**Usage**

Executing this command enters the ACL Configuration Mode in which rules and criteria are defined for the ACL.

**Important:** A maximum of 64 rules can be configured per ACL. The maximum number of ACLs that can be configured per context is limited by the amount of available memory in the VPN Manager software task; it is typically less than 200.

The no version of this command deletes the ACL.
Refer to the *Access Control Lists* appendix of the *System Administration Guide* for more information on ACLs.

**Example**

The following command creates an access list named `sampleList`, and enters the ACL Configuration Mode:

```
ip access-list sampleList
```
ip arp

Configures the allocation retention priority (ARP) options for the current context.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration

configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

ip arp ip_address mac_address [ vrf vrf_name ]

no ip arp ip_address mac_address

no

Removes the ARP configuration data for the specified IP address from the configuration.

ip_address

Specifies the IP address for which to configure the ARP options where ip_address is an IP address expressed in IPv4 dotted-decimal notation.

mac_address

Specifies the media-specific access control layer address for the IP address. mac_address must be specified as a an 6-byte hexadecimal number with each byte separated by a colon, for example., “AA:12:bb:34:ff:0E”.

vrf vrf_name

Associates a Virtual Routing and Forwarding (VRF) context with this static ARP entry. vrf_name is name of a preconfigured virtual routing and forwarding (VRF) context configured in Context Configuration Mode via the ip vrf command.

Usage

Manage the IP address mapping which is a logical/virtual identifier to the more lower layer addressing used for address resolution in ICMP messages.

For tunnel-based interface, network IP pool can have overlapping ip-addresses across Verve. To manage it adding a preconfigured VRF context is required to associate with an static ARP entry. By default, the ARP is added in the given context. If the VRF name is specified, then the ARP is added to the VRF ARP table.

Example

The following commands set the IP and MAC address for the current context then remove it from the configuration:
The following commands set the IP and MAC address for a VRF context `vrf1` in the configuration:

```
ip arp 10.2.3.4 F1:E2:D4:C5:B6:A7
no ip arp 10.2.3.4
```

```
ip arp 10.2.3.4 F1:E2:D4:C5:B6:A7 vrf vrf1
```
ip as-path access-list


**Product**
HA

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration

**Syntax**

```
[ no ] ip as-path access-list list_name [ { deny | permit } reg_expr ]
```

- **no**
  Remove the specified regular expression from the AS path access list.

- **list_name**
  Specifies the name of an AS path list as an alphanumeric string of 1 through 79 characters.

- **{ deny | permit }**
  *deny*: Denies access to AS paths that match the regular expression.
  *permit*: Allows access to AS paths that match the regular expression.

- **reg_expr**
  A regular expression to define the AS paths to match. *reg_expr* is an alphanumeric string of 1 through 254 characters.

**Important:** The ? (question mark) character is not supported in regular expressions for this command.

**Usage**

Use this command to define AS path access lists for the BGP router in the current context. The chassis supports a maximum of 64 access lists per context.

**Example**

The following command creates an AS access list named *ASlist1* and permits access to AS paths:

```
ip as-path access-list ASlist1 permit
```
ip dns-proxy source-address

Enables the proxy DNS functionality and identifies this context as the destination context for all redirected DNS requests.

**Important:** This command must be entered in the destination context for the subscriber. If there are multiple destination contexts for different subscribers, the command must be entered in each context.

**Product**
HA

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration

`configure > context context_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
[ no ] ip dns-proxy source-address ip_address
```

- **no**
  Removes the address in this context as a destination for redirected DNS packets.

- **ip_address**
  Specifies an interface in this context used for redirected DNS packets. `ip_address` must be entered using IPv4 dotted-decimal notation.

**Usage**

Use this command to identify the interface in this context where redirected DNS packets are sent to the home DNS. The system uses this address as the source address of the DNS packets when forwarding the intercepted DNS request to the home DNS server. For a more detailed explanation of the proxy DNS intercept feature, see the `proxy-dns intercept-list` command.

**Example**

The following command identifies an interface with an address of 10.23.255.255 in a destination context where the system forwards all intercepted DNS requests:

```
ip dns-proxy source-address 10.23.255.255
```
ip domain-lookup

Enables or disables domain name lookup via domain name servers for the current context.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration

```
configure > context context_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

Syntax

```
ip domain-lookup
no ip domain-lookup
```

Disables domain name lookup.

Usage

Domain name look up is necessary if the subscribers configured for the context are to be allowed to use logical host names for services which requires the host name resolution via DNS.

Example

```
ip domain-lookup
no ip domain-lookup
```


**ip domain-name**

Configures or removes a logical domain name for the current context.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration

```bash
configure > context context_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```bash
[ no ] ip domain-name name
```

---

**no**
Indicates the logical domain name for the current context is to be removed.

---

**name**
Specifies the logical domain name to use for domain name server address resolution. *name* is an alphanumeric string of 1 through 1023 characters formatted to be a valid IP domain name.

---

**Usage**
Set a logical domain name if the context is to be accessed by logical domain name in addition to direct IP address.

**Example**

```bash
ip domain-name sampleName.org
```
ip forward

Configures an IP forwarding policy to forward outgoing pool packets whose flow lookup fails to the default-gateway.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration

class > context context_name

Entering the above command sequence results in the following prompt:

[[context_name]host_name(config-ctx) #

**Syntax**

[ no ] ip forward outbound unused-pool-dest-address default-gateway

________

no

Disables forwarding to the default gateway.

________

outbound unused-pool-dest-address default-gateway

Enables forwarding to the default gateway.

**Usage**

Use this command to set an IP forwarding policy that forwards outgoing pool packets whose flow lookup fails to the default gateway. By default, the behavior is to either send an ICMP Unreachable message or to discard the packet depending on the configuration of the IP pool.

Pool packets coming from the line card or MIO card whose flow lookup fails are discarded or ICMP unreachable is sent irrespective of whether this command is configured or not.

**Example**

To enable this functionality, enter the following command:

```
ip forward outbound unused-pool-dest-address default-gateway
```

To disable this functionality, enter the following command:

```
no ip forward outbound unused-pool-dest-address default-gateway
```
ip guarantee

Enables and disables local switching of framed route packets.

**Product**

GGSN
P-GW
SAEGW

**Privilege**

Administrator

**Mode**

Exec > Global Configuration > Context Configuration

*configure > context context_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
[no] ip guarantee framed-route local-switching
```

- **no**
  
  Disables local switching of framed route packets.

- **framed-route local-switching**
  
  Enables local switching of framed route packets. By default, this functionality is disabled.

**Usage**

Use this command to enable and disable local switching of framed route packets. This functionality will be applicable only when there are some NEMO/framed route sessions in a context.

**Example**

The following command enables local switching of framed route packets:

```
ip guarantee framed-route local-switching
```
**ip identification packet-size-threshold**

Configures the packet size above which system will assign unique IP header identification.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration
```
configure > context context_name
```

Entering the above command sequence results in the following prompt:
```
[context_name]#>
```

**Syntax**

```
ip identification packet-size-threshold size
```

```
default ip identification packet-size-threshold
```

**Usage**
This configuration is used to set the upper limit of the IP packet size. All packets above that size limit will be considered “fragmentable”, and an unique non-zero identifier will be assigned.

**Example**
The following commands set the IP packet size to 1024 bytes as threshold. Above this limit system will assign unique IP header identification for system generated IP encapsulation headers:
```
ip identification packet-size-threshold 1023
```
ip igmp profile

Configures an Internet Group Management Protocol (IGMP) profile and moves to the IGMP Profile Configuration mode.

Product
PDSN
GGSN
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration
configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name] host_name(config-ctx)#

Syntax

[ no ] ip igmp profile name

no
Removes the specified IGMP profile.

name
Specifies the name of an IGMP profile as an alphanumeric string of 1 through 63 characters. If this is not the name of an existing profile, you are prompted to create the new profile.

Usage
Configure and existing IGMP profile or create a new one. When this command is executed you are moved to the IGMP Profile Configuration mode. For additional information, refer to the IGMP Profile Configuration Mode Commands chapter.

Example

ip igmp profile default
ip localhost

Configures or removes the static local host logical name to IP address mapping for the current context.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration
configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

[ no ] ip localhost name ip_address

no
Specifies that the static mapping must be removed.

name
Specifies the logical host name (DNS) for the local machine on which the current context resides. name is an alphanumeric string of 1 through 1023 characters formatted to be a valid IP host name.

ip_address
Specifies the IP address for the static mapping. ip_address must be expressed in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

Usage
Avoid excessive DNS lookups across the network by statically mapping the logical host name to the local host’s context.

Example

    ip localhost localHostName 10.2.3.4
    no ip localhost localHostName 10.2.3.4
**ip name-servers**

Modifies the list of domain name servers the current context may use for logical host name resolution.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration

```
configure > context context_name
```

Entering the above command sequence results in the following prompt:

```
[context_name] host_name(config-ctx) #
```

**Syntax**

```
ip name-servers ip_address secondary_ip_address

no ip name-servers ip_address
```

**no**

Indicates the name server specified is to be removed from the list of name servers for the current context.

**ip_address**

Specifies the IP address of a domain name server using IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

**secondary_ip_address**

Specifies the IP address of a secondary domain name server using either IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

**Usage**

Manage the list of name servers the current context may use in resolving logical host names.

The DNS can be specified at the Context level in Context configuration as well as at the APN level in APN Configuration Mode with `dns` and `ipv6 dns` commands, or it can be received from AAA server.

When DNS is requested in PCO configuration, the following preference will be followed for DNS value:

1. DNS Values received from LNS have the first preference.
2. DNS values received from RADIUS Server has the second preference.
3. DNS values locally configured with APN with `dns` and `ipv6 dns` commands has the third preference.
4. DNS values configured at context level has the last preference.

**Important:** The same preference would be applicable for the NBNS servers to be negotiated via ICPC with the LNS.
Example

   ip name-servers 10.2.3.4
ip pool

Enables creation, configuration or deletion of IP address pools in the current context.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration

```bash
configure > context context_name
```

Entering the above command sequence results in the following prompt:

```
[context_name] host_name(config-ctx) #
```

**Syntax**

```bash
ip pool pool_name { ip_address/subnet_mask | ip_address_mask_combo | range start_ip_address end_ip_address } [ address-hold-timer address_hold_timer ] [ address-quarantine-timer seconds ] [ advertise-if-used ] [ alert-threshold [ group-available | pool-free | pool-hold | pool-release | pool-used ] low_thresh [ clear high_thresh ] ] [ explicit-route-advertise ] [ group-name group_name ] [ include-nw-bcast ] [ napt-users-per-ip-address users_per_ip [ alert-threshold { pool-free | pool-hold | pool-release | pool-used } low_thresh [ clear high_thresh ] ] + ] [ max-chunks-per-user max_chunks_per_user [ nat-binding-timer nat_binding_timer ] [ nexthop-forwarding-address ip_address ] [ on-demand ] [ port-chunk-size port_chunk_size ] [ port-chunk-threshold port_chunk_threshold ] [ send-nat-binding-update ] + ] [ nat priority ] [ nat-one-to-one [ alert-threshold { pool-free | pool-hold | pool-release | pool-used } low_thresh [ clear high_thresh ] ] + ] [ nat-binding-timer nat_binding_timer ] [ nexthop-forwarding-address ip_address ] [ on-demand ] [ send-nat-binding-update ] + ] [ nat-realm users-per-nat-ip-address users [ on-demand [ address-hold-timer address_hold_timer ] ] ] [ nexthop-forwarding-address ip_address [ overlap vlanid vlan_id ] [ respond-icmp-echo ip_address ] [ nw-reachability server server_name ] [ policy allow-static-allocation ] [ framed-route-vrf-list vrf_list_name ] [ pool-route ip_address/ip_mask ] [ private priority ] [ public priority ] [ resource priority ] [ send-icm-p-dest-unreachable ] [ skip-nat-subscriber-ip-check ] [ srp-activate ] [ subscriber-gw-address ip_address ] [ static ] [ suppress-switchover-arp ] [ tag { none | pdif-set-up-addr } ] [ unicast-gratuitous-arp-address ip_address ] [ vrf vrf_name { [ mpls-label input in_label_value | output out_label_value1 [ out_label_value2 ] } ] [ framed-route-vrf-list ]
```

no ip pool pool_name [ address-hold-timer ] [ address-quarantine-timer ] [ advertise-if-used ] [ alert-threshold { group-available | pool-free | pool-hold | pool-release } [ pool-used ] + ] [ explicit-route-advertise ] [ group-name ] [ include-nw-bcast ] [ nexthop-forwarding-address respond-icmp-echo ] [ nw-reachability server ] [ policy allow-static-allocation ] [ framed-route-vrf-list ] [ send-icm-p-dest-unreachable ] [ skip-nat-subscriber-ip-check ] [ srp-activate ] [ subscriber-gw-address ] [ suppress-switchover-arp ] [ tag { none | pdif-set-up-addr } ] [ unicast-gratuitous-arp-address ] + [ send-nat-binding-update ] [ framed-route-vrf-list ]
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Removes the specified IP address pool from the current context’s configuration, or disables the specified option(s) for the specified IP pool.</td>
</tr>
<tr>
<td>no alert-threshold</td>
<td>This command without any optional keywords disables all alert thresholds.</td>
</tr>
<tr>
<td>name</td>
<td>Specifies the logical name of the IP address pool. name must be an alphanumeric string of 1 through 31 characters.</td>
</tr>
</tbody>
</table>

**Important:** An error message displays if the `ip pool name` and the `group name` in the configuration are the same. An error message displays if the `ip pool name` or `group name` are already used in the context.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip_address</td>
<td>Specifies the beginning IP address of the IP address pool using IPv4 dotted-decimal.</td>
</tr>
<tr>
<td>subnet_mask</td>
<td>Specifies the IP address mask bits to determine the number of IP addresses in the pool. <code>ip_mask</code> must be specified using IPv4 dotted-decimal notation. 1 bits in the <code>ip_mask</code> indicate that bit position in the <code>ip_address</code> must also have a value of 1. 0 bits in the <code>ip_mask</code> indicate that bit position in the <code>ip_address</code> does not need to match – the bit can be either a 0 or a 1. For example, if the IP address and mask are specified as <code>172.168.10.0</code> and <code>255.255.255.224</code>, respectively, the pool will contain IP addresses in the range <code>172.168.10.0</code> through <code>172.168.10.31</code> for a total of 32 addresses.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip_address_mask_combo</td>
<td>Specifies a combined IP address subnet mask bits to indicate what IP addresses the route applies to. <code>ip_address_mask_combo</code> must be specified using CIDR notation where the IP address is specified using IPv4 dotted-decimal notation and the mask bits are a numeric value which is the number of bits in the subnet mask.</td>
</tr>
<tr>
<td>range start_ip_address end_ip_address</td>
<td>Specifies the IP addresses for the IP pool as a range of addresses. <code>start_ip_address</code> specifies the beginning of the range of addresses for the IP pool. <code>end_ip_address</code> specifies the end of the range of addresses for the IP pool. The IP address range must be specified using IPv4 dotted-decimal notation. For example, if <code>start_ip_address</code> is specified as <code>172.168.10.0</code> and <code>end_ip_address</code> is specified as <code>172.168.10.31</code> the IP pool will contain addresses in the range <code>172.168.10.0</code> through <code>172.168.10.31</code> for a total of 32 addresses.</td>
</tr>
<tr>
<td>private [ priority ]</td>
<td>Address pool may only be used by mobile stations which have requested an IP address from a specified pool. When private pools are part of an IP pool group, they are used in a priority order according to the precedence setting. <code>priority</code> must be an integer from 0 through 10 with 0 being the highest priority. The default value is 0.</td>
</tr>
</tbody>
</table>
public [ priority ]
Address pool is used in priority order for assigning IP addresses to mobile stations which have not requested
a specific address pool. priority must be an integer from 0 through 10 with 0 being the highest priority.
The default value is 0.

static
Designates local IP address pool to statically assign pooled addresses.

---

**Important:** The keyword static must be used for DHCP served IP addresses.

tag { none | pdif-setup-addr }
Default: none
none: default tag for all IP address pools
pdif-setup-addr: pool with this tag should only be used for PDIF calls.

address-hold-timer seconds
When this is enabled, and an active subscriber is disconnected, the IP address is held or considered still in
use, and is not returned to the free state until the address-hold-timer expires. This enables subscribers who
reconnect within the length of time specified (in seconds) to obtain the same IP address from the IP pool.
seconds is the time in seconds and must be an integer from 0 through 31556926.

---

**Important:** Currently, the address-hold-timer only supports IPv4 addresses.

address-quarantine-timer seconds
Specifies the timer value in seconds for an address quarantine timer as an integer from 20 through 86400.
This timer cannot be configured with an address-hold-timer in the same pool.
The IP pool address-quarantine-timer is a mechanism to busy out a released IP address for a specified
interval. This prevents an IP address from being reused until the quarantine timer expires.
Each IP pool can be configured with a timer value that determines how long a recently released address will
be held in quarantine before being freed. When the timer has expired, the address is returned to the list of free
addresses, to be allocated again to a new subscriber. Any address that has been released, but for which the
address-quarantine-timer has not expired, is still considered to be in use for the purposes of allocation. If a
subscriber tries to reconnect while the address-quarantine timer is armed, even though it is the same
subscriber ID, the subscriber does not get the same address.

advertise-if-used
Advertises to the peer routes only if addresses are being used in pool.

alert-threshold { group-available | pool-free | pool-hold | pool-release | pool-used } low_thresh [ clear high_thresh ]
Default: All thresholds are disabled.
Configures IP address pool-level utilization thresholds. These thresholds take precedence over context-level
IP pool thresholds.
group-available: Set an alert based on the available percentage of IP addresses for the entire IP pool
group.
pool-free: Set an alert based on the percentage of IP addresses that are unassigned in this IP pool.
pool-hold: Set an alert based on the percentage of IP addresses from this IP pool that are on hold.
pool-release: Set an alert based on the percentage of IP addresses from this IP pool that are in the release state.
pool-used: This command sets an alert based on the percentage of IP addresses that have been assigned from this IP pool.

**Important:** Refer to the threshold available-ip-pool-group and threshold monitoring commands in this chapter for additional information on IP pool utilization thresholding.

low_thresh: The IP pool utilization percentage that must be met or exceeded within the polling interval to generate an alert or alarm. It can be configured as an integer between 0 and 100.

clear high_thresh: The IP pool utilization percentage that maintains a previously generated alarm condition. If the utilization percentage rises above the high threshold within the polling interval, a clear alarm is generated. It may be configured as an integer between 0 and 100.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the low threshold.

**group-name** group_name

Assigns one or more preconfigured IP pools to the IP pool group. group_name is case sensitive and must be an alphanumeric string of 1 through 31 characters. One or more IP pool groups are assigned to a context and one IP pool group consists one or more IP pool(s).

IP pool group name is used in place of an IP pool name. When specifying a desired pool group in a configuration the IP pool with the highest precedence is used first. When that IP pool’s addresses are exhausted the pool with the next highest precedence is used.

include-nw-bcast

Includes the network and broadcast addresses for ordinary pools and NAT pools.
To remove the include-nw-bcast option from the ip pool, use the no ip pool test include-nw-bcast command.

napt-users-per-ip-address users_per_ip [ alert-threshold { { pool-free | pool-hold | pool-release | pool-used } low_thresh [ clear high_thresh ] } + ] [ max-chunks-per-user max_chunks_per_user [ nat-binding-timer nat_binding_timer ] [ nexthop-forwarding-address ip_address ] [ on-demand ] [ port-chunk-size port_chunk_size ] [ port-chunk-threshold port_chunk_threshold ] [ send-nat-binding-update ] +

**Important:** In UMTS deployments this keyword is available in 9.0 and later releases. In CDMA deployments this keyword is available in 8.3 and later releases.

**Important:** In UMTS deployments, on upgrading from Release 8.1 to Release 9.0, and in CDMA deployments, on upgrading from Release 8.1 to 8.3, all NAT realms configured in Release 8.1 using the nat-realm keyword must be reconfigured using either the nat-one-to-one (for one-to-one NAT realms) or the napt-users-per-ip-address (for many-to-one NAT realms) keywords.

Configures many-to-one NAT realms.
• **users_per_ip:** Specifies how many users can share a single NAT IP address as an integer from 2 through 2016.

• **alert-threshold:** Specifies the alert threshold for the pool:

  **Important:** Thresholds configured using the `alert-threshold` keyword are specific to the pool that they are configured in. Thresholds configured using the `threshold ip-pool-*` commands in the Context Configuration Mode apply to all IP pools in that context, and override the threshold configurations set within individual pools.

  • **pool-free:** Percentage free alert threshold for this pool
  • **pool-hold:** Percentage hold alert threshold for this pool
  • **pool-release:** Percentage released alert threshold for this pool
  • **pool-used:** Percentage used alert threshold for this pool
  • **low_thresh:** The IP pool utilization percentage that must be met or exceeded within the polling interval to generate an alert or alarm. `low_thresh` must be an integer from 0 through 100.
  • **clear high_thresh:** The IP pool utilization percentage that maintains a previously generated alarm condition. If the utilization percentage rises above the high threshold within the polling interval, a clear alarm is generated. `high_thresh` must be an integer from 0 through 100.

  **Important:** The `highthresh` value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the low threshold.

  • **max-chunks-per-user max_chunks_per_user:** Specifies the maximum number of port chunks to be allocated per subscriber in the many-to-one NAT pool. `max_chunks_per_user` must be an integer from 1 through 2016. Default: 1
  • **nat-binding-timer binding_timer:** Specifies NAT Binding Timer for the NAT pool. `binding_timer` must be an integer from 0 through 31556926. If set to 0, is disabled. Default: 0
  • **nexthop-forwarding-address address:** Specifies the nexthop forwarding address for this pool. `address` must be an IPv4 or IPv6 address. If configured for a NAT pool, packets that are NATed using that NAT pool will be routed based on the configured nexthop address.

  **Important:** The `nexthop-forwarding-address` support for NAT IP pools is functional only in later releases of Release 9.0 and in 10.0 and later releases.

  • **on-demand:** Specifies allocating IP when matching data traffic begins.
  • **port-chunk-size size:** Specifies NAT port chunk size (number of NAT ports per chunk) for many-to-one NAT pool. `size` must be an integer from 32 through 32256 (in multiples of 32).

  **Important:** The `port-chunk-size` configuration is only available for many-to-one NAT pools.

  **Important:** The `port-chunk-size` must be a minimum of 64 with systems configured as an A-BG or P-CSCF.

  • **port-chunk-threshold chunk_threshold:** Specifies NAT port chunk threshold in percentage of number of chunks for many-to-one NAT pool. `chunk_threshold` must be an integer from 1 through 100. Default: 100%
Important: The port-chunk-threshold configuration is only available for many-to-one NAT pools.

**send-nat-binding-update**: Specifies sending NAT binding updates to AAA for this realm. Default: Disabled

Important: send-nat-binding-update is supported for both one-to-one and many-to-one realms.

The following IP pool configuration keywords can also be used in the many-to-one NAT pool configuration:

*group-name group_name*: Specifies the pool group name. The grouping enables to bind discontiguous IP address blocks in individual NAT IP pools to a single pool group.

This keyword is available for NAT pool configuration only in Release 10.0 and later.

NAT pool and NAT pool group names must be unique.

*srp-activate*

Activates the IP pool for Interchassis Session Recovery (ICSR).

```
nat priority
```

Designates the IP address pool as a Network Address Translation (NAT) address pool.

*priority* specifies the priority of the NAT pool. 0 is the highest priority. If *priority* is not specified, the priority is set to 0.

Must be a value from 0 (default) to 10.

Important: This functionality is currently supported for use with systems configured as an A-BG or P-CSCF.

```
nat-one-to-one [ alert-threshold { { pool-free | pool-hold | pool-release | pool-used } low_thresh [ clear high_thresh ] } + ] [ nat-binding timer
nat_binding_timer ] [ nexthop-forwarding-address ip_address ] [ on-demand ] [ send-nat-binding-update ] +
```

Important: In UMTS deployments this keyword is available in Release 9.0 and later releases. In CDMA deployments this keyword is available in Release 8.3 and later releases.

Important: In UMTS deployments, on upgrading from Release 8.1 to Release 9.0, and in CDMA deployments, on upgrading from Release 8.1 to Release 8.3, all NAT realms configured in Release 8.1 using the *nat-realm* keyword must be reconfigured using either the *nat-one-to-one* (for one-to-one NAT realms) or the *napt-users-per-ip-address* (for many-to-one NAT realms) keywords.

```
Configures one-to-one NAT realm.
*alert-threshold*: Specifies alert threshold for this pool:

Important: Thresholds configured using the *alert-threshold* keyword are specific to the pool in which they are configured. Thresholds configured using the *thresholdip-pool* * commands in the Context Configuration Mode apply to all IP pools in the context, and override the threshold configurations set within individual pools.
**pool-free**: Percentage free alert threshold for this pool

**pool-hold**: Percentage hold alert threshold for this pool

**pool-release**: Percentage released alert threshold for this pool

**pool-used**: Percentage used alert threshold for this pool

**low_thresh**: The IP pool utilization percentage that must be met or exceeded within the polling interval to generate an alert or alarm. *low_thres* must be an integer from 0 through 100.

**clear_high_thresh**: The IP pool utilization percentage that maintains a previously generated alarm condition. If the utilization percentage rises above the high threshold within the polling interval, a clear alarm is generated. *high_thres* must be an integer from 0 through 100.

**Important**: The *high_thres* value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the low threshold.

**nat-binding-timer** *nat_binding_timer*: Specifies NAT Binding Timer for the NAT pool.

*binding_timer* must be an integer from 0 through 31556926. If set to 0, is disabled.

**Important**: For many-to-one NAT pools, the default NAT Binding Timer value is 60 seconds. For one-to-one NAT pools, it is 0. By default, the feature is disabled—the IP addresses/ port-chunks once allocated will never be freed.

**nexthop-forwarding-address** *ip_address*: Specifies the nexthop forwarding address for this pool. *address* must be an IPv4 or IPv6 address. If configured for a NAT pool, packets that are NATed using that NAT pool will be routed based on the configured nexthop address.

**Important**: The *nexthop-forwarding-address* support for NAT IP pools is functional only in later releases of Release 9.0 and in Release 10.0 and later releases.

**on-demand**: Specifies allocating IP address when matching data traffic begins.

**send-nat-binding-update**: Specifies sending NAT binding updates to AAA for this realm. Default: Disabled

**Important**: *send-nat-binding-update* is supported for both one-to-one and many-to-one realms.

The following IP pool configuration keywords can also be used in the one-to-one NAT pool configurations:

**address-hold-timer** *address_hold_timer*

**group-name** *group_name*: specifies the pool group name. The grouping enables to bind discontiguous IP address blocks in individual NAT IP pools to a single pool group. NAT pool and NAT pool group names must be unique. *group_name* is an alphanumeric string of 1 through 31 characters that is case sensitive. This keyword is available for NAT pool configuration only in StarOS 10.0 and later releases.

**srp-activate**: Activates the IP pool for Interchassis Session Recovery (ICSR).
Designates the IP address pool as a Network Address Translation (NAT) realm pool.

users-per-nat-ip-address users: specifies the number of users sharing a single NAT IP address as an integer from 1 through 5000.

on-demand: Specifies to allocate IP when matching data traffic begins.

address-hold-timer address_hold_timer: Specifies the address hold timer (in seconds) for this pool as an integer from 0 through 31556926. If set to 0, the address hold timer is disabled.

Currently, the address-hold-timer only supports IPv4 addresses.

A subscriber that is assigned an IP address from this pool is forwarded to the next hop gateway with the specified IP address.

When a nexthop forwarding address is configured, this keyword can be configured to enable over-lapping IP address pool support and associates the pool with the specified virtual LAN (VLAN). vlan_id is the identification number of a VLAN assigned to a physical port and can be configured to any integer from 1 through 4095.

For more information on configuring VLANs, refer to the System Administration Guide.

This functionality is currently supported for use with systems configured as an HA, or as a PDSN for Simple IP, or as a GGSN. This keyword can only be issued for pools of type private or static and must be associated with a different nexthop forwarding address and VLAN. A maximum of 256 over-lapping pools can be configured per context and a maximum of 256 over-lapping pools can be configured per HA or simple IPPDSN. For GGSNs, the total number of pools is limited by the number of VLANs defined but the maximum number per context is 256. Additional network considerations and configuration outside of the system maybe required.

Binds the name of a configured network reachability server to the IP pool and enables network reachability detection for the IP pool. This takes precedence over any network reachability server settings in a subscriber configuration.

server_name: Specifies the name of a network reachable server that has been defined in the current context, expressed as an alphanumeric string of 1 through 16 characters.
**Important:** Also see the following commands for more information: Refer to the `policy nw-reachability-fail` command in the HA Configuration Mode to configure the action that should be taken when network reachability fails. Refer to the `nw-reachability server` command in this chapter to configure network reachability servers. Refer to the `nw-reachability-server` command in the Subscriber Configuration Mode to bind a network reachability server to a specific subscriber.

```
respond-icmp-echo ip_address
```

Pings the first IP address from overlapping IP address pools.

**Important:** In order for this functionality to work, all of the pools should contain an initial IP address that can be pinged.

```
resource
```

Specifies this IP pool as a resource pool. The IP addresses in resource pools may have IP addresses that also exist in other resource pools. IP addresses from a resource pool should not be used for IP connectivity within the system where the pool is defined. These IP addresses should be allocated for sessions which are L3 tunneled through the system (IP-in-IP or GRE). It is possible for resource pools in the same context to have overlapping addresses when the terminating network elements for the L3 tunnels are in different VPNs.

Default: Disabled

Also refer to the `Subscriber Configuration Mode Commands` chapter for a description of the `13-to-12-tunnel-address-policy` command.

```
send-icmp-dest-unreachable
```

When enabled, this generates an ICMP destination unreachable PDU when the system receives a PDU destined for an unused address within the pool.

Default: Disabled

```
skip-nat-subscriber-ip-check
```

When enabled, this is configured to skip private IP address check for non-NAT pools. This can be configured only for non-NAT pools during call-setup if NAT is enabled for the subscriber. If NAT is disabled, this value is not considered.

Default: Disabled (subscriber IP check is done).

```
explicit-route-advertise
```

When enabled, the output of `show ip pool verbose` includes the total number of explicit host routes.

Default: Enabled

```
srp-activate
```

Activates the IP pool for Interchassis Session Recovery (ICSR).

```
subscriber-gw-address ip_address
```

Configures the subscriber gateway address for this pool.

```
suppress-switchover-arp
```

Suppress corresponding gratuitous ARP generation when a line card or MIO card switchover occurs. Default: Disabled
unicast-gratuitous-arp-address  ip_address
Perform a unicast gratuitous ARP to the specified IP address rather than broadcast gratuitous ARP when gratuitous ARP generation is required. Default: Perform broadcast gratuitous ARP.

vrf  vrf_name { [ mpls-label input in_label_value | output out_label_value1 [ out_label_value2 ] ] }
Associates a preconfigured Virtual Routing and Forwarding (VRF) instance with this IP pool and configures MPLS label parameters.

**Important:** This command must be used with next-hop parameters.

vrf name is name of a preconfigured virtual routing and forwarding (VRF) context configured in Context Configuration Mode through `ip vrf` command.
- `in_label_value` is the MPLS label that identifies the inbound traffic destined for this pool.
- `out_label_value1` and `out_label_value2` identify the MPLS labels to be added to the outgoing packets sent for subscribers from this pool. Where `out_label_value1` is the inner output label and `out_label_value2` is the outer output label.

MPLS label values must be an integer from 16 through 1048575.
By default, the pools configured are bound to the default VRF unless specified with a VRF name.

**Important:** You cannot have overlapping pool addresses using the same VRF. Also you cannot have two pools using different VRFs but the same in-label irrespective of whether or not the pools overlap. The pool must be private or static in-order to be associated with a certain VRF. If the VRF with such a name is not configured, you are prompted to add the VRF before configuring a pool.

policy allow-static-allocation
Configures static address allocation policy for dynamic IP pool. This keyword enables a dynamic IP pool to accept a static address for allocation.

**Important:** In static allocation scenario, the pool group name is returned by AAA in the attribute **SN1-IP-Pool-Name**, and the IP address to use will be returned in the **Framed-IP-Address** attribute.

framed-route-vrf-list vrf_list_name
Configures a vrf-list in order for NVSE VRF authorization.

pool-route  ip_address/ip_mask
Configures the IP pool route instead of generating by-default. The address followed by the `pool-route` keyword can be an IPv4 or IPv6 address with the mask value.

+ Indicates that more than one of the previous keywords can be entered within a single command.
Usage

Define one or more pools of IP addresses for the context to use in assigning IPs to mobile stations. This command is also useful in resizing existing IP pools to expand or contract the number of addresses allocated. If you resize an IP pool, the change is effective immediately.

When using the `ip pool` command to resize an IP pool, the type must be specified since by default the command assumes the type as public. In other words, the CLI syntax to resize an IP pool is the same syntax used to create the pool. See examples below.

```
ip pool pool1 100.1.1.0/24 static
```

The syntax to resize that pool would be:

```
ip pool pool1 100.1.1.0/25 static
```

A pool which is deleted will be marked as such. No new IP addresses will be assigned from a deleted pool. Once all assigned IP addresses from a deleted pool have been released, the pool, and all associated resources, are freed.

**Important:** If an IP address pool is matched to a ISAKMP crypto map and is resized, removed, or added, the corresponding security association must be cleared in order for the change to take effect. Refer to the `clear crypto` command in the Exec mode for information on clearing security associations.

Over-lapping IP Pools: The system supports the configuration of over-lapping IP address pools within a particular context. Over-lapping pools are configured using either the resource or overlap keywords. The `resource` keyword allows over-lapping addresses tunneled to different VPN end points.

The `overlap` keyword allows over-lapping addresses each associated with a specific virtual LAN (VLAN) configured for an egress port. It uses the VLAN ID and the nexthop address to determine how to forward subscriber traffic with addresses from the pool thus resolving any conflicts with overlapping addresses.

Note that if an overlapping IP Pool is bound to an IPSec Tunnel (refer to the `match ip pool` command in the Crypto Group Configuration Mode chapter), that tunnel carries the traffic ignoring the nexthop configuration. Therefore, the IPSec Tunnel takes precedence over the nexthop configuration. (Thus, one can configure the overlapping IP Pool with fake VLAN ID and nexthop and still be able to bind it to an IPSec Tunnel for successful operation. The `overlap` keyword allows over-lapping addresses each associated with a specific VLAN can only be issued for pools of type private or static and must be associated with a different nexthop forwarding address and VLAN. A maximum of 128 over-lapping pools can be configured per context and a maximum of 256 over-lapping pools can be configured per system.

**Important:** Overlapping IP address functionality is currently supported for use with systems configured as an HA for Mobile IP, or as a PDSN for Simple IP, or as a GGSN. For deployments in which subscriber traffic is tunneled from the FA to the HA using IP-in-IP, a separate HA service must be configured for each over-lapping pool.

IP Pool Address Assignment Method: IP addresses can be dynamically assigned from a single pool or from a group of pools. The addresses are placed into a queue in each pool. An address is assigned from the head of the queue and, when released, returned to the end. This method is known as least recently used (LRU).

When a group of pools have the same priority, an algorithm is used to determine a probability for each pool based on the number of available addresses, then a pool is chosen based on the probability. This method, over time, allocates addresses evenly from the group of pools.
**Important:** Note that setting different priorities on each individual pool in a group can cause addresses in some pools to be used more frequently.

**Important:** In NAT IP pool configurations, the minimum number of public IP addresses that must be allocated to each NAT pool must be greater than or equal to the number of Session Managers (SessMgrs) available on the system. On the ASR 5000, it is $\geq 84$ public IP addresses. This can be met by a range of 84 host addresses from a single Class C. The remaining space from the Class C can be used for other allocations.

**Example**

The following commands define a private IP address pool, a public IP address pool, and a static address pool, respectively.

```
  ip pool samplePool1 1.2.3.0 255.255.255.0 private
  ip pool samplePool2 1.3.0.0 255.255.0.0 public
  ip pool samplePool3 1.4.5.0 255.255.255.0 static
```

The following command defines a private IP pool specified with a range of IP addresses. The pool has 101 addresses.

```
ip pool samplePool4 range 10.5.5.0 10.5.5.100 private
```

The following command sets the address hold timer on the pool to 60 minutes ($3600$ seconds):

```
ip pool samplePool4 address-hold-timer 3600
```

The following command removes the IP address pool from the configuration:

```
  no ip pool samplePool1
```

The following command creates a static IP pool:

```
ip pool pool1 100.1.1.0/24 static
```

The following command resizes the static IP pool created in the previous example:

```
ip pool pool1 100.1.1.0/25 static
```
ip prefix-list

Creates an IP prefix list for filtering routes.

Product
PDSN
HA
GGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration
configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

ip prefix-list name list_name [ seq seq_number ] { deny | permit } { any | network_address/net_mask [ ge ge_value ] [ le le_value ]

no ip prefix-list list_name [ seq seq_number ] { deny | permit } { any | network_address/net_mask [ ge ge_value ] [ le le_value ]

no
Delete the specified prefix-list entry.

ame list_name
Specifies a name for the prefix list as an alphanumeric string of 1 through 79 characters.

seq seq_number
Assigns the specified sequence number to the prefix list entry as an integer from 1 through 4294967295.

deny
Specifies prefixes to deny.

permit
Specifies prefixes to permit.

any
Matches any prefix.

network_address/net_mask [ ge ge_value ] [ le le_value ]
Specifies the prefix to match.
network_address/net_mask: the IP address and the length, in bits, of the network mask that defines the prefix. The IP address and mask must be entered in IPv4 dotted-decimal notation. When neither ge (greater than or equal to) or le (less than or equal to) are specified an exact match is assumed.

ge ge_value: Specifies the minimum prefix length to match as an integer from 0 through 32. If only the ge value is specified, the range is from the ge value to 32. The ge value must be greater than net_mask and less than the le value.

le le_value: Specifies the maximum prefix length to match as an integer from 0 through 32. If only the le value is specified, the range is from the net_mask to the le value. The le value must be less than or equal to 32.

The following equation describes the conditions that ge and le values must satisfy:

\[ \text{net_mask} < \text{ge_value} < \text{le_value} \leq 32 \]

Usage

Use this command to filter routes by their IP prefix.

Example

```
ip prefix-list name prelist10 seq 5 permit 192.168.100.0/8 ge 12 le 24
```
ip prefix-list sequence-number

Enables or disables the inclusion of IP prefix list sequence numbers in the configuration file. This option is enabled by default.

Product

PDSN
HA
GGSN

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > Context Configuration
configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name] host_name(config-ctx)#

Syntax

[ no ] ip prefix-list sequence-number

no

Disables the listing of IP prefix list sequence numbers in the configuration file.

Usage

Use this command to enable and disable the inclusion of IP prefix list sequence numbers in the configuration file.

Example

To disable the inclusion of IP prefix list sequence numbers in the configuration file, enter the following command:

    no ip prefix-list sequence-number
**ip route**

Adds or removes routing information from the current context’s configuration.

**Product**
All

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration

configure > context context_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
[ no ] ip route { ip_address/ip_mask | ip_address ip_mask } { gateway_ip_address | next-hop next_hop_ip_address | point-to-point | tunnel } egress_intrf_name [ cost cost ] [ precedence precedence ] [ vrf vrf_name [ cost value ] [ precedence precedence ] ]

[ no ] ip route static bfd if_name remote-endpt_ipv4_address
```

**no**

Indicates the route specified by this options is to be removed from the configuration.

**ip_address/ip_mask | ip_address/ip_mask**

Specifies a destination IP address or group of addresses that will use this route.

**ip_address/ip_mask:** Specifies a combined IP address subnet mask bits to indicate what IP addresses to which the route applies. *ip_address* must be entered using IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation. *ip_mask* is entered using CIDR notation; the mask bits are a numeric value which is the number of bits in the subnet mask.

**ip_address/ip_mask:** Specifies an IP address and the networking (subnet) mask pair which is used to identify the set of IP addresses to which the route applies. *ip_address* must be specified using the standard IPv4 dotted decimal notation as network mask for subnets.

The mask as specified by *ip_mask* or resulting from *ip_address/ip_mask* is used to determine the network for packet routing.

0’s in the resulting mask indicate the corresponding bit in the IP address is not significant in determining the network for packet routing.

1’s in the resulting mask indicate the corresponding bit in the IP address is significant in determining the network.

**gateway_ip_address | next-hop next_hop_ip_address | point-to-point | tunnel**

Specifies which device or network to use when forwarding packets.

**gateway_ip_address:** Specifies the IP address of the network gateway to which to forward packets. The address must be entered in IPv4 dotted-decimal notation (###.###.###.###).
**next-hop next_hop_ip_address**: Specifies the next-hop IP address to which packets are to be forwarded. The address must be entered in IPv4 dotted-decimal notation.

**point-to-point**: Specifies that the egress port is an ATM point-to-point interface.

**tunnel**: Sets the static route for this egress interface as tunnel type, such as IPv6-over-IPv4 or GRE.

**egress_intrfc_name**: Specifies the name of the egress (out-bound) interface name in the current context as an alphanumeric string of 1 through 79 characters.

**cost**: Specifies the relative cost of the route. **cost** must be an integer from 0 through 255 where 255 is the most expensive. Default: 0

**precedence**: Specifies the selection order precedence for this routing information. **precedence** must be an integer from 1 through 254 where 1 is the highest precedence. Default: 1

**vrf vrf_name**: Associates a Virtual Routing and Forwarding (VRF) context with this static route configuration. **vrf_name** is the name of a preconfigured VRF context configured in **Context Configuration Mode** via the **ip vrf** command.

**static bfd if_name remote-endpt_ipv4_address**: Creates a static IP route that will be associated with Bidirectional Forwarding Detection (BFD). For additional information, see the **BFD Configuration Mode Commands** chapter. **if_name**: Specifies the name of the interface to which the static BFD neighbor is bound as an alphanumeric string of 1 through 79 characters. **remote_endpt_ipv4_address**: Specifies the gateway address of the BFD neighbor in IPv4 dotted-decimal notation.

**Usage**

Use this command to configure IP route parameters, precedence and cost options for the route selections such that routes of the same precedence are grouped together then lowest cost is selected first. This results in route’s being selected first by lower precedence then the cost is used if multiple route’s are defined with the same precedence. This command also configures static IP routes when implementing Bidirectional Forwarding Detection (BFD).

**Important**: A maximum of 1,200 static routes may be configured per context.

**Example**

Virtual Routing and Forwarding (VRF) context can be associated with static IP route for BGP/MPLS, GRE, or IPSec tunnel support.

The following command adds a route using the combined IP address and subnet mask form:

```
ip route 10.2.3.0/32 192.168.1.2 egressSample1 precedence 160
```
The following configures route options for a route specified using the distinct IP address and subnet mask form:

```
ip route 10.2.3.4 255.224.0.0 10.1.2.3 egressSample2 cost 43
```

The following deletes the two routes configured above:

```
no ip route 10.2.3.0/32 192.168.1.2 egressSample1 precedence 160
no ip route 10.2.3.4 255.224.0.0 10.1.2.3 egressSample2 cost 43
```

The following command adds a route using the combined IP address and subnet mask form and specifies the egress interface as tunnel type:

```
ip route 10.2.3.0/32 tunnel egressSample1 precedence 160 vrf vrf1
```
ip routing maximum-paths

Enables Equal Cost Multiple Path (ECMP) routing support and specifies the maximum number of ECMP paths that can be submitted by a routing protocol in the current context.

**Product**
All products that support Cost Multiple Path (CMP)

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration
```
configure > context context_name
```
Entering the above command sequence results in the following prompt:
```
[context_name]host_name(config-ctx)#
```

**Syntax**
```
ip routing maximum-paths [ max_num ]

[ default | no ] ip routing maximum-paths
```

- **default**
  Resets the command to its default setting of 4.

- **max_num**
  The maximum number of ECMP paths that can be submitted by a routing protocol. `max_num` must be an integer from 1 through 10 (releases prior to 18.2) or 1 through 32 (release 18.2+). Default: 4

- **no**
  Disables ECMP for the current context.

**Usage**
Use this command to enable ECMP for routing and set the maximum number of ECMP paths that can be submitted by a routing protocol.

**Example**
To enable ECMP and set the maximum number of paths that may be submitted by a routing protocol in the current context to 10, enter the following command:

```
ip routing maximum-paths 10
```

To disable ECMP in the current context, enter the following command:

```
no ip routing maximum-paths
```
ip routing overlap-pool

Configures the routing behavior for overlap-pool addresses.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration

```
configure > context context_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
[ no | default ] ip routing overlap-pool
```

---

**default**
Resets the command to its default setting of disabled.

---

**no**
Disables the routing behavior for overlap-pool addresses for the current context.

**Usage**

Use this command configuration to advertise overlap-pool addresses in dynamic routing protocols when overlap pools are configured using vlan-ids. If the "ip routing overlap-pool" is configured, then the overlap-addresses are added as interface addresses and advertised.
**ip vrf**

Creates a Virtual Routing and Forwarding (VRF) context instance, assigns a VRF identifier, and configures the VRF parameters for BGP/MPLS VPN, GRE tunnel, and IPSec interface configuration.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration
`configure > context context_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
ip vrf vrf_name
no ip vrf
```

- **no**
  Disables IP Virtual Routing and Forwarding (VRF) parameters.

  - **vrf_name**
    Specifies the name of the virtual routing and forwarding interface as an alphanumeric string of 1 through 63 characters.

**Usage**

Use this command to create a VRF context and assign a VRF identifier for BGP/MPLS VPN, IPSec, GRE tunnel configuration in this context instance. This command is used when the system works as a BGP router with MPLS VPN and binds an MPLS VPN to the system or to facilitate GRE or IPSec tunnelling. The addresses assigned to this interface are visible in the VRF routing table.

This command switches the command mode to IP VRF Context Configuration Mode:

```
[context_name>]>host_name(config-context-vrf)#
```

If required, this command creates an IP VRF Context Configuration Mode instance.

When using this command please note of the following:

- A VRF context instance must be created and configured before referring, associating, or binding the same with any command or mode.

- If the interface binding to a VRF context instance is changed or any IP address assigned to the interface is deleted, a warning is displayed.

- All interfaces bound with a VRF context instance will be deleted when that VRF is removed/deleted.

- An interface can be bound to only one VRF context instance.
A maximum of 100 VRF context instances can be configured on a system.

Refer to the *IP VRF Context Configuration Mode Commands* chapter for parameter configuration.

**Example**

The following command configures the virtual routing and forwarding context instance `vrf1` in a context:

```
ip vrf vrf1
```
ip vrf-list

Creates a VRF list and adds VRFs to the list. The VRFs must have been previously created via the `ip vrf` command.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration

`configure > context context_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cxt)#
```

**Syntax**

```
ip vrf-list list_name [permit vrf_name]
no ip vrf-list list_name [permit vrf_name]
```

- **no**
  
  Deletes a VRF list or delete VRFs from this list. If `permit` and `vrf-name` are not specified, the entire list of VRFs is deleted. Otherwise, the specified VRF(s) is deleted from the list.

- **list_name**
  
  Specifies the name of the VRF list as an alphanumerical string of 1 through 63 characters.

- **vrf_name**
  
  Specifies the name of the virtual routing and forwarding interface as an alphanumeric string of 1 through 63 characters.

**Usage**

Create a VRF list and add VRFs to the list. The VRFs must have been previously created via the `ip vrf` command. This command supports multiple VRFs over NEMO.

**Example**

The following command creates a VRF list named `corp103` and adds a VRF named `vrf3567`:

```
ip vrf-list corp103 permit vrf3567
```
**ipms**

Enables/disables/manages an intelligent packet monitoring system (IPMS) client service and enters the IPMS Client Configuration Mode within the current context.

**Product**

IPMS

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration

`configure > context context_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
[ no ] ipms [ -noconfirm ]
```

- **no**
  Deletes a previously configured IPMS client service.

- **-noconfirm**
  Executes the command without any additional prompt and confirmation from the user.

**Caution:** If this keyword option is used with `no ipms` command, the IPMS client service will be deleted with all active/inactive IPMS sessions without prompting any warning or confirmation.

**Usage**

Use this command to enable/disable/manage the IPMS client service within a context and configure certain functionality. This command enables and allows the configuration of service enabling the system to function as an IPMS-enabled Access Gateway in a network. This command is also used to remove previously configured IPMS client service.

A maximum of 1 IPMS client can be configured per system.

**Important:** The IPMS is a license enabled external application support. Refer to the *IPMS Installation and Administration Guide* for more information on this product.

**Example**

Refer to the *IPMS Installation and Administration Guide* and *IPMS Configuration Mode* chapter of this reference for additional information.

The following command creates an IPMS client service name within the context:

```
ipms
```
ipsec replay

Configures IKEv2 IPSec specific anti-replay.

Product
- ePDG
- PDIF
- SCM

Privilege
- Security Administrator, Administrator

Mode
- Exec > Global Configuration > Context Configuration
  - configure > context context_name

Syntax
```
[ no ] ipsec replay [ window-size window_size ]
```

- no
  - Disables this option.

replay
Confuges IKEv2 IPSec anti-replay.

window-size window_size
Confuges anti-replay window size.

Usage
Use this command to configure IKEv2 IPSec specific anti-replay.

Example
The following command sets the window size to 256:

  ipsec replay window-size 256
**ipsec transform-set**

Creates a new or specifies an existing IPSec transform set and enters the IPSec Transform Set Configuration Mode for the current context.

**Product**
- ePDG
- PDIF
- SCM

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration > Context Configuration
- configure > context context_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
[ no ] ipsec transform-set transform_set_name
```

- **no**
  - Removes an existing transform set from the system.

- **transform-set name**
  - Specifies the name of a new or existing transform set as an alphanumerical string of 1 through 127 characters.

**Usage**

Use this command to Configure IKEv2 IPsec child security association transform set parameters. Up to four transform-sets can be created.

Entering this command results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

This command applies to IKEv2. Please check `crypto ipsec transform-set` command for ipsec transform-set configuration for IKEv1.

**Example**

The following command configures an IPSec transform set called `ipsec12` and enters the IPSec Transform Set Configuration Mode:

```
ipsec transform-set ipsec12
```
ipsg-service

This command allows you to create/modify/delete an IP Services Gateway (IPSG) service in the current context.

**Product**
- eWAG
- IPSG

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration

`configure > context context_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
ipsg-service ipsg_service_name [ mode { radius-server [ ewag ] | radius-snoop } ] [ -noconfirm ]
```

```
no ipsg-service ipsg_service_name [ mode { radius-server [ ewag ] | radius-snoop } ]
```

- **ipsg_service_name**
  Specifies the name of the IPSG service.
  `ipsg_service_name` must be an alphanumeric string of 1 through 63 characters.

- **mode { radius-server [ ewag ] | radius-snoop }**
  Configures the IPSG to perform as either a RADIUS server or as a device to extract user information from RADIUS accounting request messages (snoop). If the optional keyword `mode` is not entered, the system defaults to `radius-server`.
    - **radius-server**: Creates the named IPSG RADIUS Server service in the current context and/or enters the IPSG RADIUS Server Configuration Mode.
    - **radius-server ewag**: Enables the eWAG service (IPSG service in eWAG mode), and enters the IPSG RADIUS Server Configuration Mode, which is common for the eWAG and IPSG services.
    - **radius-snoop**: Creates the named IPSG RADIUS Snoop service in the current context and/or enters the IPSG RADIUS Snoop Configuration Mode.

- **-noconfirm**
  Specifies to execute the command without additional prompt or confirmation.

**Important:** Service names must be unique across all contexts within a chassis.
Usage

Use this command to create/configure/delete an IPSG service.
A maximum of one IPSG service can be configured per context.
IPSG service commands are defined in the IPSG RADIUS Snoop Configuration Mode Commands chapter and
the IPSG RADIUS Server Configuration Mode Commands chapters.
A maximum of 256 services (regardless of type) can be configured per system.

⚠️ Caution: A large number of services greatly increases the complexity of system management and may impact
overall system performance (i.e., resulting from system handoffs). Do not configure a large number of services unless
your application requires it. Contact your Cisco account representative for more information.

⚠️ Important: IP Services Gateway functionality is a license-controlled feature. A valid feature license must be
installed prior to configuring an IPSG service. Contact your Cisco account representative for more information.

Example

On entering the command with the radius-server mode or without any mode, the CLI prompt changes to:

```
[context_name]hostname(config-ipsg-service-radius-server)#
```

On entering the command with the radius-snoop mode, the CLI prompt changes to:

```
[context_name]hostname(config-ipsg-service-radius-snoop)#
```

For more information about the IP Services Gateway, refer to the IP Services Gateway Administration Guide.

The following command configures an IPSG RADIUS Snoop service named ipsg1 and enters the IPSG
RADIUS Snoop Configuration Mode:

```
ipsg-service ipsg1 mode radius-snoop
```

The following command enables the eWAG service (IPSG service in eWAG mode), and enters the IPSG
RADIUS Server Configuration Mode, which is common for the eWAG and IPSG services:

```
ipsg-service ipsg2 mode radius-server ewag
```
### ipv6 access-group

Configures the IPv6 Access group.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration

```bash
configure > context context_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
ipv6 access-group group name { priority_value }
```

- **group_name**
  Specifies the name of the access group as an alphanumeric string of 1 through 79 characters.

- **priority_value**
  Specifies the priority of the access group. 0 is the highest priority. If `priority_value` is not specified the priority is set to 0. `priority_value` must be an integer from 0 through 4294967295. Default: 0
  If access groups in the list have the same priority, the last one entered is used first.

**Usage**

Use this command to specify IPv6 access group name and priority. Use a lower value to indicate a higher priority for the group.

**Example**

```
ipv6 access-group group_1
```
**ipv6 access-list**

Configures access list (or packet filter) name and enters the IPv6 ACL Configuration Mode.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration

```
configure > context context_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
[ no ] ipv6 access-list name
```

- **no**
  Indicates the access list specified is to be removed from the configuration.

- **name**
  Specifies the access list for which to enter the IPv6 ACL Configuration Mode or the list to remove. *name* is an alphanumeric string of 1 through 79 characters.

**Usage**

Executing this command enters the IPv6 ACL Configuration Mode in which rules and criteria are defined for the ACL.

**Example**

```
ipv6 access-list samplelist

no ipv6 access-list samplelist
```
ipv6 dns-proxy

Configures the domain name server proxy for the context.

Product
PDSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration

configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

[ no ] ipv6 dns-proxy source-ipv4-address ip_address

no

Removes the predefined IP address for local interface in the destination context.

ip_address

Specifies the IPv4 address of one of the local interface in the destination context to configure the IPv6 DNS proxy where ip_address must be specified using IPv4 dotted-decimal notation.

Usage

The IPv6 DNS proxy source IPv4 address is used as the source IP address for the DNS proxy transaction.

Example

The following command provides an example of configuring a IPv6 DNS proxy of 192.168.23.1:

ipv6 dns-proxy source-ipv4-address 192.168.23.1
ipv6 neighbor

Adds a static IPv6 neighbor entry into the neighbor discovery table.

**Product**
PDIF

**Privilege**
Administrator, Security Administrator

**Mode**
Exec > Global Configuration > Context Configuration
configure > context context_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
[ no ] ipv6 neighbor ipv6_address hardware_address
```

- **no**
  - Removes the specified address.

```
ipv6_address hardware_address
```

- *ipv6_address* is the IP address of node to be added to the table.
- *hardware_address* is the associated 48-bit MAC address.

**Usage**
Add a static IPv6 neighbor entry into the neighbor discovery table.

**Important:** On the ASR 5000, routes with IPv6 prefix lengths less than /12 and between the range of /64 and /128 are not supported.

**Example**
Add the ipv6 address *fe80::210:83ff:feff:7a9d::/24* and associated 48 bit MAC address *0:10:83:f7:7a:9d* to the table.

```
ipv6 neighbor fe80::210:83ff:feff:7a9d::/24 0:10:83:f7:7a:9d
```
ipv6 pool

Modifies the current context’s IP address pools by adding, updating or deleting a pool. This command also resizes an existing IP pool.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration
configure > context context_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
ipv6 pool name [ 6to4 local-endpoint ipv4_address [ default-relay-router router_address ] ]
| alert threshold | group-name name | policy { allow-static-allocation | dup-addr-detection } | prefix ip_address/len [ 6to4-tunnel local-endpoint ip_address | default-relay-router router_address ] | range start_address end_address | suppress-switchover-arps ] | [ prefix-length prfx_length ] | [ private priority ] | [ public priority ] | [ shared priority ] | [ static priority ] | [ group-name name ] | [ vrf vrf-name ]

no ipv6 pool name
```

**no**
Deletes the previously configured IPv6 pool.

**name**
Specifies the logical name of the IP address pool as an alphanumeric string of 1 through 31 characters.

**6to4-tunnel local-endpoint ip_address**
Specifies the IPv4 address of the local interface to be used for IPv6-to-IPv4 compatible pool address construction.

```
alert threshold { 6to4 local-endpoint ipv4_address | alert threshold | group-available | group-name name | policy { allow-static-allocation | dup-addr-detection } | pool-free | pool-used | prefix | range start_address end_address }
```

Default: All thresholds are disabled.

Configures IP address pool-level utilization thresholds. These thresholds take precedence over context-level IPv6 pool thresholds.

- **6to4**: Sets an alert based on the IPv6 Pool for an IPv6-to-IPv4 compatible address type.
- **alert-threshold**: Sets an alert based on the percentage free alert threshold for this group.
- **group-available**: Sets an alert based on the percentage free alert threshold for this group.
- **group-name**: Sets an alert based on the IPv6 Pool Group.
• **policy allow-static-allocation**: Sets an alert based on the address allocation policy.

• **pool-free**: Sets an alert based on the percentage free alert threshold for this pool.

• **pool-used**: Sets an alert based on the percentage used alert threshold for this pool.

• **prefix**: Sets an alert based on the IPv6 Pool address prefix.

• **range**: Sets an alert based on the IPv6 address pool range of addresses.

• **suppress-switchover-arps**: Sets an alert based on the Suppress Gratuitous ARPs when performing a line card or an MIO switchover.

---

```
 IPv6 Pool Group.
The following options are available:

• **6to4**: IPv6 Pool for IPv6-to-IPv4 compatible address type

• **alert-threshold**: Percentage free alert threshold for this group

• **group-name**: IPv6 Pool Group

• **policy**: Configure an address allocation policy

• **prefix**: IPv6 Pool address prefix

• **range**: Configures IPv6 address pool to use a range of addresses

• **supress-switchover-arps**: Suppress gratuitous ARPs when performing a line card or an MIO switchover.

---

```

```ipv4_address```
Specifies the beginning IPv4 address of the IPv4 address pool. `ipv4_address` must be specified using IPv4 dotted-decimal notation.

---

```default-relay-router router address```
Specifies the default relay router for the tunnel.

---

**policy allow-static-allocation**
Allows a dynamic pool to accept a static address allocation.
The following options are available:

• **6to4**: IPv6 Pool for IPv6-to-IPv4 compatible address type

• **alert-threshold**: Percentage free alert threshold for this group

• **group-name**: IPv6 Pool Group

• **policy**: Configure an address allocation policy

• **prefix**: IPv6 Pool address prefix

• **range**: Configures IPv6 address pool to use a range of addresses

• **suppress-switchover-arps**: Suppress gratuitous ARPs when performing a line card or an MIO switchover

---

**policy dup-addr-detection**
This command is valid for IPv6 shared pools only (Sample syntax: `ipv6 pool name prefix ip_address/len shared policy dup-addr-detection`). When this policy is enabled, the IPv6 shared
pool allows a prefix to be shared in different call sessions with different interface IDs for an IPv6 address. This allows the tracking of interface IDs per prefix and the detection of duplicate IDs. With this policy disabled, the IPv6 shared pool will allow a prefix to be shared across different call sessions. The interface ID is not considered for any duplicate address detection. Default: Disabled

The following options are available:

- **6to4**: IPv6 pool for IPv6-to-IPv4 compatible address type
- **alert-threshold**: Percentage free alert threshold for this group
- **group-name**: IPv6 pool group
- **policy**: Configure an address allocation policy
- **prefix**: IPv6 pool address prefix
- **range**: Configures IPv6 address pool to use a range of addresses
- **suppress-switchover-arps**: Suppress gratuitous ARPs when performing a line card or an MIO switchover

**prefix ip_address/len**

Specifies the beginning IPv6 address of the IPv6 address pool. `ip_address/len` must be specified using IPv6 colon-separated-hexadecimal. `len` is an integer that indicates the number bits of prefix length.

**Important**: On the ASR 5000, routes with IPv6 prefix lengths less than /12 and between the range of /64 and /128 are not supported.

**range start_address end_address**

Configures an IPv6 address pool to use a range of addresses.

`start_address` specifies the beginning of the range of addresses for the IPv6 pool. It must be specified using IPv6 colon-separated-hexadecimal notation.

`end_address` specifies the end of the range of addresses for the IPv6 pool. It must be specified using IPv6 colon-separated-hexadecimal notation.

**suppress-switchover-arps**

Suppresses gratuitous ARPs when performing a line card switchover.

The following options are available:

- **6to4**: IPv6 Pool for IPv6-to-IPv4 compatible address type
- **alert-threshold**: Percentage free alert threshold for this group
- **group-name**: IPv6 Pool Group
- **policy**: Configure an address allocation policy
- **prefix**: IPv6 Pool address prefix
- **range**: Configures IPv6 address pool to use a range of addresses
- **suppress-switchover-arps**: Suppress gratuitous ARPs when performing a line card or an MIO switchover

**prefix-length prfx_length**

Specifies a configured length of prefixes. `prfx_length` can be 48, 52, 56 or 64 bits of prefix (Default = 64). This option supports S-GW/P-GW validation of fixed-length addresses via DHCPv6 (TS 29.274 – 7.2.2 and 8.14).
On the ASR 5000, routes with IPv6 prefix lengths less than /12 and between the range of /64 and /128 are not supported.

```
private priority | public priority | shared priority | static priority
```

Default: public

**private priority:** Specifies that the address pool may only be used by mobile stations which have requested an IP address from a specified pool. When private pools are part of an IP pool group, they are used in a priority order according to the precedence setting. `priority` must be an integer from 0 through 10 with 0 being the highest. The default is 0.

**public priority:** Specifies that the address pool is used in priority order for assigning IP addresses to mobile stations which have not requested a specific address pool. `priority` must be an integer from 0 through 10 with 0 being the highest and with a default of 0.

**shared priority:** Specifies that the address pool that may be used by more than one session at any time. `priority` must be an integer from 0 through 10 with 0 being the highest and with a default of 0.

**static priority:** Specifies that the address pool is used for statically assigned mobile stations. Statically assigned mobile stations are those with a fixed IP address at all times. `priority` must be an integer from 0 through 10 with 0 being the highest and with a default of 0.

```
group-name name
```

Groups the IPv6 pools into different groups. The subscribers/domain can be configured with the group-name instead of the prefix-pool names. `name` is the name of the group by which the IPv6 pool is to be configured expressed as an alphanumeric string of 1 through 79 characters.

```
vrf vrf-name
```

Associates the pool with the VRF specified as an alphanumeric string of 1 through 63 characters. By default the configured IPv6 pool will be associated with the global routing domain.

**Usage**

Use this command to modify the current context’s IP address pools by adding, updating or deleting a pool. Also use this command to resize an existing IP pool.

**Example**

The following command adds an IPv6 pool named `ip6Star`:

```
ipv6 pool ip6Star
```
ipv6 prefix-list

Creates an IPv6 prefix list for filtering routes.

**Product**
PDSN
HA
GGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration
configure > context context_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
ipv6 prefix-list name list_name [ seq seq_number ] { deny | permit } { any | network_address/net_mask [ ge ge_value ] [ le le_value ] }

no ipv6 prefix-list list_name [ seq seq_number ] { deny | permit } { any | network_address/net_mask [ ge ge_value ] [ le le_value ] }
```

**no**
Delete the specified prefix-list entry.

**name list_name**
Specifies a name for the prefix list as an alphanumeric string of 1 through 79 characters.

**seq seq_number**
Assigns the specified sequence number to the prefix list entry as an integer from 1 through 4294967295.

**deny**
Specifies prefixes to deny.

**permit**
Specifies prefixes to permit.

**any**
Matches any prefix.

```
network_address/net_mask [ ge ge_value ] [ le le_value ]
```
Specifies the prefix to match.
network_address/net_mask: the IPv6 address and the length, in bits, of the network mask that defines the prefix. The IP address and mask must be entered in IPv6 colon-separated-hexadecimal notation. When neither ge (greater than or equal to) or le (less than or equal to) are specified an exact match is assumed.

**Important:** On the ASR 5000, routes with IPv6 prefix lengths less than /12 and between the range of /64 and /128 are not supported.

ge ge_value: Specifies the minimum prefix length to match as an integer from 0 through 128. If only the ge value is specified, the range is from the ge value to 128. The ge value must be greater than net_mask and less than the le value.

le le_value: Specifies the maximum prefix length to match as an integer from 0 through 128. If only the le value is specified, the range is from the net_mask to the le value. The le value must be less than or equal to 128.

The following equation describes the conditions that ge and le values must satisfy:

net_mask < ge_value < le_value <= 128

**Usage**

Use this command to filter routes by their IPv6 prefix.

**Example**

```
ipv6 prefix-list name prelistv6-10 seq 5 permit 2002::123.45.67.89/32
```
ipv6 prefix-list sequence-number

Enables or disables the inclusion of IPv6 prefix list sequence numbers in the configuration file. This option is enabled by default.

Product
PDSN
HA
GGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration
configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

[ no ] ipv6 prefix-list sequence-number

no

Disables the listing of IPv6 prefix list sequence numbers in the configuration file.

Usage
Use this command to enable and disable the inclusion of IPv6 prefix list sequence numbers in the configuration file.

Example
To disable the inclusion of IPv6 prefix list sequence numbers in the configuration file, enter the following command:

no ipv6 prefix-list sequence-number
**ipv6 route**

Configures a static IPv6 route to the next-hop router.

**Product**

All

**Privilege**

Administrator

**Mode**

Exec > Global Configuration > Context Configuration

`configure > context context_name`

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-ctx)#`

**Syntax**

```
[ no ] ipv6 route ipv6_address/prefix_length { interface name | next-hop ipv6_address interface name } [ cost cost ] [ precedence precedence ] [ vrf vrf_name [ cost value ] [ precedence precedence ] ]
```

```
[ no ] ipv6 route static bfd if_name remote-endpt_ipv6address
```

**no**

Removes the specified static route.

---

`ipv6_address/prefix_length`

Specifies a destination IPv6 address or group of addresses that will use this route. `ipv6_address/prefix_length` must be specified using IPv6 colon-separated-hexadecimal with CIDR notation.

**Important:** On the ASR 5000, routes with IPv6 prefix lengths less than /12 and between the range of /64 and /128 are not supported.

---

`interface name`

Specifies the name of the interface on this system associated with the specified route or next-hop address. `name` must be an existing interface name on the system expressed as an alphanumeric string of 1 through 79 characters.

---

`next-hop ipv6_address`

The IPv6 address of the directly connected next hop device in IPv6 colon-separated-hexadecimal notation.

---

`cost cost`

Defines the number of hops to the next gateway as an integer from 0 through 255. Default: 0
precedence  
Indicates the administrative preference of the route. A low precedence specifies that this route takes preference over the route with a higher precedence. precedence must be an integer from 1 through 254. Default: 1

vrf  
Associates a Virtual Routing and Forwarding (VRF) context with this static route configuration. 
vrf_name is the name of a preconfigured VRF context configured in Context Configuration Mode via the ip vrf command.

static bfd if_name remote-endpt_ipv6address  
Creates a static IP route that will be associated with Bidirectional Forwarding Detection (BFD). For additional information, see the BFD Configuration Mode Commands chapter.  
if_name: Specifies the name of the interface to which the static BFD neighbor is bound as an alphanumeric string of 1 through 79 characters.  
remote_endpt_ipv6address: Specifies the gateway address of the BFD neighbor in IPv6 colon-separated-hexadecimal notation.

Usage  
Use this command to configure IPv6 route parameters, precedence and cost options for the route selections such that routes of the same precedence are grouped together then lowest cost is selected first. This results in route’s being selected first by lower precedence then the cost is used if multiple route’s are defined with the same precedence.  
This command also configures static IP routes when implementing Bidirectional Forwarding Detection (BFD).

**Important:** A maximum of 1,200 static routes may be configured per context. 

Virtual Routing and Forwarding (VRF) context can be associated with static IP route for BGP/MPLS, GRE, or IPSec tunnel support.

Example  
The following example configures a static route with IPv6 prefix/length 2001:0db8:3c4d:0015:0000:abcd:ef12/24 to the next hop interface egress1:  

```
ipv6 route 2001:0db8:3c4d:0015:0000:0000:abcd:ef12/24 interface egress1
```
**ipv6 route-access-list**

Configures an IPv6 route access list for filtering routes.

**Product**
- GGSN
- HA
- PDSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration
```markdown
configure > context context_name
```

Entering the above command sequence results in the following prompt:
```
[context_name]host_name(config-ctx)#
```

**Syntax**

```markdown
ipv6 route-access-list named list_name [ deny | permit ] network_address/net_mask [ exact-match ]

no ipv6 prefix-list list_name [ deny | permit ] [ any | network_address/net_mask [ exact-match ]
```

- **no**
  Delete the specified prefix-list entry.

- **name list_name**
  Specifies a name for the prefix list as an alphanumeric string of 1 through 79 characters.

- **deny**
  Specifies prefixes to deny.

- **permit**
  Specifies prefixes to permit.

- **network_address/net_mask [ exact-match ]**
  Specifies the prefix to match.
  `network_address/net_mask`: the IPv6 address and the length, in bits, of the network mask that defines the prefix. The IP address and mask must be entered in IPv6 colon-separated-hexadecimal notation.

- **Important**: On the ASR 5000, routes with IPv6 prefix lengths less than /12 and between the range of /64 and /128 are not supported.

- **exact-match le_value**: Specifies that only an exact match will initiate access list deny/permit function.
Usage
Use this command to filter routes by their IPv6 prefix.

Example

```
ipv6 route-access-list name routelistv6 seq 5 permit
2002::123.45.67.89/24
```
isakmp disable-phase1-rekey

This command is deprecated. Use **ikev1 disable-phase1-rekey** command to configure the parameters for Phase1 SA rekeying when ISAKMP lifetime expires for IKE v1 protocol.
isakmp keepalive

This command is deprecated. Use `ikev1 keepalive dpd` command to configure ISAKMP IPSec Dead Peer Detection (DPD) message parameters for IKE v1 protocol.
isakmp policy

This command is deprecated. Use `ikev1 policy` command to create/configure an ISAKMP policy with the specified priority for IKE v1 protocol.
iups-service

Creates an Iu-PS service instance and enters the Iu-PS Service Configuration Mode. This mode defines the configuration and usage of Iu-PS interfaces between the SGSN and the RNCs in the UMTS radio access network (UTRAN). It defines both the control plane (GTP-C) and the data plane (GTP-U) between these nodes.

**Important:** For details about the commands and parameters for this mode, check the *IuPS Service Configuration Mode Commands* chapter.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration
configure > context context_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
[ no ] iups-service srvc_name
```

- **no**
  Remove the configuration for the specified Iu-PS service from the configuration for the current context.

- **srvc_name**
  Specifies the IuPS service name as a unique alphanumeric string of 1 through 63 characters.

**Important:** Service names must be unique across all contexts within a chassis.

**Usage**

Use this command to create, edit, or remove an Iu-PS service. Add up to eight definitions to be used with a single SGSN service so the SGSN can support multiple PLMNs.

**Example**

The following command creates an Iu-PS service named *iu-ps1*:

```
iups-service iu-ps1
```

The following command removes the Iu-PS service named *iu-ps1*:

```
no iups-service iu-ps1
```
I2tp peer-dead-time

Configures a delay when attempting to tunnel to a specific peer which is initially unreachable due to reasons such as a network issue or temporarily having reached its capacity.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration

```bash
configure > context context_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
l2tp peer-dead-time seconds
```

**default l2tp peer-dead-time**

<table>
<thead>
<tr>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rests the command to its default setting of 60.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>seconds</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the interval (in seconds) to wait before attempting to tunnel to a specific peer which is initially unreachable as an integer from 5 through 64,000. Default: 60</td>
</tr>
</tbody>
</table>

**Usage**
The time to wait before trying to establish a tunnel to a known peer after the initial attempt was unsuccessful.

**Example**
The following example configures the delay in attempting to tunnel to a temporarily unreachable peer. The delay is set to 120 seconds in this example.

```
l2tp peer-dead-time 120
```
**lac-service**

Enters the LAC Service Configuration Mode, or is used to add or remove a specified L2TP Access Concentrator (LAC) service.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration

```
configure > context context_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
[ no ] lac-service name
```

- **no**
  Removes the specified lac-service from the current context.

- **name**
  Specifies the name of a LAC service to configure, add, or remove as an alphanumeric string of 1 through 63 characters that is case-sensitive.

**Important:** Service names must be unique across all contexts within a chassis.

**Usage**
Enter the LAC Service Configuration Mode for an existing service or for a newly defined service. This command is also used to remove an existing service.

A maximum of 256 services (regardless of type) can be configured per system.

**Caution:** Large numbers of services greatly increase the complexity of management and may impact overall system performance (i.e. resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

**Example**

To add a new LAC service named **LAC1** and enter the LAC Service Configuration Mode, enter the following command:

```
lac-service LAC1
```

To configure an existing LAC service named **LAC2**, enter the following command:
lac-service LAC2

To delete an existing LAC service named \textit{LAC3}, enter the following command:

\texttt{no lac-service LAC3}
lawful-intercept

Refer to the Lawful Intercept Configuration Guide for a description of this command.
lawful-intercept dictionary

Refer to the Lawful Intercept Configuration Guide for a description of this command.
**Imla-service**

Creates an Local Mobility Anchor (LMA) service or specifies an existing LMA service and enters the LMA Service Configuration Mode for the current context.

**Product**
- P-GW
- SAEGW

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration

```bash
configure > context context_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
lma-service service_name [ -noconfirm ]
```

**no lma-service service_name**

```
no
```

Removes the specified LMA service from the context.

```
service_name
```

Specifies the name of the LMA service. If `service_name` does not refer to an existing service, the new service is created if resources allow.

`service_name` is an alphanumeric string of 1 through 63 characters.

**Important:** Service names must be unique across all contexts within a chassis.

```
-noconfirm
```

Executes the command without any additional prompt and confirmation from the user.

**Usage**

Enter the LMA Service Configuration Mode for an existing service or for a newly defined service. This command is also used to remove an existing service. A maximum of 256 services (regardless of type) can be configured per system.

**Caution:** Large numbers of services greatly increase the complexity of management and may impact overall system performance (for example, resulting from such things as system handoffs). Therefore, it is recommended that a
large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Entering this command results in the following prompt:

```
[context_name]hostname(config-lma-service)#
```

LMA Service Configuration Mode commands are defined in the *LMA Service Configuration Mode Commands* chapter.

Use this command when configuring the following eHRPD and PMIP SAE components: P-GW (SAEGW).

**Example**

The following command enters the existing LMA Service Configuration Mode (or creates it if it does not already exist) for the service named `lma-service1`:

```
lma-service lma-service1
```

The following command will remove `lma-service1` from the system:

```
no lma-service lma-service1
```
Ins-service

Enters the LNS Service Configuration Mode, or is used to add or remove a specified L2TP Network Server (LNS) service.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration

configuration > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

[ no ] lns-service name

no

Removes the specified lns-service from the current context.

name

Specifies the name of a LNS service to configure, add or remove as an alphanumeric string of 1 through 63 characters that is case-sensitive.

Important: Service names must be unique across all contexts within a chassis.

Usage

Enter the LNS Service Configuration Mode for an existing service or for a newly defined service. This command is also used to remove an existing service. A maximum of 256 services (regardless of type) can be configured per system.

Caution: Large numbers of services greatly increase the complexity of management and may impact overall system performance (i.e. resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Example

To add a new LNS service named LNS1 and enter the LNS Service Configuration Mode, enter the following commands:

lns-service LNS1

To configure an existing LNS service named LNS2, enter the following command:
lns-service LNS2

To delete an existing LNS service named LNS3, enter the following command:

no lns-service LNS3
location-service

Creates a location service configuration instance or configures an existing location service configuration and enters the Location Service Configuration Mode. LoCation Services (LCS) are used to determine the geographic location of a UE.

Product
MME
SGSN

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration

configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

location-service service_name [ -noconfirm ]

no location-service service_name

no
Removes the specified location service configuration instance from the context.

service_name
Specifies the name of the location service configuration instance. If service_name does not refer to an existing service, the new service is created if resources allow. service_name is an alphanumeric string of 1 through 63 characters.

Important: Service names must be unique across all contexts within a chassis.

-noconfirm
Executes the command without any additional prompt and confirmation from the user.

Usage
Enter the Location Service Configuration Mode for an existing service or for a newly defined service. This command is also used to remove an existing Service Configuration instance.

Location Service Configuration Mode commands are defined in the Location Service Configuration Mode Commands chapter.

A maximum of 16 location service instances can be configured per system.

Entering this command results in the following prompt:

[context_name]hostname(config-location-service)#
Example

The following command enters the existing Location Service Configuration Mode (or creates it if it does not already exist) for the service named `location-service1`:

```
location-service location-service1
```

The following command will remove `location-service1` from the system:

```
no location-service location-service1
```
logging

Modifies the logging options for a specified system log server for the current context.

Product
All

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration

configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

[ no ] logging syslog ip_address [ event-verbosity { min | concise | full } ] [ facility facilities ] [ pdu-data { none | hex | hex-ascii } ] [ pdu-verbosity pdu_level ] [ rate value ]

no

Indicates that internal logging is to be disabled for the options specified.

syslog ip_address

Specifies the IP address of a system log server on the network in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

event-verbosity { min | concise | full }

Specifies the level of detail to use in logging of events. Detail level must be one of the following:

- **min**: Displays minimal detail.
- **concise**: Displays summary detail.
- **full**: Displays full detail.

facility facilities

Default: local7

Specifies the local facility for which the system logging server’s logging options shall be applied. Local facility must be one of the following:

- local0
- local1
- local2
- local3
- local4
- local5
Multiple system log servers can share the logging options of a given local facility. This allows for the logical grouping of system log servers and the options which affect all of those associated with the same local facility.

**pdu-data** { none | hex | hex-ascii }

Specifies output format for packet data units when logged. Format must be one of the following:

- **none**: Displays data in raw format.
- **hex**: Displays data in hexadecimal format.
- **hex-ascii**: Displays data in hexadecimal and ASCII format (similar to a main-frame dump).

**pdu-verbosity** pdu_level

Specifies the level of verboseness to use in logging of packet data units as a value from 1 through 5, where 5 is the most detailed.

**rate** value

Specifies the rate at which log entries are allowed to be sent to the system log server. No more than the number specified by value will be sent to a system log server within any given one-second interval. value must be an integer from 0 through 100000. Default: 1000

### Usage

Set the log servers to enable remote review of log data.

The following sets the logging for events to the maximum for the local7 facility:

```
logging syslog 10.2.3.4 event-verbosity full
```

The following command sets the logging for packet data units to level 3 and sets the output format to the main-frame style hex-ascii for the local3 facility:

```
logging syslog 10.2.3.4 facility local3 pdu-data hex-ascii pdu-verbosity 3
```

The following sets the rate of information for the local1 facility:

```
logging syslog 10.2.3.4 facility local1 rate 100
```

The following disables internal logging to the system log server specified:

```
no logging syslog 10.2.3.4
```
**mag-service**

Creates a Mobile Access Gateway (MAG) service or specifies an existing MAG service and enters the MAG Service Configuration Mode for the current context.

**Product**

HSGW

S-GW

**Privilege**

Administrator

**Mode**

Exec > Global Configuration > Context Configuration

```
configure > context context_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
mag-service service_name [ -noconfirm ]

no mag-service service_name
```

- **no**
  - Removes the specified MAG service from the context.

- **service_name**
  - Specifies the name of the MAG service. If `service_name` does not refer to an existing service, the new service is created if resources allow.
  - `service_name` is an alphanumeric string of 1 through 63 characters.

**Important:** Service names must be unique across all contexts within a chassis.

- **-noconfirm**
  - Executes the command without any additional prompt and confirmation from the user.

**Usage**

Enter the MAG Service Configuration Mode for an existing service or for a newly defined service. This command is also used to remove an existing service.

A maximum of 256 services (regardless of type) can be configured per system.

**Caution:** Large numbers of services greatly increase the complexity of management and may impact overall system performance (for example, resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your Cisco service representative for more information.
Entering this command results in the following prompt:

```
[context_name]hostname(config-mag-service)#
```

MAG Service Configuration Mode commands are defined in the *MAG Service Configuration Mode Commands* chapter. Use this command when configuring the following eHRPD and PMIP SAE components: HSGW and S-GW.

**Example**

The following command enters the existing MAG Service Configuration Mode (or creates it if it does not already exist) for the service named `mag-service1`:

```
mag-service mag-service1
```

The following command will remove `mag-service1` from the system:

```
no mag-service mag-service1
```
map-service

Creates a Mobile Application Part (MAP) Service instance and enters the MAP Service Configuration mode to define or edit the MAP service parameters.

MAP is the SS7 protocol that provides the application layer required by some of the nodes in GPRS/UMTS networks to communicate with each other in order to provide services to mobile phone users. MAP is used by the serving GPRS support node (SGSN) to access SS7 network nodes such as a home location register (HLR) or a radio access network (RAN).

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration

*configure > context context_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

Syntax

```
map-service srvc_name

no map-service srvc_name
```

**no**

Remove the specified MAP service from the configuration for the current context.

**srvc_name**

Specifies the name of the MAP service as a unique alphanumeric string of 1 through 63 characters.

---

**Important:** Service names must be unique across all contexts within a chassis.

Usage

Use this command to create, edit, or remove a MAP service configuration.

---

**Important:** For details about the commands and parameters, check the MAP Service Configuration Mode Commands chapter.

Example

The following command creates a MAP service named *map_1*:

```
map-service map_1
```
The following command removes the configuration for a MAP service named `map_1` from the configuration for the current context:

```
no map-service map_1
```
mipv6ha-service

Creates a Mobile IPv6 Home Agent (MIPv6-HA) service instance and enters the MIPv6 HA Service Configuration mode to define or edit the MIPv6-HA service parameters.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration

`configure > context context_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
mipv6ha-service srvc_name

no mipv6ha-service srvc_name
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>mipv6ha-service</code></td>
<td>Creates a MIPv6-HA service instance and enters the MIPv6 HA Service Configuration mode.</td>
</tr>
<tr>
<td><code>no mipv6ha-service</code></td>
<td>Removes the specified MIPv6-HA service from the configuration for the current context.</td>
</tr>
</tbody>
</table>

**srvc_name**

Specifies the name of the MIPv6-HA service as a unique alphanumeric string of 1 through 63 characters.

**Important:** Service names must be unique across all contexts within a chassis.

**Usage**

Use this command to create, edit, or remove a MIPv6-HA service configuration.

**Important:** For details about the commands and parameters, check the *MIPv6 HA Service Configuration Mode Commands* chapter.

**Example**

The following command creates a MIPv6-HA service named `mipv6ha_1`:

```
mipv6ha-service mipv6ha_1
```

The following command removes the configuration for a MIPv6-HA service named `mipv6ha_1` from the configuration for the current context:

```
no mipv6ha-service mipv6ha_1
```
mme-service

Creates an Mobility Management Entity (MME) service or configures an existing MME service and enters the MME Service Configuration Mode for Evolved Packet Core (EPC) networks in the current context.

**Product**
MME

**Privilege**
Administrator

**Mode**

```
Exec > Global Configuration > Context Configuration
configure > context context_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
mme-service service_name [ -noconfirm ]
no mme-service service_name
```

- **no**
  Removes the specified MME service from the context.

- **service_name**
  Specifies the name of the MME service. If `service_name` does not refer to an existing service, the new service is created if resources allow.
  `service_name` is an alphanumeric string of 1 through 63 characters.

**Important:** Service names must be unique across all contexts within a chassis.

- **-noconfirm**
  Executes the command without any additional prompt and confirmation from the user.

**Usage**

Enter the MME Service Configuration Mode for an existing service or for a newly defined service. This command is also used to remove an existing service.

A maximum of 8 MME service can be configured on a system which is further limited to a maximum of 256 services (regardless of type) can be configured per system.

**Caution:** Large numbers of services greatly increase the complexity of management and may impact overall system performance (for example, resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.
Entering this command results in the following prompt:

`[context_name]hostname(config-mme-service)#`

MME Service Configuration Mode commands are defined in the MME Service Configuration Mode Commands chapter.

**Caution:** This is a critical configuration. The MME service cannot be configured without this configuration. Any change to this configuration would lead to restarting the MME service and removing or disabling this configuration will stop the MME service.

**Example**

The following command enters the existing MME Service Configuration Mode (or creates it if it does not already exist) for the service named `mme-service1`:

```
  mme-service mme-service1
```

The following command will remove `mme-service1` from the system:

```
  no mme-service mme-service1
```
mobile-access-gateway

Controls whether duplicate MAG sessions are allowed in HSGW. By default, duplicate sessions are rejected.

Product
HSGW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration

configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-cxt)#

Syntax

mobile-access-gateway newcall duplicate-session { purge | reject }

[ default | no ] mobile-access-gateway newcall duplicate-session

default | no

Disables the feature. New session create request is discarded.

newcall duplicate-session { purge | reject }

Determines new call related behavior on context when duplicate MAG sessions are requested in HSGW (Mobile Access Gateway).

purge: Enables the feature. Old MAG session is deleted and new session create request is rejected, but on retry the new call comes up.

reject: Disables the feature. Rejects new call with duplicate session create request; new session create request is discarded.

Usage

This command controls whether duplicate MAG sessions are allowed in HSGW.
When enabled, HSGW rejects new session create request initially and creates new call on retry.
When disabled, HSGW rejects new call and new session create request is discarded.

Example

The following command allows duplicate MAG sessions in HSGW on this context:

mobile-access-gateway newcall duplicate-session purge
**mobile-ip fa**

Configures settings that effect all FA services in the current context.

**Product**
FA

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration

```plaintext
configure > context context_name
```

Entering the above command sequence results in the following prompt:

```plaintext
[context_name]host_name(config-ctx)#
```

**Syntax**

```plaintext
mobile-ip fa \{ multiple-dynamic-reg-per-nai | newcall duplicate-home-address \{ accept | reject \} \}
\{ default | no \} mobile-ip fa \{ multiple-dynamic-reg-per-nai | newcall duplicate-home-address \}
```

### default

Configures the default setting for the specified parameter.

- **multiple-dynamic-reg-per-nai**: All FA services in the current context can not simultaneously setup multiple dynamic home address registrations that have the same NAI.
- **newcall duplicate-home-address**: reject

### no

- **multiple-dynamic-reg-per-nai**: Disables all FA services in the current context from simultaneously setting up multiple dynamic home address registrations that have the same NAI.
- **newcall duplicate-home-address**: Resets this option to its default of reject.

### multiple-dynamic-reg-per-nai

This keyword allows all FA services in the current context to simultaneously setup multiple dynamic home address registrations that have the same NAI.

```plaintext
newcall duplicate-home-address \{ accept | reject \}
```

- **accept**: The new call is accepted and the existing call is dropped.
- **reject**: The new call is rejected with an Admin Prohibited code.

**Usage**

Use this command to set the behavior of all FA services in the current context.
Example

To configure all FA services to accept new calls and drop the existing call when the new call requests an IP address that is already in use by an existing call, enter the following command:

    mobile-ip fa newcall duplicate-home-address accept

To enable all FA services in the current context to allow all FA services in the current context to simultaneously setup multiple dynamic home address registrations that have the same NAI, enter the following command:

    mobile-ip fa multiple-dynamic-reg-per-nai
**mobile-ip ha assignment-table**

Creates a Mobile IP HA assignment table and enters Mobile IP HA Assignment Table Configuration Mode.

**Product**
HA

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration
configure > context context_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
mobile-ip ha assignment-table atable_name [ -noconfirm ]
no mobile-ip ha assignment-table atable_name
```

- **no**
  This keyword deletes the specified assignment table

- **atable_name**
  Specifies the name of the MIP HA assignment table to create or edit as an alphanumeric string of 1 through 63 characters.

- **-noconfirm**
  Executes the command without any additional prompt and confirmation from the user.

**Usage**

Use this command to create a new MIP HA assignment table or edit an existing MIP HA assignment table.

**Important:** A maximum of eight MIPHA assignment tables can be configured per context with a maximum of 8 MIP HA assignment tables across all contexts.

**Important:** A maximum of 256 non-overlapping hoa-ranges can be configured per MIP HA Assignment table with a maximum of 256 non-overlapping hoa-ranges across all MIP HA Assignment tables.

**Example**

The following command creates a new MIP HA assignment table name `MIPHAtable1` and enters MIP HA Assignment Table Configuration Mode without asking for confirmation from the user:

```
mobile-ip ha assignment-table MIPHAtable1
```
mobile-ip ha newcall

Configures the behavior of all HA services when duplicate home addresses and duplicate IMSI sessions occur for new calls.

Product
HA

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration
configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

mobile-ip ha newcall { duplicate-home-address { accept | reject } | duplicate-imsi-session { allow | disallow | global-disallow } | wimax-session-overwrite { allow | disallow } }

{ default | no } mobile-ip ha newcall { duplicate-home-address | duplicate-imsi-session | wimax-session-overwrite }

default

Configures the default setting for the specified parameter.

• **duplicate-home-address: reject**—sets HA services to reject a new call that requests an IP address that is already assigned.

• **duplicate-imsi-session: allow**—sets HA services to accept new calls that have the same IMSI as a call that is already active.

• **wimax-session-overwrite: disallow**—disable session overwrite feature for WiMax mobile-ip calls on the HA.

no

Configures the default setting for the specified parameter.

duplicate-home-address { accept | reject }

Configures the HA to either accept or reject new calls if the new call requests a static IP home address that is already assigned to an existing call from an IP address pool in the same destination context.

• **accept**: The new call is accepted and the existing call is dropped.

• **reject**: The new call is rejected with an Admin Prohibited code.

duplicate-imsi-session { allow | disallow | global-disallow }

Configures the HA to either permit or not permit multiple sessions for the same IMSI.

• **allow**: Allows multiple sessions for the same IMSI.
**mobile-ip ha newcall**

- **disallow**: If a mobile node already has an active session and a new session is requested using the same IMSI, the currently active session is dropped and the new session is accepted.

- **global-disallow**: Enables HA services in this context to accept a new session and disconnect any other session(s) having the same IMSI being processed in this context. In addition, a request is sent to all other contexts containing HA services to do the same.

**Important**: In order to ensure a single session per IMSI across all contexts containing HA services, the global-disallow option must be configured in every context.

**wimax-session-overwrite** { allow | disallow }

Use this command to enable or disable the overwrite feature for WiMAX mobile ip (MIPv4) calls on the HA.

**Usage**

Use this command to set the behavior of all HA services for new calls.

**Example**

To configure all HA services to accept new calls when the new call requests a static IP that is already assigned from an IP pool in the same destination context, enter the following command:

```
mobile-ip ha newcall duplicate-home-address accept
```

To configure all HA services to drop an active call and accept a new one that uses the same IMSI, enter the following command:

```
mobile-ip ha newcall duplicate-imsi-session disallow
```
mobile-ip ha reconnect

Sets the behavior of all HA services to reconnect dropped calls.

Product
HA

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration
configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax


static-homeaddr
Specifies that the home address as a static IP address.

dynamic-pool-allocation
Allows a dynamic pool to accept a static address allocation.

Usage
Use this command to reset the HA behavior for new calls.

Example

  mobile-ip ha reconnect
  mobile-ip ha reconnect static-homeaddr
  mobile-ip ha reconnect static-homeaddr dynamic-pool-allocation
  no mobile-ip ha reconnect
  no mobile-ip ha reconnect static-homeaddr
mpls bgp forwarding

Globally enables Multi protocol Label Switching (MPLS) Border Gateway Protocol (BGP) forwarding.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration

`configure > context context_name`

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-ctx)#`

**Syntax**

```
[ no ] mpls bgp forwarding
```

- `no`
  Disables MPLS BGP forwarding.

**Usage**

Use this command to globally enable the MPLS BGP forwarding. By enabling this command, the BGP VPNv4 routes need not have an underlying LSP to forward the IP packets. If this command is not enabled, then the nexthop for the BGP routes must be reachable via LDP.

⚠️ **Caution:** This command should always be enabled when nexthop is not reachable thorough LSP.

**Example**

The following command enables the MPLS BGP forwarding on the system:

```
mpls bgp forwarding
```
**mpls exp**

Sets the default behavior as Best Effort using a zero value in the 3-bit MPLS EXP (Experimental) header. This setting overrides the value sent by the mobile subscriber.

**Product**
- eHRPD
- GGSN
- PDSN (HA)

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration > Context Configuration
  ```
  configure > context context_name
  ```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
[ no ] mpls exp <value>
```

- **no**
  
  Reverts back to the default behavior, which is to copy the DSCP from the mobile subscriber packet to the EXP header of the packet, if there is no explicit configuration for DSCP to EXP.

- **<value>**
  
  Specifies the MPLS EXP header value as an integer from 0 through 7. Higher value indicates higher priority.

**Usage**

Set the default behavior as Best Effort using a zero value in the 3-bit MPLS EXP header. This value applies to all the VRFs in the context. The default behavior is to copy the DSCP value of mobile subscriber traffic to the EXP header, if there is no explicit configuration for DSCP to EXP (via the **mpls map-dscp-to-exp dscp <n> exp <m>** command).

This command disables the default behavior and sets the EXP value to the configured `<value>`.

**Example**

The following command sets the MPLS EXP header value to 2:

```
mpls exp 2
```
mpls ip

Globally enables the Multiprotocol Label Switching (MPLS) forwarding of IPv4 packets along normally routed paths.

**Product**
- GGSN
- HA
- P-GW
- SAEGW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration
```
configure > context context_name
```
Entering the above command sequence results in the following prompt:
```
[context_name]host_name(config-ctx)#
```

**Syntax**
```
[ no ] mpls ip
```
- **no**
  Disables MPLS forwarding of IPv4 packets configured on the system. `no mpls ip` stops dynamic label distribution on all the interfaces regardless of interface configuration.

**Usage**
Globally enables the MPLS forwarding of IPv4 packets along normally routed paths for the entire context. It does not start label distribution over an interface until MPLS has been enabled for the interface as well. Refer to the Ethernet Interface Configuration Mode Commands chapter for additional information.

⚠️ **Caution:** This feature is not enabled by default.

**Example**
Following command enables (but does not start) MPLS forwarding of IPv4 packets along normally routed paths:
```
mpls ip
```
mseg-service

This command is not supported in this release.
multicast-proxy

Creates, configures or deletes a multicast proxy host configuration.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration

```plaintext
configure > context context_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```plaintext
[no] multicast-proxy { igmp interface ip_address range-start start_ip_address range-end end_ip_address | listen address listen_ip_address port port_number protocol protocol_number sessmgr instance }
```

**no**
If previously configured, deletes the specified multicast proxy parameter from the current context.

```plaintext
igmp interface ip_address range-start start_ip_address range-end end_ip_address
```
Specifies the IP address and range of associated addresses for this Internet Group Management Protocol (IGMP) interface.

- **ip_address** is the IP address of this interface expressed in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.
- **range-start start_ip_address** is the start point for the multicast address range expressed in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.
- **range-end end_ip_address** is the end point for the multicast address range expressed in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

```plaintext
listen address listen_ip_address port port_number protocol protocol_number sessmgr instance
```
Configures this context as a multicast proxy listener.

- **listen_ip_address** is the IP address that will be listened to, expressed in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.
- **port port_number** is the port number which will be listened to. If this is not provided, the listener will receive all packets from the **listen_ip_address**.
- **protocol protocol_number** is the IANA protocol number associated with the port number. If this is not provided, the listener will receive all packets from the **listen_ip_address** and **port_number**.
- **sessmgr instance** is an integer from 1 through 270.
Usage

Use this command to create/configure/delete a multicast proxy host configuration.

Example

The following command creates an IGMP multicast host configuration:

```
multicast proxy igmp interface 192.155.1.34 range-start 255.0.0.0 range-end 255.0.0.1
```
Chapter 54
Context Configuration Mode Commands N-R

This section includes the commands `nw-reachability server` through `router` service.

**Mode**

Exec > Global Configuration > Context Configuration

`configure > context context_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
**nw-reachability server**

Adds or deletes a reachability-detect server and configures parameters for retrying the failure-detection process. When network reachability is enabled, an ICMP ping request is sent to this device. If there is no response after a specified number of retries, the network is deemed failed. Execute this command multiple times to configure multiple network reachability servers.

**Product**
P-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration

```
configure > context context_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
nw-reachability server server_name [ interval seconds ] [ local-addr ip_addr ] [ num-retry num ] [ remote-addr ip_addr ] [ timeout seconds ] [ vfr name]
```

```
no nw-reachability server server_name
```

Delete the reference to the specified network reachability server.

```
server_name
```

Specifies the name for the network device that is sent ping packets to test for network reachability.

```
interval seconds
```

Specifies the frequency in seconds for sending ping requests as an integer from 1 through 3600. Default: 60

```
local-addr ip_addr
```

Specifies the IP address to be used as the source address of the ping packets; If this is unspecified, an arbitrary IP address that is configured in the context is used. *ip_addr* must be entered using IPv4 dotted-decimal notation.

```
um-retry num
```

Specifies the number of retries before deciding that there is a network-failure as an integer from 0 through 100. Default: 5

```
remote-addr ip_addr
```

Specifies the IP address of a network element to use as the destination to send the ping packets for detecting network failure or reachability. *ip_addr* must be entered using IPv4 dotted-decimal notation.
timeout seconds

Specifies how long to wait (in seconds) before retransmitting a ping request to the remote address as an integer from 1 through 1. Default: 3

vrf name

Specifies an existing VRF name as an alphanumeric string of 1 through 63 characters.

Usage

Use this command to set up a network device on a destination network that is used to ensure that Mobile IP sessions can reach the required network from the P-GW.

**Important**: Refer to the P-GW Configuration Mode command `policy nw-reachability-fail` to configure the action that should be taken when network reachability fails.

**Important**: Refer to the Subscriber Config Mode command `nw-reachability-server` to bind the network reachability to a specific subscriber.

**Important**: Refer to the `nw-reachability_server server_name` keyword of the `ip pool` command in this chapter to bind the network reachability server to an IP pool.

Example

To set a network device called Internet Device with the IP address of 192.168.100.10 as the remote address that is pinged to determine network reachability and use the address 192.168.200.10 as the origination address of the ping packets sent, enter the following command:

```
nw-reachability server InternetDevice local-addr 192.168.200.10 remote-addr 192.168.100.10
```
network-requested-pdp-context activate

Configures the mobile station(s) (MSs) for which network initiated PDP contexts are supported.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration

```
configure > context context_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
network-requested-pdp-context activate address ip_address dst-context context_name imsi
imsi apn apn_name
```

```
no network-requested-pdp-context activate address ip_address dst-context context_name
```

**Usage**

Use this command to specify the MS(s) for which network initiated PDP contexts are supported.

When a packet is received for an MS that does not currently have a PDP context established, the system checks the configuration of this parameter to determine if the destination IP address specified in the packet is specified by this parameter. If the address is not specified, then the system discards the packet. If the address
is specified, the system uses the configured IMSI and APN to determine the appropriate SGSN from the Home Location Register (HLR). The system communicates with the HLR through the interworking node configured using the network-requested-pdp-context gsn-map command.

Once the session is established, the destination context specified by this command is used in place of the one either configured within the specified APN template or returned by a RADIUS server during authentication. This command can be issued multiple times supporting network initiated PDP contexts for up to 1,000 configured addresses per system context.

Example

The following command enables support for network initiated PDP contexts for an MS with a static IP address of 20.13.5.40 from a pool configured in the destination context pdn1 with an IMSI of 3319784450 that uses an APN template called isp1:

```
network-requested-pdp-context activate address 20.13.5.40 dst-context pdn1 imsi 3319784450 apn isp1
```
network-requested-pdp-context gsn-map

Configures the IP address of the interworking node that is used by the system to communicate with the Home Location Register (HLR), and optionally sets the GTP version to use.

Product
GGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration
configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

network-requested-pdp-context gsn-map ip_address [ gtp-version { 0 | 1 } ]

no network-requested-pdp-context gsn-map

no

Deletes a previously configured gsn-map node.

ip_address

Specifies the IP address of the gsn-map node in Pv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

gtp-version { 0 | 1 }

Specifies the gtp version used. Default: 1

Usage

Communications from the system to the HLR must go through a GSN-map interworking node that performs the protocol conversion from GTPC to SS7.
The UDP port for this communication is 2123.
Support for network requested PDP contexts must be configured within source contexts on the system. Only one gsn-map node can be configured per source context.
The source context also contains the GGSN service configuration that specifies the IP address of the Gn interface. If multiple GGSN services are configured in the source context, one is selected at random for initiating the Network Requested PDP Context Activation procedure.
Communication with the gsn-map node is done over the Gn interface configured for the GGSN service. The IP address of that interface is used as the system’s source address.

Example

The following command configures the system to communicate with a gsn-map node having an IP address of 192.168.2.5:
network-requested-pdp-context gsn-map 192.168.2.5
network-requested-pdp-context hold-down-time

Configures the time duration to that the system will wait after the SGSN rejects an attempt for a network-requested PDP context creation for the subscriber.

Product
GGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration

configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

network-requested-pdp-context hold-down-time time

default network-requested-pdp-context hold-down-time

default

Configures the default setting.

Default: 60 seconds

time

Specifies the time interval (in seconds) as an integer from 0 through 86400.

Usage

Packets received during this time period would be discarded, rather than being used to cause another network-requested PDP context creation attempt for the same subscriber. After the time period has expired, any subsequent packets received would cause another network-requested PDP context creation procedure to begin.

Example

The following command configures a hold-down-time of 120 seconds:

network-requested-pdp-context hold-down-time 120
network-requested-pdp-context interval

Configures the minimum amount of time that must elapse between the deletion of a network initiated PDP context and the creation of a new one for the same MS.

Product
GGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration

configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

network-requested-pdp-context interval time

default network-requested-pdp-context interval

default

Returns the command to its default setting of 60.

time

Specifies the minimum amount of time (in seconds) that must pass before the system allows another network-requested PDP context for a specific MS after the previous context was deleted. time is an integer from 0 through 86400. Default: 60

Usage

Once an MS deletes a PDP context that initiated from the network, the system automatically waits the amount of time configured by this parameter before allowing another network initiated PDP context for the same MS.

Example

The following command specifies that the system waits 120 seconds before allowing another network requested PDP context for an MS:

network-requested-pdp-context interval 120
network-requested-pdp-context sgsn-cache-time

Configures the time duration that the GGSN keeps the SGSN/subscriber pair cached in its local memory.

Product
GGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration

configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

network-requested-pdp-context sgsn-cache-time time

default network-requested-pdp-context sgsn-cache-time

default

Configures the default setting.
Default: 300 seconds

time

Specifies the time interval (in seconds) as an integer from 0 through 86400.

Usage

For an initial network-requested PDP context creation, the system contacts the HLR (via the GSN-MAP interworking node) to learn which SGSN is currently servicing the subscriber. The system keeps that information in cache memory for the configured time, so that future network-requested PDP context creations for that subscriber can be initiated without having to contact the HLR again.

Example

The following command configures an sgsn-cache-time of 500 seconds:

network-requested-pdp-context sgsn-cache-time 500
**operator**

Configures a context-level operator account within the current context.

**Product**
All

**Privilege**
Security Administrator

**Mode**
Exec > Global Configuration > Context Configuration

configure > context  context_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
operator  user_name  [ encrypted ] password  password  [ ecs ]  [ expiry-date  date_time ]  [ li-administration ]  [ noecs ]  [ timeout-absolute  abs_seconds ]  [ timeout-min-absolute  abs_minutes ]  [ timeout-idle  timeout_duration ]  [ timeout-min-idle  idle_minutes ]
```

```
no operator  user_name
```

---

**no**

Removes a previously configured context-level operator account.

---

**user_name**

Specifies a name for the account as an alphanumeric string of 1 through 32 characters.

---

**[ encrypted ] password  password**

Specifies the password to use for the user which is being given context-level operator privileges within the current context. The encrypted keyword indicates the password specified uses encryption. The password is an alphanumeric string of 1 through 63 characters without encryption, or 1 through 127 with encryption. The encrypted keyword is intended only for use by the system while saving configuration scripts. The system displays the encrypted keyword in the configuration file as a flag that the variable following the password keyword is the encrypted version of the plain text password. Only the encrypted password is saved as part of the configuration file.

---

**ecs**

Permits the specific user to access ACS-specific configuration commands from Exec Mode only. Default: ACS-specific configuration commands are not allowed.

---

**expiry-date  date_time**

Specifies the date and time that this account expires. Enter the date and time in the format YYYY:MM:DD:HH:mm or YYYY:MM:DD:HH:mm:ss.
Where YYYY is the year, MM is the month, DD is the day of the month, HH is the hour, mm is minutes, and ss is seconds.

**li-administration**
Refer to the *Lawful Intercept Configuration Guide* for a description of this parameter.

**noecs**
Prevents the user from accessing ACS-specific configuration commands. Default: Enabled

**timeout-absolute abs_seconds**
This keyword is obsolete. It has been left in place for backward compatibility. If used a warning is issued and the value entered is rounded to the nearest whole minute. Specifies the maximum amount of time (in seconds) the context-level operator may have a session active before the session is forcibly terminated. abs_seconds must be a value in the range from 0 through 300000000. The value 0 disables the absolute timeout. Default: 0

**timeout-min-absolute abs_minutes**
Specifies the maximum amount of time (in minutes) the context-level operator may have a session active before the session is forcibly terminated. abs_minutes must be an integer from 0 through 300000000. The value 0 disables the absolute timeout. Default: 0

**timeout-idle timeout_duration**
This keyword is obsolete. It has been left in place for backward compatibility. If used a warning is issued and the value entered is rounded to the nearest whole minute. Specifies the maximum amount of idle time (in seconds) the context-level operator may have a session active before the session is terminated. timeout_duration must be an integer from 0 through 300000000. The value 0 disables the idle timeout. Default: 0

**timeout-min-idle idle_minutes**
Specifies the maximum amount of idle time (in minutes) the context-level operator may have a session active before the session is terminated. idle_minutes must be an integer from 0 through 300000000. The value 0 disables the idle timeout. Default: 0

**Usage**
Use this command to create new context-level operator or modify existing operator’s options, in particular, the timeout values.
Operators have read-only privileges. They can maneuver across multiple contexts, but cannot perform configuration operations. Refer to the *Command Line Interface Overview* chapter for more information.

**Important:** A maximum of 128 administrative users and/or subscribers may be locally configured per context.

**Example**
The following command creates a context-level operator account named *user1* with ACS control:

```
operator user1 password secretPassword ecs
```
The following command removes a previously configured context-level operator account named `user1`:

```
no operator user1
```
optimize pdsn inter-service-handoff

Controls the optimization of the system’s handling of inter-PDSN handoffs.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration

```
configure > context context_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
[ default | no ] optimize pdsn inter-service-handoff
```

- **default**
  
  Resets the command to its default setting of enabled.

- **no**
  
  Disables the feature.

**Usage**

When more than one PDSN service is defined in a context, each PDSN-Service acts as an independent PDSN. When a Mobile Node (MN) moves from one PDSN service to another PDSN service, by rule, it is an inter-PDSN handoff. This command optimizes PDSN handoffs between PDSN Services that are defined in the same context in the system.

The default for this parameter is enabled. The no keyword disables this functionality.

When enabled, the system treats handoffs happening between two PDSN services in the same context as an inter-PDSN handoff. Existing PPP session states and connection information is reused. If the inter-PDSN handoff requires a PPP restart, then PPP is restarted. The optimized inter-service-handoff may not restart the PPP during handoffs allowing the MN to keep the same IP address for the Simple IP session.

**Example**

```
optimize pdsn inter-service-handoff
```
pcc-af-service

Creates or removes an IPCF Policy and Charging Control (PCC) Application Function (AF) service or configures an existing PCC-AF service. It enters the PCC-AF Service Configuration Mode to link, configure, and manage the Application Function endpoints and associated PCC services over the Rx interface for the IPCF services.

Product
- IPCF

Privilege
- Administrator

Mode
- Exec > Global Configuration > Context Configuration
- configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

pcc-af-service service_name [ -noconfirm ]

no pcc-af-service service_name

no

Removes the specified PCC-AF service from the context.

service_name

Specifies the name of the PCC-AF service. If service_name does not refer to an existing service, the new service is created if resources allow. service_name is an alphanumerical string of 1 through 63 characters.

Important: Service names must be unique across all contexts within a chassis.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage

Use this command to enter the PCC-AF Service Configuration Mode for an existing service or for a newly defined PCC-AF service. This command is also used to remove an existing service. The PCC-AF-Service consolidates the provisioning and management required for the PCC-AF services being supported by the network that fall under the PCC regime. The application service handles the Rx interface over which the IPCF may receive media information for the application usage from AF.

Important: In the absence of an Rx interface, the media information is available in the PCC-AF Service statically.
A maximum of 256 services (regardless of type) can be configured per system.

⚠️ **Caution:** Large numbers of services greatly increase the complexity of management and may impact overall system performance (for example, resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Entering this command results in the following prompt:

```
[context_name]hostname(config-imsapp-service)#
```

The commands available in this mode are defined in the *PCC-AF Service Configuration Mode Commands* chapter.

⚠️ **Caution:** This is a critical configuration. The PCC-AF service cannot be configured without this configuration. Any change to this configuration would lead to restarting the PCC-AF service and removing or disabling this configuration will stop the PCC-AF service.

**Example**

The following command enters the existing PCC-AF Service Configuration Mode (or creates it if it does not already exist) for the service named *af-service1*:

```
pcc-af-service af-service1
```

The following command will remove *af-service1* from the system:

```
no pcc-af-service af-service1
```
pcc-policy-service

Creates or removes an IPCF PCC-Policy service or configures an existing PCC-Policy service. It enters the PCC-Policy Service Configuration Mode to link, configure, and manage the Gx interface endpoints for policy authorization where IPCF acts as a policy server.

**Product**

IPCF

**Privilege**

Administrator

**Mode**

Exec > Global Configuration > Context Configuration

`configure > context context_name`

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-ctx)#`

**Syntax**

`pcc-policy-service service_name [ -noconfirm ]`

no pcc-policy-service service_name

- **no**
  - Removes the specified PCC-Policy service from the context.

- **service_name**
  - Specifies the name of the PCC-Policy service. If `service_name` does not refer to an existing service, the new service is created if resources allow. `service_name` is an alphanumeric string of 1 through 63 characters.

**Important:** Service names must be unique across all contexts within a chassis.

- **-noconfirm**
  - Executes the command without any additional prompt and confirmation from the user.

**Usage**

Use this command to enter the PCC-Policy Service Configuration Mode for an existing service or for a newly defined PCC-Policy service. This command is also used to remove an existing service. The PCC-Policy-Service is mainly used to provide a mechanism to manage the external Gx or similar interfaces required for policy authorization purpose. It manages Gx and Gx-like interfaces such as Gxc/Gxa between IPCF/PCRF and PCEF or BBERF, which is based on the dictionary used for PCC. Multiple instances of PCC-Policy-Service may exist in a system which could link with the same PCC-Service that controls the business logic. This service allows for management of configuration for peers as well self related to Gx like functions. A maximum of 256 services (regardless of type) can be configured per system.
Caution: Large numbers of services greatly increase the complexity of management and may impact overall system performance (for example, resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Entering this command results in the following prompt:

```
[context_name]hostname(config-pccpolicy-service)#
```

The commands available in this mode are defined in the PCC-Policy Service Configuration Mode Commands chapter.

Caution: This is a critical configuration. The PCC-Policy service cannot be configured without this configuration. Any change to this configuration would lead to restarting the PCC-Policy service and removing or disabling this configuration will stop the PCC-Policy service.

Example

The following command enters the existing PCC-Policy Service Configuration Mode (or creates it if it does not already exist) for the service named `gx-service1`:

```
pcc-policy-service gx-service1
```

The following command will remove `gx-service1` from the system:

```
no pcc-policy-service gx-service1
```
**pcc-service**

Creates or removes an IPCF Policy and Charging Control (PCC) service or configures an existing PCC service. It enters the PCC Service Configuration Mode for IPCF related configurations in the current context.

**Product**  
IPCF

**Privilege**  
Administrator

**Mode**  
Exec > Global Configuration > Context Configuration  
`configure > context context_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
pcc-service service_name [ -noconfirm ]
```

```
no pcc-service service_name
```

- **no**  
Removes the specified PCC service from the context.

- **service_name**  
Specifies the name of the PCC service. If `service_name` does not refer to an existing service, the new service is created if resources allow. `service_name` is an alphanumeric string of 1 through 63 characters.

**Important:** Service names must be unique across all contexts within a chassis.

```
-service_name
```

- **-noconfirm**  
Executes the command without any additional prompt and confirmation from the user.

**Usage**

Use this command to enter the PCC Service Configuration Mode for an existing service or for a newly defined PCC service. This command is also used to remove an existing service.  
The IPCF PCC Service Configuration Mode is used to link, consolidate and manage the policy logic for the networks. The authorization of resources for a subscriber’s data usage under various conditions and policies are defined in the IPCF PCC service.  
Only one PCC service can be configured on a system which is further limited to a maximum of 256 services (regardless of type) configured per system.

**Caution:** Large numbers of services greatly increase the complexity of management and may impact overall system performance (for example, resulting from such things as system handoffs). Therefore, it is recommended that a
large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Entering this command results in the following prompt:

```
[context_name]hostname(config-pcc-service)#
```

The commands available in this mode are defined in the *PCC Service Configuration Mode Commands* chapter.

⚠️ **Caution:** This is a critical configuration. The PCC service cannot be configured without this configuration. Any change to this configuration would lead to restarting the Policy and Charging Control service and removing or disabling this configuration will stop the PCC service.

**Example**

The following command enters the existing PCC Service Configuration Mode (or creates it if it does not already exist) for the service named `ipcf-service1`:

```
pcc-service ipcf-service1
```

The following command will remove `ipcf-service1` from the system:

```
no pcc-service ipcf-service1
```
pcc-sp-endpoint

Creates or removes a PCC Sp interface endpoint or configures an existing PCC Sp interface client endpoint. It enters the PCC Sp Endpoint Configuration Mode to link, configure, and manage the operational parameters related to its peer.

**Product**
IPCF

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration

`configure > context context_name`

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-ctx)#`

**Syntax**

```
pcc-sp-endpoint sp_intfc1 [ -noconfirm ]

no pcc-sp-endpoint name sp_intfc1
```

- `no`
  Removes the specified PCC Sp interface endpoint from the context.

- `sp_intfc1`
  Specifies the name of the PCC Sp interface endpoint. If `sp_intfc_endpoint` does not refer to an existing endpoint, the new endpoint is created if resources allow. `sp_intfc_endpoint` is an alphanumeric string of 1 through 63 characters.

- `-noconfirm`
  Executes the command without any additional prompt and confirmation from the user.

**Usage**

Use this command to enter the PCC-Sp-Endpoint Configuration Mode for an existing interface or for a newly defined PCC Sp interface endpoint. This command is also used to remove an existing endpoint.

An instance of PCC Sp endpoint represents a client end for SSC/SPR interactions. It is possible to support multiple Sp endpoints each supporting the same or different protocol(s). The PCC Sp endpoint facilitates the configuration of the treatment required of the Sp interface as well as manages the connection and operational parameters related to its peer.

Only one PCC Sp endpoint across a chassis can be configured on a system.

Entering this command results in the following prompt:

`[context_name]hostname(config-spendpoint)#`

The commands available in this mode are defined in the **PCC-Sp-Endpoint Configuration Mode Commands** chapter.
**Caution:** This is a critical configuration. The PCC Sp endpoint cannot be configured without this configuration. Any change to this configuration would lead to reset the PCC Sp interface and removing or disabling this configuration also disables the PCC Sp interface.

**Example**

The following command enters the existing PCC Sp Endpoint Configuration Mode (or creates it if it does not already exist) for the endpoint named `sp_intfc1`:

```
pcc-sp-endpoint sp_intfc1
```

The following command will remove `sp_intfc1` from the system:

```
pcc-sp-endpoint name sp_intfc1
```
pdg-service

Creates a new PDG service or specifies an existing PDG service and enters the PDG Service Configuration Mode. A maximum of 16 PDG services can be created. This limit applies per ASR 5000 chassis and per context.

Product
PDG/TTG

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration
configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

[ no ] pdg-service name

- no name
  Deletes the specified PDG service.

- name
  Specifies the name of a new or existing PDG service as an alphanumeric string 1 through 63 characters that must be unique across all FNG services within the same context and across all contexts.

Important: Service names must be unique across all contexts within a chassis.

Usage
Use this command in Context Configuration Mode to create a new PDG service or modify an existing one. Executing this command enters the PDG Service Configuration Mode.

Example
The following command configures an PDG service named pdg_service_1 and enters the PDG Service Configuration Mode:

    pdg-service pdg_service_1
**pdif-service**

Creates a new, or specifies an existing, Packet Data Interworking Function (PDIF) service and enters the PDIF Service Configuration Mode.

**Product**

PDIF

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration

`configure > context context_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
[ no ] pdif-service name [ -noconfirm ]
```

- `name`
  Specifies the name of a new or existing PDIF service as an alphanumeric string of 1 through 63 characters.

**Important:** Service names must be unique across all contexts within a chassis.

**Usage**

Use this command to create a new or enter an existing PDIF service.

Entering this command results in the following prompt:

```
[context_name]host_name(config-pdif-service)#
```

PDIF Service Configuration Mode commands are defined in the *PDIF Service Configuration Mode Commands* chapter.

**Example**

The following command configures a PDIF service called *pdif2* and enters the PDIF Service Configuration Mode:

```
pdif-service pdif2
```
pdsn-service

Creates or deletes a packet data service or specifies an existing PDSN service for which to enter the Packet Data Service Configuration Mode for the current context.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration

```bash
configure > context context_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
[ no ] pdsn-service name
```

- **no**
  Indicates the packet data service specified is to be removed.

- **name**
  Specifies the name of the PDSN service to configure. If `name` does not refer to an existing service, the new service is created if resources allow. `name` is an alphanumeric string of 1 through 63 characters.

---

**Important:** Service names must be unique across all contexts within a chassis.

---

**Usage**

Enter the PDSN Service Configuration Mode for an existing service or for a newly defined service. This command is also used to remove an existing service.

A maximum of 256 services (regardless of type) can be configured per system.

---

**Caution:** Large numbers of services greatly increase the complexity of management and may impact overall system performance (resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your Cisco service representative for more information.

---

**Example**

The following command will enter the PDSN Service Configuration Mode creating the service `sampleService`, if necessary.

```
pdsn-service sampleService
```

The following command will remove `sampleService` as being a defined PDSN service.
no pdsn-service sampleService
pgw-service

Creates a PDN-Gateway (P-GW) service or specifies an existing P-GW service and enters the P-GW Service Configuration Mode for the current context.

Product:
P-GW
SAEGW

Privilege:
Administrator

Mode:
Exec > Global Configuration > Context Configuration

```
configure > context context_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

Syntax:

```
pgw-service service_name [ -noconfirm ]
no pgw-service service_name
```

- **service_name**
  Specifies the name of the P-GW service. If `service_name` does not refer to an existing service, the new service is created if resources allow. `service_name` is an alphanumeric string of 1 through 63 characters.

**Important:** Service names must be unique across all contexts within a chassis.

- **-noconfirm**
  Executes the command without any additional prompt and confirmation from the user.

- **no pgw-service service_name**
  Removes the specified P-GW service from the context.

Usage:

Enter the P-GW Service Configuration Mode for an existing service or for a newly defined service. This command is also used to remove an existing service. A maximum of 256 services (regardless of type) can be configured per system.

**Caution:** Large numbers of services greatly increase the complexity of management and may impact overall system performance (for example, resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.
Entering this command results in the following prompt:

```plaintext
[context_name] hostname(config-pgw-service)#
```

P-GW Service Configuration Mode commands are defined in the *P-GW Service Configuration Mode Commands* chapter.

Use this command when configuring the following eHRPD and SAE components: P-GW.

**Example**

The following command enters the existing P-GW Service Configuration Mode (or creates it if it does not already exist) for the service named `pgw-service1`:

```
pgw-service pgw-service1
```

The following command will remove `pgw-service1` from the system:

```
no pgw-service pgw-service1
```
pilot-packet

Configures Pilot Packets containing key pieces of information about a subscriber session to third party network elements.

Product
HA
NAT
PDSN
P-GW

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration
configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

pilot-packet { attribute { foreign-agent-ip-address | nai | rat-type | serving-nw-id } | source-ip-address source_ip_address destination-ip-address destination_ip_address

no pilot-packet

---

no

Disables the Pilot packet option.

---

name server_name

Specifies Pilot packet server name.

---

source-ip-address source_ip_address

Specifies the IP addresses for the sourcing and terminating Pilot Packets. The IP address must be entered using IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

- source_ip_address: Specifies the IP address of the source for sending Pilot Packets.
- destination_ip_address: Specifies the IP address of the destination for the Pilot Packets.

---

destination-udp-port udp_port_value

Specifies the UDP port value as an integer from 1 through 65535.

---

dscp-marking dscp_value

Enables DSCP marking. DSCP is used for control plane packets. dscp_value must be a hexadecimal number between 0x0 and 0x3F.
**Important:** For Pilot Packet, the generated UDP packet is currently expected to use DSCP 0x20 (32).

**Usage**

Use this command to configure Pilot Packet parameters.

**Example**

The following command configures pilot packets with source and destination IPv4/IPv6 addresses along with the destination port:

```
  pilot-packet source-ip-address 10.2.3.4 destination-ip-address 10.3.4.5
  destination-udp-port 221
```
policy

Enters an existing accounting policy or creates a new one where accounting parameters are configured.

**Product**

- HSGW
- P-GW
- S-GW
- SAEGW

**Privilege**

Administrator

**Mode**

Exec > Global Configuration > Context Configuration

```plaintext
configure > context context_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
[ no ] policy accounting name
```

- **no**
  
  Removes the specified accounting policy from the context.

- **name**
  
  Specifies the name of the existing or new accounting policy as an alphanumeric string of 1 through 63 characters.

**Usage**

Use this command to enter the Accounting Policy Configuration mode to edit an existing accounting policy or configure a new policy.

Entering this command results in the following prompt:

```
[context_name]hostname(config-accounting-policy)#
```

Accounting Policy Configuration Mode commands are defined in the *Accounting Policy Configuration Mode Commands* chapter.

**Example**

The following command enters the Accounting Policy Configuration Mode for a policy named *acct5*:

```
policy accounting acct5
```
policy-group

Creates or deletes a policy group. It enters the Policy-Group Configuration Mode within the current destination context for flow-based traffic policing to a subscriber session flow.

Product
- PDSN
- HA
- ASN-GW
- HSGW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration

configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

[ no ] policy-group name policy_group

- no
  Deletes configured policy group within the context.

- name policy_group
  Specifies the name of Policy-Group as an alphanumeric string of 1 through 15 characters that is case sensitive.

Usage
Use this command to form a policy group from a set of configured Policy-Maps. A policy group supports up to 16 policies for a subscriber session flow.

Example

The following command configures a policy group policy_group1 for a subscriber session flow:

    policy-group name policy_group1
policy-map

Creates or deletes a policy map. It enters the Traffic Policy-Map Configuration Mode within the current destination context to configure the flow-based traffic policing for a subscriber session flow.

Product
PDSN
HA
ASN-GW
HSGW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration
configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

[ no ] policy-map name policy_name

  no
  Deletes configured Policy-Map within the context.

  name policy_name
  Specifies the name of Policy-Map as an alphanumeric string of 1 through 15 characters that is case sensitive.

Usage

Use this command to enter Traffic Policy-Map Configuration Mode and to set the Class-Map and corresponding traffic flow treatment to traffic policy for a subscriber session flow.

Example

Following command configures a policy map policy1 where other flow treatments is configured.

    policy-map name policy1
Context Configuration Mode Commands

**ppp**

Configures point-to-point protocol parameters for the current context.

**Product**

- PDSN
- GGSN

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration

```bash
configure > context context_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```bash
ppp { acfc { receive { allow | deny } | transmit { apply | ignore | reject } } | auth-retry suppress-aaa-auth | chap fixed-challenge-length length | dormant send-lcp-terminate | echo-max-retransmissions num_retries | echo-retransmit-timeout msec | first-lcp-retransmit-timeout milliseconds | lcp-authentication-discard retry-alternate num_discard | lcp-authentication-reject retry-alternate | lcp-start-delay delay | lcp-terminate connect-state | lcp-terminate mip-lifetime-expiry | lcp-terminate mip-revocation | max-authentication-attempts num | max-configuration-nak num | max-retransmissions number | max-terminate number | mru packet_size | negotiate default-value-options | peer-authentication user_name [ encrypted ] password password | pfc { receive { allow | deny } | transmit { apply | ignore | reject } } | reject-peer-authentication | renegotiation retain-ip-address | retransmit-timeout milliseconds }

no ppp { auth-retry suppress-aaa-auth | chap fixed-challenge-length | dormant send-lcp-terminate | lcp-authentication-descard retry-alternate num_discard | lcp-authentication-reject retry-alternate | lcp-start-delay | lcp-terminate connect-state | reject-peer-authentication | renegotiation retain-ip-address }

default lcp-authentication-descard retry-alternate num_discard
```

**default**

Restores the system defaults for the specific command/keyword.

**no**

Disables, deletes, or resets the specified option.

For **no ppp renegotiation retain-ip-address** the initially allocated IP address will be released and a new IP address will be allocated during PPP renegotiation.

```bash
acfc { receive { allow | deny } | transmit { apply | ignore | reject } }
```

Configures PPP Address and Control Field Compression (ACFC) parameters.

```bash
receive { allow | deny }
```
This keyword specifies whether to allow Address and Control Field Compressed PPP packets received from the Peer. During LCP negotiation, the local PPP side indicates whether it can handle ACFC compressed PPP packets. Default: allow
When allow is specified, the local PPP side indicates that it can process ACFC compressed PPP packets and compressed packets are allowed. When deny is specified, the local PPP side indicates that it cannot handle ACFC compressed packets and compressed packets are not allowed.

transmit { apply | ignore | reject }
Specifies how Address and Control Field Compression should be applied for PPP packets transmitted to the Peer. During LCP negotiation, the Peer indicates whether it can handle ACFC compressed PPP packets. Default: ignore
When apply is specified, if the peer requests ACFC, the request is accepted and ACFC is applied for transmitted PPP packets. When ignore is specified, if the peer requests ACFC, the request is accepted, but ACFC is not applied for transmitted PPP packets. When reject is specified, if the peer requests ACFC, the request is rejected and ACFC is not applied to transmitted packets.

auth-retry suppress-aaa-auth
This option does not allow PPP authentication retries to the AAA server after the AAA server has already authenticated a session. PPP locally stores the username and password, or challenge response, after a successful PPP authentication. If the Mobile Node retries the PAP request or CHAP-Response packet to the PDSN, PPP locally compares the incoming username, password or Challenge Response with the information stored from the previous successful authentication. If it matches, PAP ACK or CHAP Success is sent back to the Mobile Node, without performing AAA authentication. If the incoming information does not match with what is stored locally, then AAA authentication is attempted. The locally stored PPP authentication information is cleared once the session reaches a connected state. Default: no auth-retry suppress-aaa-auth

Important: This option is not supported in conjunction with the GGSN product.

chap fixed-challenge-length length
Normally PPP CHAP use a random challenge length from 17 to 32 bytes. This command allows you to configure a specific fixed challenge length of from 4 through 32 bytes. length must be an integer from 4 through 32.
Default: Disabled. PAPCHAP uses a random challenge length.

dormant send-lcp-terminate
Indicates a link control protocol (LCP) terminate message is enabled for dormant sessions.

Important: This option is not supported in conjunction with the GGSN product.

echo-max-retransmissions num_retries
Configures the maximum number of retransmissions of LCP ECHO_REQ before a session is terminated in an always-on session. num_retries must be an integer from 1 through 16. Default: 3

echo-retransmit-timeout msec
Configures the timeout (in milliseconds) before trying LCP ECHO_REQ for an always-on session. msec must be an integer from 100 through 5000. Default: 3000
first-lcp-retransmit-timeout  milliseconds

Specifies the number of milliseconds to wait before attempting to retransmit control packets. This value configures the first retry. All subsequent retries are controlled by the value configured for the ppp retransmit-timeout keyword.

milliseconds must be an integer from 100 through 5000. Default: 3000

lcp-authentication-discard retry-alternate num_discard

Sets the number of discards up to which authentication option is discarded during LCP negotiation and retries start to allow alternate authentication option. num_discard must be an integer from 0 through 5. Recommended value is 2. Default: Disabled.

lcp-authentication-reject retry-alternate

Specifies the action to be taken if the authentication option is rejected during LCP negotiation and retries the allowed alternate authentication option.

Default: Disabled. No alternate authentication option will be retried.

lcp-start-delay delay

Specifies the delay (in milliseconds) before link control protocol (LCP) is started. delay must be an integer from 0 through 5000. Default: 0

lcp-terminate connect-state

Enables sending an LCP terminate message to the Mobile Node when a PPP session is disconnected if the PPP session was already in a connected state.

Note that if the no keyword is used with this option, the PDSN must still send LCP Terminate in the event of an LCP/PCP negotiation failure or PPP authentication failure, which happens during connecting state.

Important: This option is not supported in conjunction with the GGSN product.

lcp-terminate mip-lifetime-expiry

Configures the PDSN to send an LCP Terminate Request when a MIP Session is terminated due to MIP Lifetime expiry (default).

Note that if the no keyword is used with this option, the PDSN does not send a LCP Terminate Request when a MIP session is terminated due to MIP Lifetime expiry.

lcp-terminate mip-revocation

Configures the PDSN to send a LCP Terminate Request when a MIP Session is terminated due to a Revocation being received from the HA (default).

Note that if the no keyword is used with this option, the PDSN does not send a LCP Terminate Request when a MIP session is terminated due to a Revocation being received from the HA.

max-authentication-attempts num

Configures the maximum number of time the PPP authentication attempt is allowed. num must be an integer from 1 through 10. Default: 1
**max-configuration-nak num**

This command configures the maximum number of consecutive configuration REJ/NAKs that can be sent during CP negotiations, before the CP is terminated. `num` must be an integer from 1 through 20. Default: 10

**max-retransmission number**

Specifies the maximum number of times control packets will be retransmitted. `number` must be an integer from 1 through 16. Default: 5

**max-terminate number**

Sets the maximum number of PPP LCP Terminate Requests transmitted to the Mobile Node. `number` must be an integer from 0 through 16. Default: 2

**Important:** This option is not supported in conjunction with the GGSN product.

**mru packet_size**

Specifies the maximum packet size that can be received in bytes. `packet_size` must be an integer from 128 through 1500. Default: 1500

**negotiate default-value-options**

Enables the inclusion of configuration options with default values in PPP configuration requests. Default: Disabled

The PPP standard states that configuration options with default values should not be included in Configuration Request (LCP, IPCP, etc.) packets. If the option is missing in the Configuration Request, the peer PPP assumes the default value for that configuration option.

When **negotiate default-value-options** is enabled, configuration options with default values are included in the PPP configuration Requests.

**peer-authenticate user_name [ [ encrypted ] password password ]**

Specifies the username and an optional password required for point-to-point protocol peer connection authentications. `user_name` is an alphanumeric string of 1 through 63 characters. The keyword `password` is optional and if specified `password` is an alphanumeric string of 1 through 63 characters. The password specified must be in an encrypted format if the optional keyword `encrypted` was specified.

The `encrypted` keyword is intended only for use by the system while saving configuration scripts. The system displays the `encrypted` keyword in the configuration file as a flag that the variable following the `password` keyword is the encrypted version of the plain text password. Only the encrypted password is saved as part of the configuration file.

**pfc { receive { allow | deny } | transmit { apply | ignore | reject } }**

Configures Protocol Field Compression (PFC) parameters.

**receive { allow | deny }** Default: `allow`

This keyword specifies whether to allow Protocol Field Compression (PFC) for PPP packets received from the peer. During LCP negotiation, the local PPP side indicates whether it can handle Protocol Field Compressed PPP packets.

When `allow` is specified, the peer is allowed to request PFC during LCP negotiation. When `deny` is specified, the Peer is not allowed to request PFC during LCP negotiation.

**transmit { apply | ignore | reject }** Default: `ignore`
This keyword specifies how Protocol field Compression should be applied for PPP packets transmitted to the Peer. During LCP negotiation, the Peer indicates whether it can handle PFC compressed PPP packets. When `apply` is specified, if the peer requests PFC, it is accepted and PFC is applied for transmitted PPP packets. When `ignore` is specified, If the peer requests PFC, it is accepted but PFC is not applied for transmitted packets. When `reject` is specified, all requests for PCF from the peer are rejected.

```
reject-peer-authentication
```

If disabled, re-enables the system to reject peer requests for authentication. Default: Enabled

```
renegotiation retain-ip-address
```

If enabled, retain the currently allocated IP address for the session during PPP renegotiation (SimpleIP) between FA and Mobile node. Default: Enabled

If disabled, the initially allocated IP address will be released and a new IP address will be allocated during PPP renegotiation.

```
retransmit-timeout milliseconds
```

Specifies the number of milliseconds to wait before attempting to retransmit control packets. `milliseconds` must be an integer from 100 through 5000. Default: 3000

### Usage
Modify the context PPP options to ensure authentication and communication for PPP sessions have fewer dropped sessions.

### Example
The following commands set various PPP options:

```
ppp dormant send-lcp-terminate
ppp max-retransmission 3
ppp peer-authenticate user1 password secretPwd
ppp peer-authenticate user1
ppp retransmit-timeout 1000
```

The following command disables the sending of LCP terminate messages for dormant sessions.

```
no ppp dormant send-lcp-terminate
```
**ppp magic-number**

Manages magic number checking during LCP Echo message handling. The magic number is a random number chosen to distinguish a peer and detect looped back lines.

**Product**
- PDSN
- GGSN

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration > Context Configuration

```
configure > context context_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
[ no | default ] ppp magic-number receive ignore
```

- **no**
  - Disables the specified behavior.

- **default**
  - Restores the system defaults for the specific command/keyword.

- **receive ignore**
  - Ignores the checking of magic number at the PDSN during LCP Echo message handling. Default: Disabled. If a valid magic numbers were negotiated for the PPP endpoints during LCP negotiation and LCP Echo Request/Response have invalid magic numbers, enabling this command will cause the system to ignore the checking of magic number during LCP Echo message handling.

**Usage**

Use this command to allow the system to ignore invalid magic number during LCP Echo Request/Response handling.

**Example**

The following command allows the invalid magic number during LCP Echo Request/Response negotiation:

```
ppp magic-number receive ignore
```
ppp statistics

Changes the manner in which some PPP statistics are calculated.

Product

PDSN
GGSN

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > Context Configuration
configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

[ no ] ppp statistics success-sessions { lcp-max-retry | misc-reasons | remote-terminated }

no
Disable the specified behavior.

ppp statistics success-sessions lcp-max-retry
Alters statistical calculations so that: ppp successful session = successful sessions + lcp-max-retry.

success-sessions misc-reasons
Alters statistical calculations so that: ppp successful session = successful sessions + misc-reasons.

success-sessions remote-terminated
Alters statistical calculations so that: ppp successful session = successful sessions + remote-terminated.

Usage

Use this command to alter how certain PPP statistics are calculated.

⚠️ Caution: This command alters the way that some PPP statistics are calculated. Please consult your designated service representative before using this command

Example

The following command alters the statistic “ppp successful session” so that it displays the sum of successful sessions and lcp-max-retry:

ppp statistics success-sessions lcp-max-retry

The following command disables the alteration of the statistic ppp successful session:
no ppp statistics success-sessions lcp-max-retry
## proxy-dns intercept-list

Enters the HA Proxy DNS Configuration Mode and defines a name of a redirect rules list for the domain name servers associated with a particular FA (Foreign Agent) or group of FAs.

### Important

HA Proxy DNS Intercept is a license-enabled feature.

<table>
<thead>
<tr>
<th>Product</th>
<th>HA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privilege</td>
<td>Security Administrator, Administrator</td>
</tr>
</tbody>
</table>

### Mode

```
Exec > Global Configuration > Context Configuration
configure > context context_name
```

Entering the above command sequence results in the following prompt:

```
[context_name] host_name(config-ctx)#
```

### Syntax

```
[ no ] proxy-dns intercept-list name
```

<table>
<thead>
<tr>
<th>no</th>
</tr>
</thead>
<tbody>
<tr>
<td>Removes the intercept list from the system.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defines the rules list and enters the Proxy DNS Configuration Mode. <code>name</code> must be an alphanumeric string of 1 through 63 characters.</td>
</tr>
</tbody>
</table>

### Usage

Use this command to define a name for a list of rules pertaining to the IP addresses associated with the foreign network’s DNS. Up to 128 rules of any type can be configured per rules list.

Upon entering the command, the system switches to the HA Proxy DNS Configuration Mode where the lists can be defined. Up to 64 separate rules lists can be configured in a single AAA context.

This command and the commands in the HA Proxy DNS Configuration Mode provide a solution to the Mobile IP problem that occurs when a MIP subscriber, with a legacy MN or MN that does not support IS-835D, receives a DNS server address from a foreign network that is unreachable from the home network. The following flow shows the steps that occur when this feature is enabled:
By configuring the Proxy DNS feature on the Home Agent, the foreign DNS address is intercepted and replaced with a home DNS address while the call is being handled by the home network.

**Example**

The following command creates a proxy DNS rules list named `list1` and places the CLI in the HA Proxy DNS Configuration Mode:

```
proxy-dns intercept-list list1
```
radius accounting

This command configures RADIUS accounting parameters for the current context.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration
configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

radius accounting { archive [ stop-only ] | deadtime dead_minutes | detect-dead-server { consecutive-failures consecutive_failures | keepalive | response-timeout timeout_duration } | interim interval seconds | max-outstanding max_messages | max-pdu-size octets | max-retries max_retries | max-transmissions max_transmissions | timeout timeout_duration | unestablished-sessions }

default radius accounting { deadtime | detect-dead-server | interim interval seconds | max-outstanding | max-pdu-size | max-retries | max-transmissions | timeout }

no radius accounting { archive | detect-dead-server | interim interval | max-transmissions | unestablished-sessions }

default
Configures the default settings.

no
Removes earlier configuration for the specified keyword.

archive [ stop-only ]

Enables archiving of RADIUS Accounting messages in the system after the accounting message has exhausted retries to all available RADIUS Accounting servers. All RADIUS Accounting messages generated by a session are delivered to the RADIUS Accounting server in serial. That is, previous RADIUS Accounting messages from the same call must be delivered and acknowledged by the RADIUS Accounting server before the next RADIUS Accounting message is sent to the RADIUS Accounting server. stop-only specifies archiving of STOP accounting messages only.
Default: Enabled

deadtime dead_minutes

Specifies the number of minutes to wait before attempting to communicate with a server which has been marked as unreachable.
dead_minutes must be an integer from 0 through 65535.
Default: 10

```
detect-dead-server { consecutive-failures consecutive_failures | keepalive | response-timeout timeout_duration }
```

- **consecutive-failures consecutive_failures**: Specifies the number of consecutive failures, for each AAA manager, before a server is marked as unreachable.
  
  `consecutive_failures` must be an integer from 0 through 1000.

  Default: 4

- **keepalive**: Enables the AAA server alive-dead detect mechanism based on sending keep alive authentication messages to all authentication servers.

  Default: Disabled

- **response-timeout timeout_duration**: Specifies the number of seconds for each AAA manager to wait for a response to any message before a server is detected as failed, or in a down state.

  `timeout_duration` must be an integer from 1 through 65535.

**Important**: If both `consecutive-failures` and `response-timeout` are configured, then both parameters have to be met before a server is considered unreachable, or dead.

```
interim interval seconds
```

Specifies the time interval (in seconds) for sending accounting INTERIM-UPDATE records. `seconds` must be an integer from 50 through 40000000.

**Important**: If RADIUS is used as the accounting protocol for the GGSN product, other commands are used to trigger periodic accounting updates. However, these commands would cause RADIUS STOP/START packets to be sent as opposed to INTERIM-UPDATE packets. Also note that accounting interim interval settings received from a RADIUS server take precedence over those configured on the system.

Default: Disabled

```
max-outstanding max_messages
```

Specifies the maximum number of outstanding messages a single AAA manager instance will queue. `max_messages` must be an integer from 1 through 4000. Default: 256

```
max-pdu-size octets
```

Specifies the maximum sized packet data unit which can be accepted/generated in bytes (octets). `octets` must be an integer from 512 through 4096. Default: 4096

```
max-retries max_retries
```

Specifies the maximum number of times communication with a AAA server will be attempted before it is marked as unreachable and the detect dead servers consecutive failures count is incremented. `max_retries` must be an integer from 0 through 65535. Default: 5

Once the maximum number of retries is reached this is considered a single failure for the consecutive failures count for detecting dead servers.
radius accounting

**max-transmissions max_transmissions**
Sets the maximum number of transmissions for a RADIUS accounting message before the message is declared as failed. `max_transmissions` must be an integer from 1 through 65535. Default: Disabled

**timeout seconds**
Specifies the amount of time to wait for a response from a RADIUS server before retransmitting a request. `seconds` must be an integer from 1 through 65535. Default: 3

**unestablished-sessions**
Indicates RADIUS STOP events are to be generated for sessions that were initiated but never fully established.

---

**Usage**
Manage the RADIUS accounting options according to the RADIUS server used for the context.

**Example**
The following commands configure accounting options.

```
radius accounting detect-dead-server consecutive-failures 5
radius accounting max-pdu-size 1024
radius accounting timeout 16
```
radius accounting algorithm

This command specifies the fail-over/load-balancing algorithm to select the RADIUS accounting server(s) to which accounting data must be sent.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration
  configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

radius accounting algorithm { first-n n | first-server | round-robin }

default radius accounting algorithm

default

Configures the default setting.
Default: first-server

first-n n

Specifies that the AGW must send accounting data to n (more than one) AAA accounting servers based on their priority. The full set of accounting data is sent to each of the n AAA servers. Response from any one of the servers would suffice to proceed with the call. On receiving an ACK from any one of the accounting servers, all retries are stopped.

n is the number of AAA accounting servers to which accounting data will be sent, and must be an integer from 2 through 128. Default: 1 (Disabled)

first-server

Specifies that the context must send accounting data to the RADIUS accounting server with the highest configured priority. In the event that this server becomes unreachable, accounting data is sent to the accounting server with the next-highest configured priority. This is the default algorithm.

round-robin

Specifies that the context must load balance sending accounting data among all of the defined RADIUS accounting servers. Accounting data is sent in a circular queue fashion on a per Session Manager task basis, where data is sent to the next available accounting server and restarts at the beginning of the list of configured servers. The order of the list is based upon the configured relative priority of the servers.
Usage

Use this command to specify the algorithm to select the RADIUS accounting server(s) to which accounting data must be sent.

Example

The following command specifies to use the round-robin algorithm to select the RADIUS accounting server:

```
radius accounting algorithm round-robin
```
radius accounting apn-to-be-included

This command configures the Access Point Name (APN) to be included for RADIUS accounting.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration

```
configure > context context_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
radius accounting apn-to-be-included { gi | gn }
```

```
default radius accounting apn-to-be-included
```

- **default**
  Configures the default setting.

- **gi**
  Specifies the usage of the Gi APN name in the RADIUS accounting request. The Gi APN represents the APN received in the Create PDP context request message from the SGSN.

- **gn**
  Specifies the usage of the Gn APN name in the RADIUS accounting request. The Gn APN represents the APN selected by the GGSN.

**Usage**

Use this command to configure the APN name for RADIUS Accounting. This can be set to either gi or gn.

**Example**

The following command specifies the usage of Gn APN name in the RADIUS accounting request:

```
radius accounting apn-to-be-included gn
```
radius accounting billing-version

This command configures the billing-system version of RADIUS accounting servers.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration

```
configure > context context_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
radius accounting billing-version version

default radius accounting billing-version
```

**Usage**

Use this command to configure the billing-system version of RADIUS accounting servers.

**Example**

The following command configures the billing-system version of RADIUS accounting servers as 10:

```
radius accounting billing-version 10
```
radius accounting gtp trigger-policy

This command configures the RADIUS accounting trigger policy for GTP messages.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration
configure > context context_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
radius accounting gtp trigger-policy [ standard | ggsn-preservation-mode ]
```

default radius accounting gtp trigger-policy

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Resets the RADIUS accounting trigger policy to standard behavior for GTP session.</td>
</tr>
<tr>
<td>standard</td>
<td>Sets the RADIUS accounting trigger policy to standard behavior which is configured for GTP session for GGSN service.</td>
</tr>
<tr>
<td>ggsn-preservation-mode</td>
<td>Sends RADIUS Accounting Start when the GTP message with private extension of preservation mode is received from SGSN.</td>
</tr>
</tbody>
</table>

**Important:**
This is a customer-specific keyword and needs customer-specific license to use this feature. For more information on GGSN preservation mode, refer to GGSN Service Configuration Mode Commands chapter.

**Usage**
Use this command to set the trigger policy for the AAA accounting for a GTP session.

**Example**
The following command sets the RADIUS accounting trigger policy for GTP session to standard:

```
default radius accounting gtp trigger-policy
```
radius accounting ha policy

This command configures the RADIUS accounting policy for HA sessions.

**Product**
HA

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration

`configure > context context_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
radius accounting ha policy { session-start-stop | custom1-aaa-res-mgmt }
```

**default radius accounting ha policy**

**session-start-stop**

Specifies to send Accounting Start when the session is connected, and send Accounting Stop when the session is disconnected. This is the default behavior.

**custom1-aaa-res-mgmt**

Accounting Start/Stop messages are generated to assist special resource management done by AAA servers. It is similar to the session-start-stop accounting policy, except for the following differences:

- Accounting Start is generated when a new call overwrites an existing session. Accounting Start is also generated during MIP session handoffs.
- No Accounting stop is generated when an existing session is overwritten and the new session continues to use the IP address assigned for the old session.

**Usage**

Use this command to set the behavior of the AAA accounting for an HA session.

**Example**

The following command sets the HA accounting policy to `custom1-aaa-res-mgmt`:

```
radius accounting ha policy custom1-aaa-res-mgmt
```
radius accounting interim volume

This command configures the volume of uplink and downlink volume octet counts that triggers RADIUS interim accounting.

Product
GGSN
PDSN
HA

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration
configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

radius accounting interim volume { downlink bytes uplink bytes | total bytes | uplink bytes downlink bytes }

no radius accounting interim volume

---

no

Disables volume based RADIUS accounting.

downlink bytes uplink bytes

Specifies the downlink to uplink volume limit for RADIUS Interim accounting, in bytes. bytes must be an integer to 100000 through 4000000000.

total bytes

Specifies the total volume limit for RADIUS interim accounting in bytes. bytes must be an integer from 100000 through 4000000000.

uplink bytes

Specifies the uplink volume limit for RADIUS interim accounting in bytes. bytes must be an integer from 100000 through 4000000000.

downlink bytes

Specifies the downlink volume limit for RADIUS interim accounting in bytes. bytes must be an integer from 100000 through 4000000000.
Usage
Use this command to trigger RADIUS interim accounting based on the volume of uplink and downlink bytes.

Example
The following command triggers RADIUS interim accounting when the total volume of uplink and downlink bytes reaches 110000:

radius accounting interim volume total 110000
radius accounting ip remote-address

This command configures IP remote address-based RADIUS accounting parameters.

Product
PDSN
HA

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration
 configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

[ no ] radius accounting ip remote-address { collection | list list_id }

<table>
<thead>
<tr>
<th>no</th>
</tr>
</thead>
<tbody>
<tr>
<td>Removes earlier configuration for the specified keyword.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>collection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enables collecting and reporting Remote-Address-Based accounting in RADIUS Accounting. This should be enabled in the AAA Context. It is disabled by default.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>list list_id</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enters the Remote Address List Configuration Mode. This mode configures a list of remote addresses that can be referenced by the subscriber's profile. list_id must be an integer from 1 through 65535.</td>
</tr>
</tbody>
</table>

Usage
This command is used as part of the Remote Address-based Accounting feature to both configure remote IP address lists and enable the collection of accounting data for the addresses in those lists on a per-subscriber basis.

Individual subscriber can be associated to remote IP address lists through the configuration/specification of an attribute in their local or RADIUS profile. (Refer to the radius accounting command in the Subscriber Configuration mode.) When configured/specified, accounting data is collected pertaining to the subscriber's communication with any of the remote addresses specified in the list.

Once this functionality is configured on the system and in the subscriber profiles, it must be enabled by executing this command with the collection keyword.

Example
The following command enables collecting and reporting Remote-Address-Based accounting in RADIUS Accounting:

radius accounting ip remote-address collection
radius accounting keepalive

This command configures the keepalive authentication parameters for the RADIUS accounting server.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration
configure > context context_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
radius accounting keepalive { calling-station-id id | consecutive-response responses_no_of | framed-ip-address ip_address | interval interval_duration | retries retries_no_of | timeout timeout_duration | username user_name }
```

```
no radius accounting keepalive framed-ip-address
```

```
default radius accounting keepalive { calling-station-id | consecutive-response | interval | retries | timeout | username }
```

```
no
```

Removes configuration for the specified keyword.

```
default
```

Configures the default settings.

```
calling-station-id id
```

Configures the Calling-Station ID to be used for the keepalive authentication as an alphanumeric string of size 1 to 15 characters. Default: 000000000000000

```
consecutive-response responses_no_of
```

Configures the number of consecutive authentication response after which the server is marked as reachable. responses_no_of must be an integer from 1 through 5. Default: 1

```
framed-ip-address ip_address
```

Specifies the framed ip-address to be used for the keepalive accounting in IPv4 dotted-decimal notation.

```
interval interval_duration
```

Configures the time interval (in seconds) between the two keepalive access requests. Default:30
retries retries_no_of

Configures the number of times the keepalive access request to be sent before marking the server as unreachable. retries_no_of must be an integer from 3 through 10. Default: 3

timeout timeout_duration

Configures the time interval between each keepalive access request retries. timeout_duration must be an integer from 1 through 30. Default: 3

username user_name

Configures the username to be used for the authentication as an alphanumeric string of 1 through 127 characters. Default: Test-Username

Usage

Configures the keepalive authentication parameters for the RADIUS accounting server.

Example

The following command sets the user name for the RADIUS keepalive access requests to Test-Username2:

    radius accounting keepalive username Test-Username2

The following command sets the number of retries to 4:

    radius accounting keepalive retries 4
radius accounting rp

This command configures the current context’s RADIUS accounting R-P originated call options.

Product
PDSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration
configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

radius accounting rp { handoff-stop { immediate | wait-active-stop } | tod minute hour | trigger-event { active-handoff | active-start-param-change | active-stop } | trigger-policy { airlink-usage [ counter-rollover ] | custom [ active-handoff | active-start-param-change | active-stop ] | standard } | trigger-stop-start }

no radius accounting rp { tod minute hour | trigger-event { active-handoff | active-start-param-change | active-stop } | trigger-stop-start }

default radius accounting rp { handoff-stop | trigger-policy }

no
Removes earlier configuration for the specified keyword.

default
Configures this command with the default settings.

handoff-stop { immediate | wait-active-stop }

Specifies the behavior of generating accounting STOP when handoff occurs.

•immediate: Indicates that accounting STOP should be generated immediately on handoff, i.e. not to wait active-stop from the old PCF.

•wait-active-stop: Indicates that accounting STOP is generated only when active-stop received from the old PCF when handoff occurs.

Default: wait-active-stop

tod minute hour

Specifies the time of day a RADIUS event is to be generated for accounting. Up to four different times of the day may be specified through separate commands.

minute must be an integer from 0 through 59.
hour must be an integer from 0 through 23.
trigger-event { active-handoff | active-start-param-change | active-stop }

Configures the events for which a RADIUS event is generated for accounting as one of the following:

• **active-handoff**: Disables a single R-P event (and therefore a RADIUS accounting event) when an Active PCF-to-PFC Handoff occurs. Instead, two R-P events occur (one for the Connection Setup, and the second for the Active-Start). Default: Disabled

• **active-start-param-change**: Disables an R-P event (and therefore a RADIUS accounting event) when an Active-Start is received from the PCF and there has been a parameter change. Default: Enabled

• **active-stop**: Disables an R-P event (and therefore a RADIUS accounting event) when an Active-Stop is received from the PCF. Default: Disabled

**Important**: This keyword has been obsoleted by the trigger-policy keyword. Note that if this command is used, if the context configuration is displayed, RADIUS accounting RP configuration is represented in terms of the trigger-policy.

trigger-policy { airlink-usage [ counter-rollover ] | custom [ active-handoff | active-start-param-change | active-stop ] | standard }

Default: **airlink-usage**: Disabled

**custom**:

• **active-handoff**: Disabled

• **active-start-param-change**: Disabled

• **active-stop**: Disabled

• **standard**: Enabled

Configures the overall accounting policy for R-P sessions as one of the following:

• **airlink-usage [ counter-rollover ]**: Designates the use of Airlink-Usage RADIUS accounting policy for R-P, which generates a start on Active-Starts, and a stop on Active-Stops.

If the **counter-rollover** option is enabled, the system generates a STOP/START pair before input/output data octet counts (or input/output data packet counts) become larger than \((2^{32} - 1)\) in value. This setting is used to guarantee that a 32-bit octet count in any STOP message has not wrapped to larger than \(2^{32}\) thus ensuring the accuracy of the count. The system, may send the STOP/START pair at any time, so long as it does so before the 32-bit counter has wrapped. Note that a STOP/START pair is never generated unless the subscriber RP session is in the Active state, since octet/packet counts are not accumulated in the Dormant state.

• **custom**: specifies the use of custom RADIUS accounting policy for R-P. The custom policy can consist of the following:

• **active-handoff**: Enables a single R-P event (and therefore a RADIUS accounting event) when an Active PCF-to-PFC Handoff occurs. Normally two R-P events will occur (one for the Connection Setup, and the second for the Active-Start).

• **active-start-param-change**: Enables an R-P event (and therefore a RADIUS accounting event) when an Active-Start is received from the PCF and there has been a parameter change.

**Important**: Note that a custom trigger policy with only **active-start-param-change** enabled is identical to the **standard** trigger-policy.
- **active-stop**: Enables an R-P event (and therefore a RADIUS accounting event) when an Active-Stop is received from the PCF.

**Important:** If the `radius accounting rp trigger-policy custom` command is executed without any of the optional keywords, all custom options are disabled.

- **standard**: Specifies the use of Standard RADIUS accounting policy for R-P in accordance with IS-835B.

**trigger-stop-start**

Specifies that a stop/start RADIUS accounting pair should be sent to the RADIUS server when an applicable R-P event occurs.

**Usage**

Use this command to configure the events for which a RADIUS event is sent to the server when the accounting procedures vary between servers.

**Example**

The following command enables an R-P event (and therefore a RADIUS accounting event) when an Active-Stop is received from the PCF:

```
radius accounting rp trigger-event active-stop
```

The following command generates the STOP only when active-stop received from the old PCF when handoff occurs:

```
default radius accounting rp handoff-stop
```
radius accounting server

This command configures RADIUS accounting server(s) in the current context.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration
configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

radius [ mediation-device ] accounting server ip_address [ encrypted ] key value [ acct-on { enable | disable } ] [ acct-off { enable | disable } ] [ max max_messages ] [ oldports ] [ port port_number ] [ priority priority ] [ type { mediation-device | standard } ] [ admin-status { enable | disable } ] [ -noconfirm ]

no radius [ mediation-device ] accounting server ip_address [ oldports | port port_number ]

no

Removes the server or server port(s) specified from the list of configured servers.

mediation-device

Enables mediation-device specific AAA transactions used to communicate with this RADIUS server.

Important: If this option is not used, the system by default enables standard AAA transactions.

ip_address

Specifies the IP address of the accounting server.

ip_address must be specified in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation. A maximum of 128 RADIUS servers can be configured per context. This limit includes accounting and authentication servers.

[ encrypted ] key value

Specifies the shared secret key used to authenticate the client to the servers. The encrypted keyword indicates the key specified is encrypted.

In 12.1 and earlier releases, the key value must be an alphanumeric string of 1 through 127 characters without encryption, and 1 through 256 characters with encryption.

In 12.2 and later releases, the key value must be an alphanumeric string of 1 through 127 characters without encryption, and 1 through 236 characters with encryption enabled.
The `encrypted` keyword is intended only for use by the system while saving configuration scripts. The system displays the `encrypted` keyword in the configuration file as a flag that the variable following the `key` keyword is the encrypted version of the plaintext key. Only the encrypted key is saved as part of the configuration file.

```plaintext
acct-on { enable | disable }
```

This keyword enables/disables sending of the Accounting-On message when a new RADIUS server is added to the configuration. By default, this keyword will be disabled. When enabled, the Accounting-On message is sent when a new RADIUS server is added in the configuration. However, if for some reason the Accounting-On message cannot be sent at the time of server configuration (for example, if the interface is down), then the message is sent as soon as possible. Once the Accounting-On message is sent, if it is not responded to after the configured RADIUS accounting timeout, the message is retried the configured number of RADIUS accounting retries. Once all retries have been exhausted, the system no longer attempts to send the Accounting-On message for this server.

```plaintext
acct-off { enable | disable }
```

Default: `enable`

Disables and enables the sending of the Accounting-Off message when a RADIUS server is removed from the configuration. The Accounting-Off message is sent when a RADIUS server is removed from the configuration, or when there is an orderly shutdown. However, if for some reason the Accounting-On message cannot be sent at this time, it is never sent. The Accounting-Off message is sent only once, regardless of how many accounting retries are enabled.

```plaintext
max max_messages
```

Specifies the maximum number of outstanding messages that may be allowed to the server. `max_messages` must be an integer from 0 through 4000. Default: 0

```plaintext
oldports
```

Sets the UDP communication port to the out of date standardized default for RADIUS communications to 1646.

```plaintext
port port_number
```

Specifies the port number to use for communications as an integer from 1 through 65535. Default: 1813

```plaintext
priority priority
```

Specifies the relative priority of this accounting server. The priority is used in server selection for determining which server to send accounting data to. `priority` must be an integer from 1 through 1000, where 1 is the highest priority. When configuring two or more servers with the same priority you will be asked to confirm that you want to do this. If you use the `-noconfirm` option, you are not asked for confirmation and multiple servers could be assigned the same priority. Default: 1000

```plaintext
type { mediation-device | standard }
```

Specifies the type of AAA transactions to use to communicate with this RADIUS server.

- **standard**: Use standard AAA transactions.
- **mediation-device**: This keyword is obsolete.
Default: **standard**

**type standard**

Specifies the use of standard AAA transactions to use to communicate with this RADIUS server. Default: **standard**

**admin-status { enable | disable }**

Enables or disables the RADIUS authentication/accounting/charging server functionality, and saves the status setting in the configuration file to re-establish the set status at reboot.

**-noconfirm**

Executes the command without any additional prompt and confirmation from the user.

**Usage**

This command is used to configure the RADIUS accounting servers with which the system is to communicate for accounting.

Up to 128 RADIUS servers can be configured per context. The servers can be configured as Accounting, Authentication, charging servers, or any combination thereof.

**Example**

The following commands configure the RADIUS accounting server with the IP address set to 10.2.3.4, port to 1024, and priority to 10:

```
radius accounting server 10.2.3.4 key sharedKey port 1024 max 127
radius accounting server 10.2.3.4 encrypted key scrambledKey oldports priority 10
no radius accounting server 10.2.5.6
```

The following command sets the accounting server with mediation device transaction for AAA server 10.2.3.4:

```
radius mediation-device accounting server 10.2.3.4 key sharedKey port 1024 max 127
```
radius algorithm

This command configures the RADIUS authentication server selection algorithm for the current context.

**Syntax**

radius algorithm { first-server | round-robin }

default radius algorithm

default

Configures this command with the default setting. Default: **first-server**

**first-server**

Sends authentication data to the first available RADIUS authentication server based upon the relative priority of each configured server.

**round-robin**

Sends authentication data in a circular queue fashion on a per Session Manager task basis where data is sent to the next available RADIUS authentication server and restarts at the beginning of the list of configured servers. The order of the list is based upon the configured relative priority of the servers.

**Usage**

Use this command to configure the context’s RADIUS server selection algorithm to ensure proper load distribution through the available RADIUS authentication servers.

**Example**

The following command configures to use the round-robin algorithm for RADIUS authentication server selection:

```
radius algorithm round-robin
```
radius allow

This command configures the system behavior to allow subscriber sessions when RADIUS accounting and/or authentication is unavailable.

Product
PDSN
HA
FA

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration
configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

[ no ] radius allow { accounting-down | authentication-down }

no
Removes earlier configuration for the specified keyword.

accounting-down
Allows sessions while accounting is unavailable (down). Default: Enabled

authentication-down
Allows sessions while authentication is not available (down). Default: Disabled

Usage
Allow sessions during system troubles when the risk of IP address and/or subscriber spoofing is minimal. The denial of sessions may cause dissatisfaction with subscribers at the cost/expense of verification and/or accounting data.

Important: Please note that this command is applicable ONLY to CDMA products. To configure this functionality in UMTS/LTE products (GGSN/P-GW/SAEGW), use the command mediation-device delay-GTP-response in APN Configuration mode.

Example
The following command configures the RADIUS server to allow the sessions while accounting is unavailable:

radius allow accounting-down
radius attribute

This command configures the system’s RADIUS identification parameters.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration

```
configure > context context_name
```

Entering the above command sequence results in the following prompt:

```
[context_name] host_name(config-ctx)#
```

**Syntax**

```
radius attribute { nas-identifier id | nas-ip-address address primary_address [ backup secondary_address ] [ nexthop-forwarding-address nexthop_ip_address ] [ vlan vlan_id ] [ mpls-label input in_label_value output out_label_value1 out_label_value2 ] }

no radius attribute { nas-identifier | nas-ip-address }

default radius attribute nas-identifier
```

**no**

Removes earlier configuration for the specified keyword.

**default**

Configures the default setting.

**nas-identifier id**

 Specifies the attribute name by which the system will be identified in Access-Request messages. *id* must be an alphanumeric string of 1 through 32 characters that is case sensitive.

**nas-ip-address address primary_address**

 Specifies the AAA interface IP address(es) used to identify the system. Up to two addresses can be configured. *primary_address* is the IP address of the primary interface to use in the current context in IPV4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

**backup secondary_address**

 Specifies the IP address of the secondary interface to use in the current context in IPV4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

**mpls-label input in_label_value | output out_label_value1 out_label_value2**

 This command configures the traffic from the specified AAA client NAS IP address to use the specified MPLS labels.
\textbf{radius attribute} is the MPLS label that identifies inbound traffic destined for the configured NAS IP address.

\textbf{out_label_value1} and \textbf{out_label_value2} identify the MPLS labels to be added to the packets sent from the specified NAS IP address.

- \texttt{out_label_value1} is the inner output label.
- \texttt{out_label_value2} is the outer output label.

MPLS label values must be an integer from 16 through 1048575.

**Important:** This option is available only when nexthop-forwarding gateway is also configured with the \texttt{nexthop-forwarding-address} keyword.

\texttt{nexthop-forwarding-address} \texttt{nexthop_ip_address}

Configures the next hop IP address for this NAS IP address in IPV4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

\texttt{vlan} \texttt{vlan_id}

Specifies the VLANID to be associated with the next-hop IP address as an integer from 1 through 4094.

\textbf{Usage}

This is necessary for NetWare Access Server usage such as the system must be identified to the NAS. The system supports the concept of the active nas-ip-address. The active nas-ip-address is defined as the current source ip address for RADIUS messages being used by the system. This is the content of the nas-ip-address attribute in each RADIUS message.

The system will always have exactly one active nas-ip-address. The active nas-ip-address will start as the primary nas-ip-address. However, the active nas-ip-address may switch from the primary to the backup, or the backup to the primary. The following events will occur when the active nas-ip-address is switched:

- All current in-process RADIUS accounting messages from the entire system are cancelled. The accounting message is re-sent, with retries preserved, using the new active nas-ip-address. Acct-Delay-Time, however, is updated to reflect the time that has occurred since the accounting event. The value of Event-Timestamp is preserved.

- All current in-process RADIUS authentication messages from the entire system are cancelled. The authentication message is re-sent, with retries preserved, using the new active nas-ip-address. The value of Event-Timestamp is preserved.

- All subsequent in-process RADIUS requests uses the new active nas-ip-address.

The system uses a revertive algorithm when transitioning active NAS IP addresses as described below:

- If the configured primary nas-ip-address transitions from UP to DOWN, and the backup nas-ip-address is UP, then the active nas-ip-address switches from the primary to the backup nas-ip-address

- If the backup nas-ip-address is active, and the primary nas-ip-address transitions from DOWN to UP, then the active nas-ip-address switches from the backup to the primary nas-ip-address

\textbf{Example}

The following command configures the RADIUS attribute nas-ip-address as 10.2.3.4:

\texttt{radius attribute nas-ip-address 10.2.3.4}
**radius authenticate null-username**

This command enables (allows) or disables (prevents) the authentication of user names that are blank or empty. This is enabled by default.

**Product**

PDSN

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration

```
configure > context context_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
[ no | default ] radius authenticate null-username
```

- **default**
  
  Configures the default setting.
  
  Default: Authenticate, send Access-Request messages to the AAA server, all user names, including NULL user names.

- **no**
  
  Disables sending an Access-Request message to the AAA server for user names (NAI) that are blank.

- **null-username**
  
  Enables sending an Access-Request message to the AAA server for user names (NAI) that are blank.

**Usage**

Use this command to disable, or re-enable, sending Access-Request messages to the AAA server for user names (NAI) that are blank (NULL).

**Example**

The following command disables sending of Access-Request messages for user names (NAI) that are blank:

```
no radius authenticate null-username
```

The following command re-enables sending of Access-Request messages for user names (NAI) that are blank:

```
radius authenticate null-username
```
radius authenticate apn-to-be-included

This command configures the Access Point Name (APN) to be included for RADIUS authentication.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration
configure > context context_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
[ default ] radius authenticate apn-to-be-included { gi | gn }
```

- **default**
  Configures the default setting.

- **gi**
  Specifies the use of the Gi APN name in the RADIUS authentication request. The Gi APN represents the APN received in the Create PDP Context Request message from the SGSN.

- **gn**
  Specifies the use of the Gn APN name in the RADIUS authentication request. The Gn APN represents the APN selected by the GGSN.

**Usage**

Use this command to configure the APN name for RADIUS authentication. This can be set to either gi or gn.

**Example**

The following command specifies the usage of Gn APN name in the RADIUS authentication request.

```
radius authenticate apn-to-be-included gn
```
radius authenticator-validation

This command enables (allows) or disables (prevents) the MD5 authentication of RADIUS users. By default this feature is enabled.

**Product**

PDSN
GGSN

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration

```
configure > context context_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
[ default | no ] radius authenticator-validation
```

- **default**
  Enables MD5 authentication validation for an Access-Request message to the AAA server.

- **no**
  Disables MD5 authentication validation for an Access-Request message to the AAA server.

**Usage**

Use this command to disable, or re-enable, sending Access-Request messages to the AAA server for MD5 validation.

**Example**

The following command disables MD5 authentication validation for Access-Request messages for user names (NAI):

```
no radius authenticator-validation
```

The following command enables MD5 authentication validation for Access-Request messages for user names (NAI):

```
radius radius authenticator-validation
```
**radius change-authorize-nas-ip**

This command configures the NAS IP address and UDP port on which the current context will listen for Change of Authorization (COA) messages and Disconnect Messages (DM). If the NAS IP address is not defined with this command, any COA or DM messages from the RADIUS server are returned with a Destination Unreachable error.

**Product**
- FA
- GGSN
- HA
- LNS
- PDSN

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration > Context Configuration
- `configure > context context_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
radius change-authorize-nas-ip ip_address [ encrypted ] key value [ port port ] [ event-timestamp-window window ] [ no-nas-identification-check ] [ no-reverse-path-forward-check ] [ mpls-label input in_label_value | output out_label_value1 [ out_label_value2 ] ]
```

**no radius change-authorize-nas-ip**

- **no**
  Deleting the NAS IP address information which disables the system from receiving and responding to COA and DM messages from the RADIUS server.

- **ip_address**
  Specifies the NAS IP address of the current context’s AAA interface that was defined with the `radius attribute` command.
  `ip_address` can be expressed in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

- **[ encrypted ] key value**
  Specifies the shared secret key used to authenticate the client to the servers. The `encrypted` keyword indicates the key specified is encrypted.
  In 12.1 and earlier releases, the `key value` must be an alphanumeric string of 1 through 127 characters without encryption, and 1 through 256 characters with encryption.
  In 12.2 and later releases, the `key value` must be an alphanumeric string of 1 through 127 characters without encryption, and 1 through 236 characters with encryption enabled.
  The `encrypted` keyword is intended only for use by the system while saving configuration scripts. The system displays the `encrypted` keyword in the configuration file as a flag that the variable following the
key keyword is the encrypted version of the plain text key. Only the encrypted key is saved as part of the configuration file.

port port
The UDP port on which to listen for CoA and DM messages. Default: 3799

event-timestamp-window window
When a COA or DM request is received with an event-time-stamp, if the current-time is greater than the received-pkt-event-time-stamp plus the event-time-stamp-window, the packet is silently discarded. When a COA or DM request is received without the event-time stamp attribute, the packet is silently discarded.

window must be an integer from 0 through 4294967295. If window is specified as 0 (zero), this feature is disabled; the event-time-stamp attribute in COA or DM messages is ignored and the event-time-stamp attribute is not included in NAK or ACK messages. Default: 300

no-nas-identification-check
Disables the context from checking the NAS Identifier/NAS IP Address while receiving the CoA/DM requests. By default this check is enabled.

no-reverse-path-forward-check
Disables the context from checking whether received CoA or DM packets are from one of the AAA servers configured under the default AAA group in the current context. Only the src-ip address in the received CoA or DM request is validated and the port and key are ignored. The reverse-path-forward-check is enabled by default.

If reverse-path-forward-check is disabled, the CoA and DM messages will be accepted from AAA servers from any groups. If the check is enabled, then the CoA and DM messages will be accepted only from servers under default AAA group.

mpls-label input in_label_value | output out_label_value1 [ out_label_value2 ]
This command configures COA traffic to use the specified MPLS labels.

• in_label_value is the MPLS label that identifies inbound COA traffic.

• out_label_value1 and out_label_value2 identify the MPLS labels to be added to COA response.
  • out_label_value1 is the inner output label.
  • out_label_value2 is the outer output label.

MPLS label values must be an integer from 16 through 1048575.

Usage
Use this command to enable the current context to listen for CoA and DM messages.

Any one of the following RADIUS attributes may be used to identify the subscriber:

• 3GPP-IMSI: The subscriber’s IMSI. It may include the 3GPP-NSAPI attribute to delete a single PDP context rather than all of the PDP contexts of the subscriber when used with the GGSN product.

• Framed-IP-address: The subscriber’s IP address.

• Acct-Session-Id: Identifies a subscriber session or PDP context.
Important: For the GGSN product, the value for Acct-Session-Id that is mandated by 3GPP is used instead of the special value for Acct-Session-Id that we use in the RADIUS messages we exchange with a RADIUS accounting server.

Important: When this command is used in conjunction with the GGSN, CoA functionality is not supported.

Example

The following command specifies the IP address 192.168.100.10 as the NAS IP address, a key value of 123456 and uses the default port of 3799:

```
radius change-authorize-nas-ip 192.168.100.10 key 123456
```

The following command disables the nas-identification-check for the above parameters:

```
radius change-authorize-nas-ip 192.168.100.10 key 123456 no-nas-identification-check
```
radius charging

This command configures basic RADIUS options for Active Charging Services.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration
configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

radius charging { deadtime dead_minutes | detect-dead-server { consecutive-failures consecutive_failures | response-timeout timeout_duration } | max-outstanding max_messages | max-retries max_retries | max-transmissions transmissions | timeout timeout_duration }

default radius charging { deadtime | detect-dead-server | max-outstanding | max-retries | max-transmissions | timeout }

no radius charging { detect-dead-server | max-transmissions | timeout }

no

Removes configuration for the specified keyword.

default

Configures the default settings.

deadtime dead_minutes

Specifies the number of minutes to wait before attempting to communicate with a server which has been marked as unreachable.

dead_minutes must be an integer from 0 through 65535.
Default: 10

detect-dead-server { consecutive-failures consecutive_failures | response-timeout timeout_duration }

consecutive-failures consecutive_failures: Default: 4. Specifies the number of consecutive failures, for each AAA manager, before a server is marked as unreachable. consecutive_failures must be an integer from 0 through 1000.

response-timeout timeout_duration: Specifies the number of seconds for each AAA manager to wait for a response to any message before a server is detected as failed, or in a down state. timeout_duration must be an integer from 1 through 65535.
max-outstanding max_messages

Specifies the maximum number of outstanding messages a single AAA manager instance will queue. max_messages must be an integer from 1 through 4000. Default: 256

max-retries max_retries

Specifies the maximum number of times communication with a AAA server will be attempted before it is marked as unreachable and the detect dead servers consecutive failures count is incremented. max_retries must be an integer from 0 through 65535. Default: 5

max-transmissions transmissions

Sets the maximum number of re-transmissions for RADIUS authentication requests. This limit is used in conjunction with the max-retries for each server. transmissions must be an integer from 1 through 65535. Default: Disabled

When failing to communicate with a RADIUS sever, the subscriber is failed once all of the configured RADIUS servers have been exhausted or once the configured number of maximum transmissions is reached. For example, if 3 servers are configured and if the configured max-retries is 3 and max-transmissions is 12, then the primary server is tried 4 times (once plus 3 retries), the secondary server is tried 4 times, and then a third server is tried 4 times. If there is a fourth server, it is not tried because the maximum number of transmissions (12) has been reached.

timeout timeout_duration

Specifies the number of seconds to wait for a response from the RADIUS server before re-sending the messages. timeout_duration must be an integer from 1 through 65535. Default: 3

Usage

Manage the basic Charging Service RADIUS options according to the RADIUS server used for the context.

Example

The following command configures the AAA server to be marked as unreachable when the consecutive failure count exceeds 6:

    radius charging detect-dead-server consecutive-failures 6

The following command sets the timeout value to 300 seconds to wait for a response from RADIUS server before resending the messages:

    radius charging timeout 300
radius charging accounting algorithm

This command specifies the fail-over/load-balancing algorithm to be used for selecting RADIUS servers for charging services.

**Product**
PDSN
GGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration
`configure > context context_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
radius charging accounting algorithm { first-n n | first-server | round-robin }
```

**first-n n**

Specifies that the AGW must send accounting data to \( n \) (more than one) AAA servers based on their priority. Response from any one of the \( n \) AAA servers would suffice to proceed with the call. The full set of accounting data is sent to each of the \( n \) AAA servers.

\( n \) is the number of AAA servers to which accounting data will be sent, and must be an integer from 2 through 128. Default: 1 (Disabled)

**first-server**

Specifies that the context must send accounting data to the RADIUS server with the highest configured priority. In the event that this server becomes unreachable, accounting data is sent to the server with the next-highest configured priority. This is the default algorithm.

**round-robin**

Specifies that the context must load balance sending accounting data among all of the defined RADIUS servers. Accounting data is sent in a circular queue fashion on a per Session Manager task basis, where data is sent to the next available server and restarts at the beginning of the list of configured servers. The order of the list is based upon the configured relative priority of the servers.

**Usage**

Use this command to specify the accounting algorithm to use to select RADIUS servers for charging services configured in the current context.

**Example**

The following command specifies to use the round-robin algorithm to select the RADIUS server:

```
radius charging accounting algorithm round-robin
```
radius charging accounting server

This command configures RADIUS charging accounting servers in the current context for Active Charging Services prepaid accounting.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration
configure > context context_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
radius charging accounting server ip_address [ encrypted ] key key [ max max_messages ] [ max-rate max_rate ] [ oldports ] [ port port_number ] [ priority priority ] [ admin-status { enable | disable } ] [ -noconfirm ]
```

```
no radius charging accounting server ip_address [ oldports | port port_number ]
```

---

**no**

Removes the server or server port(s) specified from the list of configured servers.

---

**ip_address**

Specifies IP address of the accounting server in IPv4 dotted-decimal notation. A maximum of 128 RADIUS servers can be configured per context. This limit includes accounting and authentication servers.

---

```
[ encrypted ] key key
```

Specifies the shared secret key used to authenticate the client to the servers. The `encrypted` keyword indicates the key specified is encrypted.

In 12.1 and earlier releases, the key value must be an alphanumeric string of 1 through 127 characters without encryption, and 1 through 256 characters with encryption.

In 12.2 and later releases, the key value must be an alphanumeric string of 1 through 127 characters without encryption, and 1 through 236 characters with encryption enabled.

The `encrypted` keyword is intended only for use by the system while saving configuration scripts. The system displays the `encrypted` keyword in the configuration file as a flag that the variable following the `key` keyword is the encrypted version of the plain text key. Only the encrypted key is saved as part of the configuration file.

---

```
max max_messages
```

Specifies the maximum number of outstanding messages that may be allowed to the server. `max_messages` must be integer from 0 through 4000. Default: 0
max-rate \textit{max\_rate}  
Specifies the rate (number of messages per second) at which the authentication messages should be sent to the RADIUS server. \textit{max\_rate} must be an integer from 0 through 1000. Default: 0 (Disabled)

oldports  
Sets the UDP communication port to the out of date standardized default for RADIUS communications to 1646.

\textbf{port} \textit{port\_number}  
Specifies the port number to use for communications as an integer from 1 through 65535. Default: 1813

\textbf{priority} \textit{priority}  
Specifies the relative priority of this accounting server. The priority is used in server selection for determining to which server to send accounting data. \textit{priority} must be an integer 1 through 1000 where 1 is the highest priority. Default: 1000

\textbf{admin-status} \{ enable | disable \}  
Enables or disables the RADIUS authentication/ accounting/charging server functionality, and saves the status setting in the configuration file to re-establish the set status at reboot.

\textbf{-noconfirm}  
Executes the command without any additional prompt and confirmation from the user.

\textbf{Usage}\n
This command is used to configure the RADIUS charging accounting server(s) with which the system is to communicate for Active Charging Services prepaid accounting requests. Up to 128 AAA servers can be configured per context when the system is functioning as a PDSN and/or HA. Up to 16 servers are supported per context when the system is functioning as a GGSN.

\textbf{Example}\n
The following commands configure RADIUS charging accounting server with the IP address set to 10.2.3.4, port to 1024, and priority to 10:

\begin{verbatim}
radius charging accounting server 10.2.3.4 key sharedKey port 1024 max 127
radius charging accounting server 10.2.3.4 encrypted key scrambledKey oldports priority 10
\end{verbatim}
radius charging algorithm

This command configures the RADIUS authentication server selection algorithm for Active Charging Services for the current context.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration

configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx) #

Syntax

radius charging algorithm { first-server | round-robin }

default radius charging algorithm

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Configures the default setting. Default: first-server</td>
</tr>
<tr>
<td>first-server</td>
<td>Sends accounting data to the first available server based upon the relative priority of each configured server.</td>
</tr>
<tr>
<td>round-robin</td>
<td>Sends accounting data in a circular queue fashion on a per Session Manager task basis where data is sent to the next available server and restarts at the beginning of the list of configured servers. The order of the list is based upon the configured relative priority of the servers.</td>
</tr>
</tbody>
</table>

Usage

Set the context’s RADIUS server selection algorithm for Active Charging Services to ensure proper load distribution through the servers available.

Example

The following command configures to use the round-robin algorithm for RADIUS server selection:

radius charging algorithm round-robin
radius charging server

This command configures the RADIUS charging server(s) in the current context for Active Charging Services prepaid authentication.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration
configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

radius charging server ip_address [ encrypted ] key key [ max max_messages ] [ max-rate max_rate ] [ oldports ] [ port port_number ] [ priority priority ] [ admin-status { enable | disable } ] [ -noconfirm ]

no radius charging server ip_address [ oldports | port port_number ]

no
Removes the server or server port(s) specified from the list of configured servers.

ip_address
Specifies the IP address of the server in IPv4 dotted-decimal notation. A maximum of 128 RADIUS servers can be configured per context. This limit includes accounting and authentication servers.

[ encrypted ] key key
Specifies the shared secret key used to authenticate the client to the servers. The encrypted keyword indicates the key specified is encrypted.
In 12.1 and earlier releases, the key value must be an alphanumeric string of 1 through 127 characters without encryption, and 1 through 256 characters with encryption.
In 12.2 and later releases, the key value must be an alphanumeric string of 1 through 127 characters without encryption, and 1 through 236 characters with encryption enabled.
The encrypted keyword is intended only for use by the system while saving configuration scripts. The system displays the encrypted keyword in the configuration file as a flag that the variable following the key keyword is the encrypted version of the plain text key. Only the encrypted key is saved as part of the configuration file.

max max_messages
Specifies the maximum number of outstanding messages that may be allowed to the server. max_messages must be an integer from 0 through 4000. Default: 256
max-rate max_rate
Specifies the rate (number of messages per second), at which the authentication messages should be sent to the RADIUS server. max_rate must be an integer from 0 through 1000. Default: 0 (Disabled)

oldports
Sets the UDP communication port to the old default for RADIUS communications to 1645.

port port_number
Specifies the port number to use for communications as an integer from 1 through 65535. Default: 1812

priority priority
Specifies the relative priority of this accounting server. The priority is used in server selection for determining to which server to send accounting data. priority must be an integer from 1 through 1000 where 1 is the highest priority. Default: 1000

admin-status { enable | disable }
Enables or disables the RADIUS authentication/accounting/charging server functionality and saves the status setting in the configuration file to re-establish the set status at reboot.

-noconfirm
Executes the command without any additional prompt and confirmation from the user.

Usage
This command is used to configure the RADIUS charging server(s) with which the system is to communicate for Active Charging Services prepaid authentication requests.
Up to 128 AAA servers can be configured per context when the system is functioning as a PDSN and/or HA.
Up to 16 servers are supported per context when the system is functioning as a GGSN.

Example
The following commands configure RADIUS charging server with the IP address set to 10.2.3.4, port to 1024, and priority to 10:

radius charging server 10.2.3.4 key sharedKey port 1024 max 127
radius charging server 10.2.3.4 encrypted key scrambledKey oldports priority 10
radius deadtime

This command configures the maximum period of time (in minutes) that must elapse between when a context marks a RADIUS server as unreachable and when it can re-attempt to communicate with the server.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration
configure > context context_name

Entering the above command sequence results in the following prompt:

\[context_name]host_name(config-ctx)#

**Syntax**

radius deadtime minutes

**default radius deadtime**

<table>
<thead>
<tr>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configures the default setting. Default: 10 minutes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>minutes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the number of minutes to wait before changing the state of a RADIUS server from “Down” to “Active”. minutes must be an integer from 0 through 65535.</td>
</tr>
</tbody>
</table>

**Usage**

Use this command to configure the basic RADIUS parameters according to the RADIUS server used for the context.

**Important:** This parameter should be set to allow enough time to remedy the issue that originally caused the server’s state to be changed to “Down”. After the dead time timer expires, the system returns the server’s state to “Active” regardless of whether or not the issue has been fixed.

**Important:** For a complete explanation of RADIUS server states, if you are using StarOS 12.3 or an earlier release, refer to the RADIUS Server State Behavior appendix in the AAA and GTPP Interface Administration and Reference. If you are using StarOS14.0 or a later release, refer to the AAA Interface Administration and Reference.

**Example**

The following command configures the RADIUS deadtime to 100 minutes:

```
radius deadtime 100
```
radius detect-dead-server

This command configures how the system detects a dead RADIUS server.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration
configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

radius detect-dead-server { consecutive-failures consecutive_failures_count | keepalive | response-timeout timeout_duration }

{ default | no } radius detect-dead-server

no
Removes the configuration.

default
Configures the default setting.

• consecutive-failures: Enabled; 4 consecutive failures
• keepalive: Disabled
• response-timeout: Disabled

consecutive-failures consecutive_failures_count

Specifies the consecutive number of times that the system must find the AAA server unreachable for the server to be marked unreachable, that is the server’s state is changed from “Active” to “Down”.

consecutive_failures_count must be an integer from 1 through 1000. Default: Enabled; 4 consecutive failures

keepalive
Enables the AAA server alive-dead detect mechanism based on sending keepalive authentication messages to all authentication servers. Default: Disabled

response-timeout timeout_duration

Specifies the time duration, in seconds, that the system must wait for a response from the AAA server to any message before the server is marked unreachable, that is the server’s state is changed from “Active” to “Down”.

timeout_duration must be an integer from 1 through 65535. Default: Disabled
**Usage**

Use this command to configure how the system detects a dead RADIUS server.

**Important:** If both `consecutive-failures` and `response-timeout` are configured, then both parameters must be met before a server’s state is changed to “Down”.

**Important:** The “Active” or “Down” state of a RADIUS server as defined by the system, is based on accessibility and connectivity. For example, if the server is functional but the system has placed it into a “Down” state, it could be the result of a connectivity problem. When a RADIUS server’s state is changed to “Down”, a trap is sent to the management station and the `deadtime` timer is started.

**Example**

The following command enables the detect-dead-server consecutive-failures mechanism and configures the consecutive number of failures to 10:

```
radius detect-dead-server consecutive-failures 10
```
radius dictionary

Configures the RADIUS dictionary.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration
configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

radius dictionary dictionary

default radius dictionary

default
Configures the default setting.

dictionary
Specifies which dictionary to use.
dictionary must be one of the following values:

Table 22. RADIUS Dictionary Types

<table>
<thead>
<tr>
<th>Dictionary</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3gpp</td>
<td>This dictionary consists of all the attributes in the standard dictionary, and all of the attributes specified in 3GPP 32.015.</td>
</tr>
<tr>
<td>3gpp2</td>
<td>This dictionary consists of all the attributes in the standard dictionary, and all of the attributes specified in IS-835-A.</td>
</tr>
<tr>
<td>3gpp2-835</td>
<td>This dictionary consists of all the attributes in the standard dictionary, and all of the attributes specified in IS-835.</td>
</tr>
<tr>
<td>customXX</td>
<td>These are customized dictionaries. For information on custom dictionaries, contact your local service representative. XX is the integer of the custom dictionary. NOTE: RADIUS dictionary custom23 should be used in conjunction with Active Charging Service (ACS).</td>
</tr>
<tr>
<td>standard</td>
<td>This dictionary consists only of the attributes specified in RFC 2865, RFC 2866, and RFC2869.</td>
</tr>
<tr>
<td>starent</td>
<td>This dictionary consists of all the attributes in the starent-vsa1 dictionary and incorporates additional VSAs by using a two-byte VSA Type field. This dictionary is the master-set of all of the attributes in all of the dictionaries supported by the system.</td>
</tr>
</tbody>
</table>
radius dictionary

<table>
<thead>
<tr>
<th>Dictionary</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>starent-835</td>
<td>This dictionary consists of all of the attributes in the starent-vsa1-835 dictionary and incorporates additional VSAs by using a two-byte VSA Type field. This dictionary is the master-set of all of the attributes in all of the -835 dictionaries supported by the system.</td>
</tr>
<tr>
<td>starent-vsal</td>
<td>This dictionary consists not only of the 3gpp2 dictionary, but also includes vendor-specific attributes (VSAs) as well. The VSAs in this dictionary support a one-byte wide VSA Type field in order to support certain RADIUS applications. The one-byte limit allows support for only 256 VSAs (0–255). This is the default dictionary.</td>
</tr>
<tr>
<td>starent-vsal-835</td>
<td>This dictionary consists not only of the 3gpp2-835 dictionary, but also includes vendor-specific attributes (VSAs) as well. The VSAs in this dictionary support a one-byte wide VSA Type field in order to support certain RADIUS applications. The one-byte limit allows support for only 256 VSAs (0–255). This is the default dictionary.</td>
</tr>
</tbody>
</table>

**Usage**

Use this command to configure the RADIUS dictionary.

**Example**

The following command configures the RADIUS dictionary standard.

```
radius dictionary standard
```
radius group

This command has been deprecated and is replaced by AAA Server Group configurations. See the "AAA Server Group Configuration Mode Commands" chapter.
**radius ip vrf**

This command associates the specific AAA group (NAS-IP) with a Virtual Routing and Forwarding (VRF) Context instance for BGP/MPLS, GRE, and IPSec tunnel functionality which needs VRF support for RADIUS communication. By default the VRF is NULL, which means that AAA group is associated with global routing table.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration

```plaintext
configure > context context_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```plaintext
radius ip vrf vrf_name

no radius ip vrf
```

**no**
Disables the configured IP Virtual Routing and Forwarding (VRF) context instance and removes the association between the VRF context instance and the AAA group instance (NAS-IP).
By default this command is disabled, which means the NAS-IP being used is assumed a non-VRF IP and specific AAA group does not have any VRF association.

**vrf_name**
Specifies the name of a pre-configured VRF context instance. *vrf_name* is the alphanumeric string of a pre-configured VRF context configured in Context Configuration Mode via the `ip vrf` command.

⚠️ **Caution:** Any incorrect configuration, such as associating AAA group with wrong VRF instance or removing a VRF instance, will fail the RADIUS communication.

**Usage**
Use this command to associate/disassociate a pre-configured VRF context for a feature such as BGP/MPLS VPN or GRE, and IPSec tunneling which needs VRF support for RADIUS communication.
By default the VRF is NULL, which means that AAA group (NAS-IP) is associated with global routing table and NAS-IP being used is assumed a non-VRF IP.
This IP VRF feature can be applied to RADIUS communication, which associates the VRF with the AAA group. This command must be configured whenever a VRF IP is used as a NAS-IP in the AAA group or at the Context level for ‘default’ AAA group.
This is a required configuration as VRF IPs may be overlapping hence AAA needs to know which VRF the configured NAS-IP belongs to. By this support different VRF-based subscribers can communicate with...
different RADIUS servers using the same, overlapping NAS-IP address, if required across different AAA groups.

**Example**

The following command associates VRF context instance `ip_vrf1` with specific AAA group (NAS-IP):

```
radius ip vrf ip_vrf1
```
radius keepalive

This command configures the keepalive authentication parameters for the RADIUS server.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration

configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

radius keepalive [ calling-station-id id | consecutive-response responses_no_of | encrypted | interval interval_duration | password | retries retries_no_of | timeout timeout_duration | username user_name | valid-response access-accept [ access-reject ] ]

default radius keepalive { calling-station-id | consecutive-response | interval | password | retries | timeout | username | valid-response }

default

Configures the default setting for the specified parameter.

calling-station-id id

Configures the Calling-Station ID to be used for the keepalive authentication. id must be an alphanumeric string of size 1 to 15 characters. Default: 000000000000000

consecutive-response responses_no_of

Configures the number of consecutive authentication responses after which the server is marked as reachable. responses_no_of must be an integer from 1 through 10. Default: 1

encrypted password

Designates use of encryption for the password.
In 12.1 and earlier releases, password must be an alphanumeric string of 1 through 63 characters.
In 12.2 and later releases, password must be an alphanumeric string of 1 through 132 characters.
Default: Test-Password

interval interval_duration

Configures the time interval (in seconds) between two keepalive access requests. interval_duration must be an integer from 30 through 65535. Default: 30
**password**
Configures the password to be used for the authentication as an alphanumeric string of 1 through 63 characters. Default: Test-Password

**retries retries_no_of**
Configures the number of times the keepalive access request are sent before marking the server as unreachable. retries_no_of must be an integer from 3 through 10. Default: 3

**timeout timeout_duration**
Configures the time interval (in seconds) between keepalive access request retries. timeout_duration must be an integer from 1 through 30. Default: 3

**username user_name**
Configures the username to be used for authentication as an alphanumeric string of 1 through 127 characters. Default: Test-Username

**valid-response access-accept [ access-reject ]**
Configures the valid response for the authentication request.
If access-reject is configured, then both access-accept and access-reject are considered as success for the keepalive authentication request.
If access-reject is not configured, then only access-accept is considered as success for the keepalive access request.
Default: keepalive valid-response access-accept

**Usage**
Use this command to configure the Keepalive Authentication parameters for the RADIUS server.

**Example**
The following command sets the user name for the RADIUS keepalive access requests to Test-Username2:

```
radius keepalive username Test-Username2
```

The following command sets the number of retries to 4:

```
radius keepalive retries 4
```
radius max-outstanding

This command configures the maximum number of outstanding messages a single AAA Manager instance will queue.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration

```configure > context context_name```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
radius max-outstanding max_messages

default radius max-outstanding
```

**default**

Confirms the default setting.
Default: 256

**max_messages**

Specifies the maximum number of outstanding messages a single AAA Manager instance will queue.

*max_messages* must be an integer from 1 through 4000. Default: 256

**Usage**

Use this command to configure the maximum number of outstanding messages a single AAA Manager instance will queue.

**Example**

The following command configures the maximum number of outstanding messages a single AAA Manager instance will queue to 100:

```
radius max-outstanding 100
```
radius max-retries

This command configures the maximum number of times communication with a AAA server will be attempted before it is marked as “Not Responding”.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration

configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

radius max-retries max_retries

default radius max-retries

default

Configures the default setting.

max_retries

Specifies the maximum number of times communication with a AAA server will be attempted before it is marked as “Not Responding”, and the detect dead server’s consecutive failures count is incremented. 

max_retries must be an integer from 0 through 65535. Default: 5

Usage

Use this command to configure the maximum number of times communication with a AAA server will be attempted before it is marked as “Not Responding”.

Example

The following command configures the maximum number of times communication with a AAA server will be attempted before it is marked as “Not Responding” to 10:

radius max-retries 10
radius max-transmissions

This command configures the maximum number of re-transmissions for RADIUS authentication requests.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration
configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

radius max-transmissions max_transmissions

{ default | no } radius max-transmissions

no
Deletes the RADIUS max-transmissions configuration.

default
Configures the default setting.
Default: Disabled

max_transmissions

Specifies the maximum number of re-transmissions for RADIUS authentication requests. This limit is used in conjunction with radius max-retries configuration for each server. max_transmissions must be an integer from 1 through 65535. Default: Disabled

When failing to communicate with a RADIUS server, the subscriber is failed once all of the configured RADIUS servers have been exhausted, or once the configured number of maximum transmissions is reached. For example, if three servers are configured and if the configured max-retries is 3 and max-transmissions is 12, then the primary server is tried four times (once plus three retries), the secondary server is tried four times, and then a third server is tried four times. If there is a fourth server, it is not tried because the maximum number of transmissions (12) has been reached.

Usage

Use this command to configure the maximum number of re-transmissions for RADIUS authentication requests.

Example

The following command configures the maximum number of re-transmissions for RADIUS authentication requests to 10:

    radius max-transmissions 10
radius mediation-device

See the radius accounting server command.
radius probe-interval

This command configures the interval between two RADIUS authentication probes.

Product
All products supporting Interchassis Session Recovery (ICSR)

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration
configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

radius probe-interval seconds

default radius probe-interval

default

Configures the default setting of 3.

seconds

Specifies the time duration (in seconds) to wait before sending another probe authentication request to a RADIUS server. The value must be an integer from 1 through 65535. Default: 3

Usage
Use this command for ICSR support to set the duration between two authentication probes to the RADIUS server.

Example
The following command sets the authentication probe interval to 30 seconds.

radius probe-interval 30
radius probe-max-retries

This command configures the number of retries for RADIUS authentication probe response.

Product
All products supporting Inter chassis Session Recovery (ICSR)

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration

configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

radius probe-max-retries retries

default radius probe-max-retries

default

Configures the default setting.
Default: 5

retries

Specify the number of retries for RADIUS authentication probe response before the authentication is declared as failed. retries must be an integer from 1 through 65535. Default: 5

Usage
Use this command for ICSR support to set the number of attempts to send RADIUS authentication probe without a response before the authentication is declared as failed.

Example

The following command sets the maximum number of retries to 6:

radius probe-max-retries 6
radius probe-message

This command configures the service ip-address to be sent as an AVP in RADIUS authentication probe messages.

Product
All products supporting Inter chassis Session Recovery (ICSR)

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration
configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

radius probe-message local-service-address ipv4/ipv6_address

no radius probe-message local-service-address

no
Disables sending of AVPs configured under probe-message cli in RADIUS authentication probe messages.

radius probe-message local-service-address
radius probe-message
Configures AVPs to be sent in RADIUS authentication probe messages.
local-service-address
Configures the service ip-address to be sent as an AVP in RADIUS authentication probe messages.

ipv4/ipv6_address
Specifies the IPv4/IPv6 address of the server in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation. A maximum of 128 RADIUS servers can be configured per context. This limit includes accounting and authentication servers.

Example

The following command configures the service ip-address 21.32.36.25 to be sent as an AVP in RADIUS authentication probe messages:

radius probe-message local-service-address 21.32.36.25
radius probe-timeout

This command configures the timeout duration to wait for a response for RADIUS authentication probes.

Product
All products supporting Interchassis Session Recovery (ICSR)

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration
configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

radius probe-timeout timeout_duration

default radius probe-timeout

---
default

Configures the default setting.
Default: 3

---
timeout_duration

Specifies the time duration (in seconds) to wait for a response from the RADIUS server before resending the authentication probe. timeout_duration must be an integer from 1 through 65535. Default: 3

Usage

Use this command for ICSR support to set the duration to wait for a response before re-sending the RADIUS authentication probe to the RADIUS server.

Example

The following command sets the authentication probe timeout to 120 seconds:

radius probe-timeout 120
radius server

This command configures RADIUS authentication server(s) in the current context.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration

configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

radius server ip_address [ encrypted ] key value [ max max_messages ] [ max-rate max_rate ] [ oldports ] [ port port_number ] [ priority priority ] [ probe | no-probe ] [ probe-username user_name ] [ probe-password [ encrypted ] password password ] [ type { mediation-device | standard } ] [ admin-status { enable | disable } ] [ -noconfirm ]

no radius server ip_address [ oldports | port port_number ]

no
Removes the server or server port(s) specified from the list of configured servers.

ip_address
Specifies the IP address of the server in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation. A maximum of 128 RADIUS servers can be configured per context. This limit includes accounting and authentication servers.

[ encrypted ] key value
Specifies the shared secret key used to authenticate the client to the servers. The encrypted keyword indicates the key specified is encrypted.
In 12.1 and earlier releases, the key value must be an alphanumeric string of 1 through 127 characters without encryption, and 1 through 256 characters with encryption.
In 12.2 and later releases, the key value must be an alphanumeric string of 1 through 127 characters without encryption, and 1 through 236 characters with encryption enabled.
The encrypted keyword is intended only for use by the system while saving configuration scripts. The system displays the encrypted keyword in the configuration file as a flag that the variable following the key keyword is the encrypted version of the plain text key. Only the encrypted key is saved as part of the configuration file.

max max_messages
Specifies the maximum number of outstanding messages that may be allowed to the server. max_messages must be an integer from 0 through 4000. Default: 256
max-rate max_rate

Specifies the rate (number of messages per second), at which the authentication messages should be sent to the RADIUS server. max_rate must be an integer from 0 through 1000. Default: 0 (Disabled)

oldports

Sets the UDP communication port to the old default for RADIUS communications to 1645.

port port_number

Specifies the port number to use for communications as an integer from 1 through 65535. Default: 1812

priority priority

Specifies the relative priority of this accounting server. The priority is used in server selection for determining to which server is to send accounting data. priority must be an integer from 1 through 1000 where 1 is the highest priority. When configuring two or more servers with the same priority you will be asked to confirm that you want to do this. If you use the -noconfirm option, you are not asked for confirmation and multiple servers could be assigned the same priority. Default: 1000

probe

Enables probe messages to be sent to the specified RADIUS server.

no-probe

Disables probe messages from being sent to the specified RADIUS server. This is the default behavior.

probe-username username

Specifies the username sent to the RADIUS server to authenticate probe messages. username must be an alphanumeric string of 1 through 127 characters.

probe-password [ encrypted ] password password

The password sent to the RADIUS server to authenticate probe messages. encrypted: This keyword is intended only for use by the system while saving configuration scripts. The system displays the encrypted keyword in the configuration file as a flag that the variable following the password keyword is the encrypted version of the plain text password. Only the encrypted password is saved as part of the configuration file. password password: Specifies the probe-user password for authentication. password must be an alphanumeric string of 1 through 63 characters.

type { mediation-device | standard }

Specifies the type of transactions the RADIUS server accepts. mediation-device: Specifies mediation-device specific AAA transactions. This device is available if you purchased a transaction control services license. Contact your local sales representative for licensing information. standard: Specifies standard AAA transactions. (Default)
admin-status { enable | disable }

Enables or disables the RADIUS authentication/accounting/charging server functionality, and saves the status setting in the configuration file to re-establish the set status at reboot.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage

This command is used to configure the RADIUS authentication server(s) with which the system is to communicate for authentication. Up to 128 RADIUS servers can be configured per context. The servers can be configured as Accounting, Authentication, charging servers, or any combination thereof.

Example

The following commands configure RADIUS server with the IP address set to 10.2.3.4, port to 1024, and priority to 10:

```
radius server 10.2.3.4 key sharedKey port 1024 max 127
radius server 10.2.3.4 encrypted key scrambledKey oldports priority 10
```
**radius strip-domain**

This command configures the stripping of the domain from the user name prior to authentication or accounting.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration

```
configure > context context_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
radius strip-domain { authentication-only | accounting-only }
no radius strip-domain
```

**Usage**

Use this command to configure the stripping of domain from the user name prior to authentication or accounting.

By default, strip-domain configuration will be applied to both authentication and accounting messages, if configured. When the argument `authentication-only` or `accounting-only` is present, `strip-domain` is applied only to the specified RADIUS message types.

**Example**

The following command configures the stripping of domain from the user name prior to authentication:

```
radius strip-domain authentication-only
```
radius timeout

This command configures the time duration to wait for a response from the RADIUS server before resending the messages.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration

*configure > context context_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
radius timeout timeout_duration
```

**default radius timeout**

**default**

Configures the default setting.

**timeout_duration**

Specifies the time duration (in seconds) to wait for a response from the RADIUS server before resending the messages. `timeout_duration` must be an integer from 1 through 65535. Default: 3

**Usage**

Use this command to configure the time duration to wait for a response from the RADIUS server before resending the messages.

**Example**

The following command configures the RADIUS timeout parameter to 300 seconds:

```
radius timeout 300
```
radius trigger

This command enables specific RADIUS triggers. The RADIUS Trigger configuration in the Context Configuration Mode is to enable backward compatibility. To configure RADIUS triggers for the default AAA group, you must configure them in the Context Configuration Mode.

Product
GGSN
P-GW
SAEGW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration
configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

[ no ] radius trigger { ms-timezone-change | qos-change | rai-change | rat-change | serving-node-change | uli-change }

default radius trigger

- no
  Disables the specified RADIUS trigger.

- default
  Configures the default setting.
  Default: All RADIUS triggers are enabled.

- ms-timezone-change
  Specifies to enable RADIUS trigger for MS time zone change.

- qos-change
  Specifies to enable RADIUS trigger for Quality of Service change.

- rai-change
  Specifies to enable RADIUS trigger for Routing Area Information change.

- rat-change
  Specifies to enable RADIUS trigger for Radio Access Technology change.
radius trigger

serving-node-change
Specifies to enable RADIUS trigger for Serving Node change.

uli-change
Specifies to enable RADIUS trigger for User Location Information change.

Usage
Use this command to enable RADIUS triggers.

Example
The following command enables RADIUS trigger for RAT change:

```
radius trigger rat-change
```
Remote Server List

Remote Server List Commands

**remote-server-list**

Creates or specifies the name of an existing remote server list for this context and enters the Remote Access List Configuration Mode.

**Product**
All

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration

```
configure > context context_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
remote-server-list name list_name

no remote-server-list name list_name
```

**Usage**

Enter the Remote Server List Configuration Mode for an existing list or for a newly defined list. This command is also used to remove an existing remote access list.

A maximum of 256 services (regardless of type) can be configured per system. Entering this command results in the following prompt:

```
[context_name]host_name(config-remote-server-list)#
```

Remote Server List Configuration Mode commands are defined in the Remote Server List Configuration Mode Commands chapter.

**Example**

The following command enters the Remote Server List Configuration Mode for the list named remote_list_1:

```
remote-server-list remote_list_1
```

The following command will remove remote_list_1 from the system:

```
no remote-server-list remote_list_1
```
route-access-list extended

Configures an access list for filtering routes based on a specified range of IP addresses.

**Product**
- PDSN
- HA
- GGSN

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration > Context Configuration
  ```
  configure > context context_name
  ```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**
```
[ no ] route-access-list extended identifier { deny | permit } ip { network_parameter } { mask_parameter }
```

- `no`
  Deletes the specified route access list.

- `identifier`
  Specifies a value to identify the route access list as an integer from 100 through 999.

- `deny`
  Deny routes that match the specified criteria.

- `permit`
  Permit routes that match the specified criteria.

- `ip network_parameter ip_address wildcard_mask`
  Specifies the network portion of the route to match. The network portion of the route is mandatory and must be expressed in one of the following ways:
    - `ip_address wildcard_mask`: Matches a network address and wildcard mask expressed in IPv4 dotted-decimal notation.
    - `any`: Matches any network address.
    - `host network_address`: Match the specified network address exactly. `network_address` must be an IPv4 address specified in dotted-decimal notation.
mask_parameter

This specifies the mask portion of the route to match. The mask portion of the route is mandatory and must be expressed in one of the following ways:

- \textit{mask_address wildcard_mask}: A mask address and wildcard mask expressed in IPv4 dotted-decimal notation.
- \textit{any}: Match any network mask.
- \textit{host mask_address}: Match the specified mask address exactly. \textit{mask_address} must be an IPv4 address specified in dotted-decimal notation.

Usage

Use this command to create an extended route-access-list that matches routes based on network addresses and masks.

Example

Use the following command to create an extended route-access-list:

\begin{verbatim}
route-access-list extended 100 permit ip 192.168.100.0 0.0.0.255
\end{verbatim}
route-access-list named

Configures an access list for filtering routes based on a network address and net mask.

**Product**
- PDSN
- HA
- GGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration
configure > context context_name

Entering the above command sequence results in the following prompt:

```
[context_name] host_name(config-ctx)#
```

**Syntax**

```
[ no ] route-access-list named list_name { deny | permit } { ip_address/mask | any } [ exact-match ]
```

- **no**
  Deletes the specified route access list.

- **list_name**
  Specifies name that identifies the route access list as an alphanumeric string of 1 through 79 characters.

- **deny**
  Denies routes that match the specified criteria.

- **permit**
  Permits routes that match the specified criteria.

- **ip_address/mask**
  Specifies the IP address (in IPv4 dotted-decimal notation) and the number of subnet bits, representing the subnet mask in CIDR notation (for example 10.1.1.1/24).

- **any**
  Matches any route.

- **exact-match**
  Matches the IP address prefix exactly.
**Usage**

Use this command to create route-access lists that specify routes that are accepted. Up to 16 routes can be added to each route-access-list.

**Example**

Use the following command to create a route access list named `list27` that permits routes that match `192.168.1.0/24` exactly:

```
route-access-list named list 27 permit 192.168.1.0/24 exact-match
```

To delete the list, use the following command:

```
no route-access-list named list 27 permit 192.168.1.0/24 exact-match
```
route-access-list standard

Configures an access-list for filtering routes based on network addresses.

Product

- PDSN
- HA
- GGSN

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > Context Configuration

configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-cxt)#

Syntax

[ no ] route-access-list standard identifier { permit | deny } { ip_address wildcard_mask | any | host network_address }

no

Deletes the specified route access list.

identifier

Specifies a value that identifies the route-access-list as an integer from 1 through 99.

deny

Denies routes that match the specified criteria.

permit

Permits routes that match the specified criteria.

ip_address wildcard_mask

Specifies the IP address and subnet mask to match for routes. Both ip_address and wildcard_mask must be entered in IPv4 dotted-decimal notation. (For example, 192.168.100.0 255.255.255.0)

any

Matches any route.

host network_address

Matches only route having the specified network address as if it had a 32-bit network mask. network_address must be an IPv4 address specified in dotted-decimal notation.
Usage
Use this command to create route-access-lists that specify routes that are accepted.

Example
Use the following command to create a route access list with an identifier of 10 that permits routes:

```
route-access-list standard 10 permit 192.168.1.0 255.255.255.0
```

To delete the list, use the following command:

```
no route-access-list standard 10 permit 192.168.1.0 255.255.255.0
```
route-map

Creates a route-map that is used by the routing features and enters Route-map Configuration mode. A route-map allows redistribution of routes and includes a list of match and set commands associated with it. The match commands specify the conditions under which redistribution is allowed; the set commands specify the particular redistribution actions to be performed if the criteria specified by match commands are met. Route-maps are used for detailed control over route distribution between routing processes. Up to eight route-maps can be created in each context. Refer to the Route-map Configuration Mode Commands chapter for more information.

Product
PDSN
HA
GGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration

```
configure > context context_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

Syntax

```
route-map map_name { deny | permit } seq_number

no route-map map_name
```

---

**no**

Deletes the specified route map.

**map_name**

Specifies the name of the route map to create or edit as an alphanumeric string of 1 through 69 characters.

**deny**

If the deny parameter is specified and the match command criteria are met, the route is not redistributed and any other route maps with the same map name are not examined. Set commands have no affect on deny route-maps.

**permit**

If the permit parameter is specified, and the match criteria are met, the route is redistributed as specified by set actions. If the match criteria are not met, the next route map with the same name is tested.
**seq_number**

Specifies the sequence number that indicates the position a new route map is to have in the list of route maps already configured with the same name. Route maps with the same name are tested in ascending order of their sequence numbers. This must be an integer from 1 through 65535.

---

**Usage**

Use this command to create route maps that allow redistribution of routes based on specified criteria and set parameters for the routes that get redistributed. The chassis supports a maximum of 64 route maps per context.

**Example**

To create a route map named map1 that permits routes that match the specified criteria, use the following command:

```plaintext
route-map map1 permit 10
```

To delete the route-map, enter the following command:

```plaintext
no route-map map1 permit 10
```
router

Enables BGP, Open Shortest Path First (OSPF) or OSPF version 3 (OSPFv3) routing functionality and enters the corresponding Configuration Mode. Refer to the BGP Configuration Mode Commands, OSPF Configuration Mode Commands or OSPFv3 Configuration Mode Commands chapter for details on associated Configuration mode commands.

Product
- PDSN
- HA
- GGSN
- P-GW
- SAEGW

Privilege
- Security Administrator, Administrator

Mode
- Exec > Global Configuration > Context Configuration
- configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

[ no ] router { bgp as_number | ospf | ospfv3 | rip }

no
Disables the specified routing support in the current context.

bgp as_number
Enables a BGP routing service for this context and assigns it the specified Autonomous System (AS) number before entering the BGP Configuration mode. as_number must be an integer from 1 through 4294967295.

**Important**: BGP routing is supported only for use with the HA.

ospf
Enables OSPF routing in this context and enters OSPF Configuration mode.

ospfv3
Enables OSPFv3 routing in this context and enter OSPFv3 Configuration mode.

Usage

Use this command to enable and configure OSPF and BGP routing in the current context.
Example

The following command enables the OSPF routing functionality and enters the OSPF Configuration Mode:

```
router ospf
```

The following command enables the OSPFv3 routing functionality and enters the OSPFv3 Configuration Mode:

```
router ospfv3
```

The following command enables a BGP routing service with an AS number of 100, and enters the BGP Configuration Mode:

```
router bgp 100
```
This section includes the commands `s102-service` through `wsg-service`.

**Mode**

Exec > Global Configuration > Context Configuration

    configure > context context_name

Entering the above command sequence results in the following prompt:

    [context_name]host_name(config-ctx)#

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
saegw-service

Creates a System Architecture Evolution Gateway (SAEGW) service or specifies an existing SAEGW service and enters the SAEGW Service Configuration Mode for the current context.

**Product**
SAEGW

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration

```
configure > context context_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
saegw-service service_name [ -noconfirm ]
```

```
no saegw-service service_name
```

- **no**
  Removes the specified SAEGW service from the context.

- **service_name**
  Specifies the name of the SAEGW service. If `service_name` does not refer to an existing service, the new service is created if resources allow. `service_name` is an alphanumeric string of 1 through 63 characters.

**Important:** Service names must be unique across all contexts within a chassis.

- **-noconfirm**
  Executes the command without any additional prompt and confirmation from the user.

**Usage**

Enter the SAEGW Service Configuration Mode for an existing service or for a newly defined service. This command is also used to remove an existing service.

**Important:** An S-GW and/or P-GW created in the same context must be associated with this SAEGW service.

A maximum of 256 services (regardless of type) can be configured per system.

**Caution:** Large numbers of services greatly increase the complexity of management and may impact overall system performance (for example, resulting from such things as system handoffs). Therefore, it is recommended that a
large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Entering this command results in the following prompt:

```
[context_name]hostname(config-saegw-service)#
```

SAEGW Service Configuration Mode commands are defined in the *SAEGW Service Configuration Mode Commands* chapter.

Use this command when configuring the following SAE components: SAEGW.

**Example**

The following command enters the existing SAEGW Service Configuration Mode (or creates it if it does not already exist) for the service named `saegw-service1`:

```
saegw-service saegw-service1
```

The following command will remove `pgw-service1` from the system:

```
no saegw-service saegw-service1
```
server

Configures remote server access protocols for the current context. This command is used to enter the specified protocols configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration

```
configure > context context_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

Syntax

```
server { ftpd | named | sshd | telnetd | tftp }
```

```
no server { ftpd | named | sshd | telnetd | tftp } [ kill ]
```

no
Disables the specified service.

```
ftpd
```

Enters the FTP Server Configuration Mode.

**Important:** The FTPD server can only be configured in the local context.

```
named
```

Starts the named server.

```
sshd
```

Enters the SSH Server Configuration Mode.

**Important:** The SSHD server allows only three unsuccessful login attempts before closing a login session attempt.

```
telnetd
```

Enters the Telnet Server Configuration Mode.

**Important:** The TELNET server allows only three unsuccessful login attempts before closing a login session attempt.
**tftpd**

Enters the TFTP Server Configuration Mode.

**Important:** The TFTP server can only be configured in the local context.

**kill**

Indicates all instances of the server are to be stopped. This option only works with the `ftpd`, `sshd`, `telnetd`, and `tftpd` commands.

**Usage**

Enter the Context Configuration Mode for the appropriate, previously defined context, to set the server option(s). Repeat the command as needed to enable/disable more than one option server daemon.

**Example**

```
server ftpd
server named
no server tftpd
server sshd
server telnetd
no server telnetd kill
```
service-redundancy-protocol

Configures Interchassis Session Recovery (ICSR) services for the current context. This command is used to enter the Service Redundancy Protocol Configuration Mode.

**Product**
All products supporting ICSR

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration

```
configure > context context_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
service-redundancy-protocol
```

**Usage**
Enter the Configuration Mode to set the service redundancy protocol options.

**Example**
The following command enters Service Redundancy Protocol Configuration Mode.

```
service-redundancy-protocol
```
session-event-module

Enables the event module, enters the Session Event Module Configuration Mode where the sending of S-GW subscriber-specific event files to an external server can be configured. From release 15.0 onwards, the session-event module is used by SGSN for event logging. By default, EDR files are generated at the location: /hd-raid/records/edr. After upgrading to release R15.0, if this CLI is configured, the path for EDR files changes to: /hd-raid/records/event.

Product

SAEGW
S-GW
SGSN

Privilege

Administrator

Mode

Exec > Global Configuration > Context Configuration

configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

[ no ] session-event-module

no

Disables the event module configuration.

Usage

Enter the Session Event Module Configuration Mode where the sending of S-GW subscriber-specific event files to an external server can be configured.

Entering this command results in the following prompt:

[context_name]hostname(config-event)#

Session Event Module Configuration Mode commands are defined in the Session Event Module Configuration Mode Commands chapter.
sgsn-service

Creates an SGSN service instance and enters the SGSN Service Configuration mode. This mode configures or edits the configuration for an SGSN service which controls the SGSN functionality.

An SGSN mediates access to GPRS/UMTS network resources on behalf of user equipment (UE) and implements the packet scheduling policy between different QoS classes. It is responsible for establishing the packet data protocol (PDP) context with the GGSN.

**Important:** For details about the commands and parameters, check the *SGSN Service Configuration Mode* chapter.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration

```
configure > context context_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
[ no ] sgsn-service srvc_name
```

- **no**
  Remove the configuration for the specified SGSN service from the configuration of the current context.

- **srvc_name**
  Specifies the name of the SGSN service as a unique alphanumeric string of 1 through 63 characters.

**Important:** Service names must be unique across all contexts within a chassis.

**Usage**
Use this command to create, edit, or remove an SGSN service.

**Example**

The following command creates an SGSN service named *sgsn1* in the current context:

```
sgsn-service sgsn1
```

The following command removes the sgsn service named *sgsn1* from the configuration for the current context:

```
```
no sgsn-service sgsn1
sgs-service

Creates an SGs service instance and enters the SGS Service Configuration mode.

Product
MME

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration
configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

[ no ] sgs-service name

no
Remove the configuration for the specified SGs service from the configuration of the current context.

name
Specifies a name for an SGs service as a unique alphanumeric string of 1 through 63 characters.

Important: Service names must be unique across all contexts within a chassis.

-noconfirm
Executes the command without any additional prompt and confirmation from the user.

Usage

Enter the SGS Service Configuration Mode for an existing service or for a newly defined service. This command is also used to remove an existing service.
A maximum of 256 services (regardless of type) can be configured per system.

Caution: Large numbers of services greatly increase the complexity of management and may impact overall system performance (for example, resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.

Entering this command results in the following CLI prompt:

[context_name]host_name(config-sgs-service)#

SGS Service Configuration Mode commands are defined in the MME SGS Service Configuration Mode Commands chapter.
Example

The following command creates an SGS service named $sgs1$ in the current context:

```
sgs-service sgs1
```

The following command removes the SGS service named $sgs1$ from the configuration for the current context:

```
no sgs-service sgs1
```
sgtp-service

Creates an SGTP service instance and enters the SGTP Service Configuration mode. This mode configures the GPRS Tunneling Protocol (GTP) related settings required by the SGSN and eWAG to support GTP-C (control plane) messaging and GTP-U (user data plane) messaging.

**Product**
- eWAG
- SGSN

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration > Context Configuration
- `configure > context context_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
[ no ] sgtp-service sgtp_service_name
```

- **no**
  - If previously configured, removes the specified SGTP service configuration in the current context.

- **sgtp_service_name**
  - Specifies name of the SGTP service.
  - `sgtp_service_name` must be an alphanumeric string of 1 through 63 characters.

**Important:** Service names must be unique across all contexts within a chassis.

**Usage**

Use this command to create, edit, or remove an SGTP service.

On entering this command, the CLI prompt changes to:

```
[context_name]host_name(config-sgtp-service)#
```

**Example**

The following command creates an SGTP service named `sgtp1` in the current context:

```
sgtp-service sgtp1
```

The following command removes, if previously configured, the SGTP service named `sgtp1` from the current context:

```
no sgtp-service sgtp1
```
sgw-service

Creates an S-GW service or specifies an existing S-GW service and enters the S-GW Service Configuration Mode for the current context.

Product
S-GW

SAEGW

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration

`configure > context context_name`

Entering the above command sequence results in the following prompt:

```plaintext
[context_name]host_name(config-ctx)#
```

Syntax

```
sgw-service service_name [ -noconfirm ]

no sgw-service service_name
```

- `service_name`
  Specifies the name of the S-GW service. If `service_name` does not refer to an existing service, the new service is created if resources allow. `service_name` is an alphanumeric string of 1 through 63 characters.

**Important:** Service names must be unique across all contexts within a chassis.

- `-noconfirm`
  Executes the command without any additional prompt and confirmation from the user.

- `no sgw-service service_name`
  Removes the specified S-GW service from the context.

Usage

Enter the S-GW Service Configuration Mode for an existing service or for a newly defined service. This command is also used to remove an existing service.

A maximum of 256 services (regardless of type) can be configured per system.

**Caution:** Large numbers of services greatly increase the complexity of management and may impact overall system performance (for example, resulting from such things as system handoffs). Therefore, it is recommended that a large number of services only be configured if your application absolutely requires it. Please contact your local service representative for more information.
Entering this command results in the following prompt:

```
[context_name]hostname(config-sgw-service)#
```

S-GW Service Configuration Mode commands are defined in the *S-GW Service Configuration Mode Commands* chapter.

Use this command when configuring the following SAE components: S-GW.

**Example**

The following command enters the existing S-GW Service Configuration Mode (or creates it if it does not already exist) for the service named *sgw-service1*:

```
sgw-service sgw-service1
```

The following command will remove *spgw-service1* from the system:

```
no sgw-service sgw-service1
```
ssh

Generates public and private keys for use with the configured Secure Shell (SSH) server for the current context and sets the public/private key pair to specified values.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration

`configure > context context_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
ssh { generate key | key data length octets } [ type { v1-rsa | v2-rsa | v2-dsa } ]
no ssh key [ type { v1-rsa | v2-rsa | v2-dsa } ]
```

**Usage**

Generate secure shell keys for use in public key authentication.

---

**Important:** For maximum security, it is recommended that only SSH v2 be used. `v2-rsa` is the recommended key type.
Example

```plaintext
ssh generate key

ssh key g6j93fw59cx length 128
```
ssl

Creates a new Secure Sockets Layer (SSL) template or specifies an existing one and enters the SSL Template Configuration Mode.

Product
SCM

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration
configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

[ no ] ssl template name { ssl-subscriber }

no
Removes the specified SSL template from the context.

template name
Specifies the name of a new or existing SSL template as an alphanumeric string of 1 through 127 alphanumeric characters.

ssl-subscriber
Specifies that the SSL template is an SSL subscriber template.

Usage
Use this command to create a new SSL template or modify an existing one. Entering this command results in the following prompt:

[context_name]hostname(config-ctx-ssl-subscriber-template)#

SSL Template Configuration Mode commands are defined in the SSL Template Configuration Mode Commands chapter.

Example
The following command specifies the SSL template ssl_template_1 and enters the SSL Template Configuration Mode:

ssl template ssl_template_1 ssl-subscriber
subscriber

Configures the specified subscriber for the current context.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration

```bash
configure > context context_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```bash
subscriber { default | name user_name } asn-service-info mobility [ ipv4 | ipv6 | ipv6-ipv4 ]
```

```bash
no subscriber { default | name user_name }
```

- **Indicates the subscriber specified is to be removed from the list of allowed users for the current context.**

  - **default | name user_name**

    - **default**: Enters the Subscriber Configuration Mode for the context’s default subscriber settings.
    - **name user_name**: Specifies the user which is to be allowed to use the services of the current context.

    - **user_name** must be an alphanumeric string of 1 through 127 characters.

    - **asn-service-info mobility**: Indicates the type of mobility supported and enabled in the Autonomous System Number (ASN).

**Usage**

Enter the Subscriber Configuration Mode for actual users as well as for a default subscriber for the current context.

Entering this command results in the following prompt:

```
[context_name]hostname(config-subscriber)#
```

Subscriber Configuration Mode commands are defined in the *Subscriber Configuration Mode Commands* chapter.

NAS uses the specified parameter for asn-service-info mobility to indicate and pack the mobility support field for IPv4, IPv6, or both, in the Service-Info attribute in the Access-request. RADIUS sends back this attribute in the Access-accept message by indicating respective bits to authorize the service indicated by NAS.

**Important**: A maximum of 128 subscribers and/or administrative users may be locally configured per context.
Example

Following command configures the default subscriber in a context:

```
subscriber default
```

Following command removes the default subscriber from a context:

```
no subscriber default
```

Following command configures a subscriber named `user1` in a context:

```
subscriber name user1
```

Following command removes a subscriber named `user1` from a context:

```
no subscriber name user1
```
threshold available-ip-pool-group

Configures context-level thresholds for IP pool utilization for the system.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration
configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

threshold available-ip-pool-group low_thresh [ clear high_thresh ]

default threshold available-ip-pool-group

default

Configures the default setting.

low_thresh

The low threshold IP pool utilization percentage that must be met or exceeded within the polling interval to generate an alert or alarm. low_thresh can be configured as an integer from 0 through 100. Default: 10

clear high_thresh

Specifies the high threshold IP pool utilization percentage that maintains a previously generated alarm condition. If the utilization percentage rises above the high threshold within the polling interval, a clear alarm will be generated. high_thresh can be configured as an integer from 0 through 100. Default: 10

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the low threshold.

Usage

When IP address pools are configured on the system, they can be assigned to a group. IP address pool utilization thresholds generate alerts or alarms based on the utilization percentage of all IP address contained in the pool group during the specified polling interval.

All configured public IP address pools that were not assigned to a group are treated as belonging to the same group. Individual configured static or private pools are each treated as their own group.

Alerts or alarms are triggered for IP address pool utilization based on the following rules:

• Enter Condition: Actual IP address utilization percentage per pool group ≤ Low Threshold

• Clear Condition: Actual IP address utilization percentage per pool group > High Threshold
If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval. The following table describes the possible methods for configuring IP pool utilization thresholds:

Table 23. IP Pool Utilization Thresholds - Configuration Methods

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Context-level</td>
<td>A single IP pool utilization threshold can be configured for all IP pool groups within a given system context. If a single threshold is configured for all pool groups, separate alerts or alarms can be generated for each group. This command configures that threshold.</td>
</tr>
<tr>
<td>IP address pool-level</td>
<td>Each individual IP address pool can be configured with its own threshold. Thresholds configured for individual pools take precedence over the context-level threshold that would otherwise be applied (if configured). In the event that two IP address pools belonging to the same pool group are configured with different thresholds, the system uses the pool configuration that has the greatest low threshold for that group.</td>
</tr>
</tbody>
</table>

Example

The following command configures a context-level IP pool utilization low threshold percentage of 10 and a high threshold of 35 for a system using the Alarm thresholding model:

```
threshold available-ip-pool-group 10 clear 35
```
threshold ha-service init-rrq-rcvd-rate

Sets an alarm or alert based on the average number of calls setup per second for an HA service.

Product
HA

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration
configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

threshold ha-service init-rrq-rcvd-rate high_thresh [ clear low_thresh ]

no threshold ha-service init-rrq-rcvd-rate

no

Deletes the alert or alarm.

high_thresh

Sets the high threshold average number of calls setup per second that must be met or exceeded within the polling interval to generate an alert or alarm. It can be configured as an integer from 0 through 1000000. Default: 0

clear low_thresh

Sets the low threshold average number of calls setup per second that must be met or exceeded within the polling interval to clear an alert or alarm. It can be configured as an integer from 0 through 1000000. Default: 0

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Use this command to set an alert or an alarm when the average number of calls setup upper second is equal to or less than a specified number of calls per second.

Alerts or alarms are triggered for the number of calls setup per second based on the following rules:

• Enter Condition: Actual number of calls setup per second > High Threshold
  • Clear Condition: Actual number of calls setup per second ≤ Low Threshold

Example
The following command configures a number of calls setup per second threshold of 1000 and a low threshold of 500 for a system using the Alarm thresholding model:

```bash
threshold ha-service init-rrq-rcvd-rate 1000 clear 500
```
threshold ip-pool-free

Sets an alarm or alert based on the percentage of IP addresses that are unassigned in an IP pool. This command affects all IP pools in the current context.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration
configure > context context_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx)#

Syntax

threshold ip-pool-free low_thresh [ clear high_thresh ]

default threshold ip-pool-free

default

Configures the default setting.

low_thresh

Sets the low threshold percentage of addresses available in an IP pool that must be met or exceeded within the polling interval to generate an alert or alarm. It can be configured as an integer between 0 and 100. Default: 0

clear high_thresh

Sets the high threshold percentage of addresses available in an IP pool that maintains a previously generated alarm condition. If the utilization percentage rises above the high threshold within the polling interval, a clear alarm will be generated. It may be configured as an integer between 0 and 100. Default: 0

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the low threshold.

Usage

Use this command to set an alert or an alarm when the number of unassigned IP addresses in any pool is equal to or less than a specified percentage of the total number of addresses in the pool. Alerts or alarms are triggered for percentage of IP address pool free based on the following rules:

- Enter Condition: Actual percentage of IP addresses free per pool ≤ Low Threshold
- Clear Condition: Actual percentage of IP addresses free per pool > High Threshold
Important: This command is overridden by the settings of the alert-threshold keyword of the ip pool command.

Example

The following command configures a context-level IP pool percentage of IP addresses that are unused low threshold percentage of 10 and a high threshold of 35 for a system using the Alarm thresholding model:

```
threshold ip-pool-free 10 clear 35
```
threshold ip-pool-hold

Sets an alert based on the percentage of IP addresses from an IP pool that are on hold. This command affects all IP pools in the current context.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration

```
configure > context context_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
threshold ip-pool-hold high_thresh [ clear low_thresh ]
```

**default threshold ip-pool-hold**

```
default
```

Configures the default setting.

```
high_thresh
```

Sets the high threshold percentage of addresses on hold in an IP pool that must be met or exceeded within the polling interval to generate an alert or alarm. It can be configured as an integer from 0 through 100. Default: 0

```
clear low_thresh
```

Sets the low threshold percentage of addresses on hold in an IP pool that maintains a previously generated alarm condition. If the utilization percentage rises below the low threshold within the polling interval, a clear alarm will be generated. It may be configured as an integer from 0 through 100. Default: 0

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**

Use this command to set an alert or an alarm when the percentage of IP addresses on hold in any pool is equal to or greater than a specified percentage of the total number of addresses in the pool. Alerts or alarms are triggered for percentage of IP address pool addresses on hold based on the following rules:

- **Enter Condition:** Actual percentage of IP addresses on hold per pool > High Threshold
- **Clear Condition:** Actual percentage of IP addresses on hold per pool ≤ Low Threshold
**Important:** This command is overridden by the settings of the `alert-threshold` keyword of the `ip pool` command.

**Example**

The following command configures a context-level IP pool percentage of IP addresses that are on high threshold percentage of 35 and a low threshold of 10 for a system using the Alarm thresholding model:

```
threshold ip-pool-hold 35 clear 10
```
threshold ip-pool-release

Sets an alert based on the percentage of IP addresses from an IP pool that are in the release state. This command affects all IP pools in the current context.

Product

All

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > Context Configuration

`configure > context context_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

Syntax

```
threshold ip-pool-release high_thresh [ clear low_thresh ]
```

default threshold ip-pool-release

```
default
Configures the default setting.
```

```
high_thresh
Sets the high threshold percentage of addresses in the release state in an IP pool that must be met or exceeded within the polling interval to generate an alert or alarm. It can be configured as an integer from 0 through 100. Default: 0
```

```
clear low_thresh
Sets the low threshold percentage of addresses in the release state in an IP pool that maintains a previously generated alarm condition. If the utilization percentage rises below the low threshold within the polling interval, a clear alarm will be generated. It may be configured as an integer from 0 through 100. Default: 0
```

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the low threshold.

Usage

Use this command to set an alert or an alarm when the number of IP addresses the release state in any pool is equal to or greater than a specified percentage of the total number of addresses in the pool.

Alerts or alarms are triggered for percentage of IP address pool addresses in the release state based on the following rules:

- **Enter Condition:** Actual percentage of IP addresses in the release state per pool > High Threshold
- **Clear Condition:** Actual percentage of IP addresses in the release state per pool ≤ Low Threshold
threshold ip-pool-release

**Important:** This command is overridden by the settings of the `alert-threshold` keyword of the `ip pool` command.

**Example**

The following command configures a context-level IP pool percentage of IP addresses that are in the release state high threshold percentage of 35 and a low threshold of 10 for a system using the Alarm thresholding model:

```
threshold ip-pool-release 35 clear 10
```
threshold ip-pool-used

Sets an alert based on the percentage of IP addresses that have been assigned from an IP pool. This command affects all IP pools in the current context.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration

Syntax

```markdown
threshold ip-pool-used high_thresh [ clear low_thresh ]
default threshold ip-pool-used
```

**default**

Configures the default setting.

**high_thresh**

Sets the high threshold percentage of addresses assigned from an IP pool that must be met or exceeded within the polling interval to generate an alert or alarm. It can be configured as an integer from 0 through 100. Default: 0

**clear low_thresh**

Sets the low threshold percentage of addresses assigned from an IP pool that maintains a previously generated alarm condition. If the utilization percentage rises above the high threshold within the polling interval, a clear alarm will be generated. It may be configured to any integer between 0 and 100. Default: 0

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the low threshold.

Usage

Use this command to set an alert or an alarm when the number of IP addresses assigned from any pool is equal to or greater than a specified percentage of the total number of addresses in the pool. Alerts or alarms are triggered for percentage of IP address pool addresses used based on the following rules:

- **Enter Condition:** Actual percentage of IP addresses used per pool > High Threshold
- **Clear Condition:** Actual percentage of IP addresses used per pool ≤ Low Threshold
**Important:** This command is overridden by the settings of the `alert-threshold` keyword of the `ip pool` command.

**Example**

The following command configures a context-level IP pool percentage of IP addresses that are used high threshold percentage of 35 and a low threshold of 10 for an system using the Alarm thresholding model:

```
threshold ip-pool-used 35 clear 10
```
## threshold monitoring

Enables or disables thresholds alerting for a group of thresholds.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration

```
configure > context context_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
[ default | no ] threshold monitoring available-ip-pool-group
```

- **default**
  
  Configures the default setting.

- **no**
  
  Disables threshold monitoring for the specified value.

- **available-ip-pool-group**
  
  Enables threshold monitoring for IP pool thresholds at the context level and the IP address pool-level. Refer to the `threshold available-ip-pool-group` command, the `threshold ip-pool-x` commands and the `alert-threshold` keyword of the `ip pool` command for additional information on these values.

**Usage**

Thresholding on the system is used to monitor the system for conditions that could potentially cause errors or outage. Typically, these conditions are temporary (i.e high CPU utilization, or packet collisions on a network) and are quickly resolved. However, continuous or large numbers of these error conditions within a specific time interval may be indicative of larger, more severe issues. The purpose of thresholding is to help identify potentially severe conditions so that immediate action can be taken to minimize and/or avoid system downtime.

Thresholding reports conditions using one of the following mechanisms:

- **SNMP traps**: SNMP traps have been created that indicate the condition (high threshold crossing and/or clear) of each of the monitored values. Complete descriptions and other information pertaining to these traps is located in the starentMIB(8164).starentTraps(2) section of the `SNMPMIB Reference`.

  The generation of specific traps can be enabled or disabled on the system allowing you to view only those traps that are most important to you.

- **Logs**: The system provides a facility called threshold for which active and event logs can be generated. As with other system facilities, logs are generated Log messages pertaining to the condition of a monitored value are generated with a severity level of WARNING.
• **Alarm System**: High threshold alarms generated within the specified polling interval are considered “outstanding” until the condition no longer exists and/or a condition clear alarm is generated. “Outstanding” alarms are reported to through the system’s alarm subsystem and are viewable through the CLI.

The following table indicates the reporting mechanisms supported by each of the above models.

<table>
<thead>
<tr>
<th>Model</th>
<th>SNMP Traps</th>
<th>Logs</th>
<th>Alarm System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Alarm</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

Refer to the `threshold poll` command in Global Configuration Mode Commands for information on configuring the polling interval over which IP address pool utilization is monitored.

**Example**

The following command enables threshold monitoring for IP pool thresholds at the context level and the IP address pool-level:

```
threshold monitoring available-ip-pool-group
```
threshold pdsn-service init-rrq-rcvd-rate

Sets an alarm or alert based on the average number of calls setup per second for a PDSN service.

Product
PDSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration
configure > context context_name
Entering the above command sequence results in the following prompt:

[context_name] host_name(config-ctx)#

Syntax

threshold pdsn-service init-rrq-rcvd-rate high_thresh [ clear low_thresh ]

no threshold pdsn-service init-rrq-rcvd-rate

no
Deletes the alert or alarm.

high_thresh
Sets the high threshold average number of calls setup per second that must be met or exceeded within the polling interval to generate an alert or alarm. It can be configured as an integer between 0 and 1000000. Default: 0

clear low_thresh
Sets the low threshold average number of calls setup per second that must be met or exceeded within the polling interval to clear an alert or alarm. It can be configured as an integer between 0 and 1000000. Default: 0

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage
Use this command to set an alert or an alarm when the average number of calls set upper second is equal to or less than a specified number of calls per second.
Alerts or alarms are triggered for the number of calls setup per second based on the following rules:
• Enter Condition: Actual number of calls setup per second > High Threshold
• Clear Condition: Actual number of calls setup per second ≤ Low Threshold

Example
The following command configures a number of calls setup per second threshold of 1000 and a low threshold of 500 for a system using the Alarm thresholding model:

```
threshold psdn-service init-rrq-rcvd-rate 1000 clear 500
```
**udr-module active-charging-service**

Enables creation, configuration and deletion of the User Data Record (UDR) module for the context.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration

```
configure > context context_name
```

Entering the above command sequence results in the following prompt:

```
[context_name] host_name(config-ctx)#
```

**Syntax**

```
[ no ] udr-module active-charging-service
```

- **no**
  
  Deletes the UDR module configuration for the current context.

**Usage**

Use this command to create the UDR module for the context, and configure the UDR module for active charging service records. You must be in a non-local context when specifying this command, and you must use the same context when specifying the EDR module command. 

On entering this command, the CLI prompt changes to:

```
[context_name] host_name(config-udr)#
```

**Example**

The following command creates the UDR module for the context, and enters the UDR Module Configuration Mode:

```
udr-module active-charging-service
```
wsg-service

Enables or disables Wireless Security Gateway (WSG) service. When enabled you are in WSG Service Configuration mode. (VPC only)

**Product**
SecGW (WSG)

**Privilege**
Security Administrator

**Mode**
Exec > Global Configuration > Context Configuration
`configure > context context_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx)#
```

**Syntax**

```
 wsg-service service_name
no wsg-service service_name
```

- **no**
  Disables the specified WSG service.

- **service_name**
  Specifies the name of the WSG service as an alphanumeric string of 1 through 63 characters.

**Important:** Service names must be unique across all contexts within a chassis.

**Usage**
Use this command to enter the WSG Service Configuration Mode. For additional information, see the *WSG Service Configuration Mode Commands* chapter.

**Example**
The following command enters the WSG Service Configuration Mode:
```
 wsg-service wsg01
```
Chapter 56
Credit Control Configuration Mode Commands

The Credit Control configuration Mode is used to configure prepaid services for Diameter/RADIUS applications.

Mode

Exec > ACS Configuration > Credit Control Configuration

active-charging service service_name > credit-control

Entering the above command sequence results in the following prompt:

[local]host_name(config-dcca)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
apn-name-to-be-included

This command configures whether the virtual or real Access Point Name (APN) is sent in Credit Control Application (CCA) messaging.

Product

All

Privilege

Security Administrator, Administrator

Mode

Exec > ACS Configuration > Credit Control Configuration

active-charging service service_name > credit-control

Entering the above command sequence results in the following prompt:

[local]host_name(config-dcca)#

Syntax

apn-name-to-be-included { gn | virtual }

default apn-name-to-be-included

  default
  Configures this command with the default setting.
  Default: gn

  gn
  Sends the Gn APN name in the CCA messages.

  virtual
  Sends the virtual APN name, if configured in the APN Configuration Mode, in the CCA messages.

Usage

Use this command to configure the APN information in CCA messages. Virtual APN name can be set to be sent in CCA messages if it is configured in the APN Configuration Mode.

Example

The following command sets the virtual APN name to be sent in CCA message:

apn-name-to-be-included virtual
app-level-retransmission

This command enables/disables application-level retransmissions with the “T” bit set.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Credit Control Configuration

`active-charging service service_name > credit-control`

Entering the above command sequence results in the following prompt:

[local]host_name(config-dcca)#

**Syntax**

```
app-level-retransmission { set-retransmission-bit | unset-retransmission-bit }
```

**default**

```
default app-level-retransmission
```

| Configures this command with the default setting. |
| Default: *unset-retransmission-bit* |

**set-retransmission-bit**

Sets the retransmission bit.

**unset-retransmission-bit**

Unsets the retransmission bit.

**Usage**

Use this command to enable application-level transmission with “T” bit set.
'T' bit setting is done only for DIABASE protocol-based rerouting and not for application-based retransmissions. In order to identify such retransmissions, the server expects the T bit to be set at all levels (both DIABASE and application) of retransmission, which can be achieved with this CLI command.

**Example**

The following command specifies to set retransmission bit:

```
app-level-retransmission set-retransmission-bit
```
associate

This command associates/disassociates a failure handling template with the Diameter Credit Control Application (DCCA) service.

Product
- GGSN
- HA
- HSGW
- IPSG
- PDSN
- P-GW
- S-GW
- SAEGW

Privilege
- Security Administrator
- Administrator

Mode
- Exec > ACS Configuration > Credit Control Configuration

active-charging service service_name > credit-control

Entering the above command sequence results in the following prompt:

[local]host_name(config-dcca)#

Syntax

associate failure-handling-template template_name

no associate failure-handling-template

no

Disassociates a failure handling template with the DCCA service.

failure-handling-template template_name

Associates a previously created failure handling template with the DCCA service. template_name specifies the name for a pre-configured failure handling template. template_name must be an alphanumeric string of 1 through 63 characters.

For more information on failure handling templates, refer to the failure-handling-template command in the Global Configuration Mode Commands chapter.

Usage

Use this command to associate a configured failure handling template with the DCCA service.

The failure handling template defines the action to be taken when the Diameter application encounters a failure supposing a result-code failure, Tx-expiry or response-timeout. The application will take the action given by the template. For more information on failure handling template configurations, refer to the Diameter Failure Handling Template Configuration Mode Commands chapter.
**Important:** Only one failure handling template can be associated with the DCCA service. The failure handling template should be configured prior to issuing this command.

If the association is not made to the template then failure handling behavior configured in the application with the `failure-handling` command will take its effect.

**Example**

The following command associates a pre-configured failure handling template called `fht1` to the DCCA service:

```
associate failure-handling-template fht1
```
diameter dictionary

This command configures the Diameter Credit Control dictionary for the Active Charging Service (ACS).

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Credit Control Configuration

```
active-charging service service_name > credit-control
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-dcca)#
```

**Syntax**

```
diameter dictionary { dcca-custom1 | dcca-custom10 | dcca-custom11 | dcca-custom12 | dcca-custom13 | dcca-custom14 | dcca-custom15 | dcca-custom16 | dcca-custom17 | dcca-
custom18 | dcca-custom19 | dcca-custom2 | dcca-custom20 | dcca-custom21 | dcca-custom22 |
dcca-custom23 | dcca-custom24 | dcca-custom25 | dcca-custom26 | dcca-
custom27 | dcca-custom28 | dcca-
custom29 | dcca-custom3 | dcca-
custom30 | dcca-
custom4 | dcca-
custom5 | dcca-
custom6 | dcca-
custom7 | dcca-
custom8 | dcca-
custom9 | dynamic-load | standard }
```

**default diameter dictionary**

```
default
```

Configures this command with the default setting.
Default: standard dictionary

```
dcca-custom1 ... dcca-custom30
```

Configures a custom Diameter dictionary.

**dynamic-load**

```
dynamic-load
```

Configures the dynamically loaded Diameter dictionary. The dictionary name must be an alphanumeric string of 1 through 15 characters.
For more information on dynamic loading of Diameter dictionaries, see the diameter dynamic-
dictionary in the Global Configuration Mode Commands chapter of this guide.

```
standard
```

Configures the standard Diameter dictionary.
Default: Enabled

**Usage**

Use this command to select the Diameter dictionary for ACS.

**Example**

The following command selects the standard Diameter dictionary:
diameter dictionary standard
**diameter disable-final-reporting-in-ccru**

This command controls sending of CCR-U with reporting reason as FINAL immediately on receiving a 4012 or 4010 result-code at MSCC level.

**Product**
- GGSN
- HA
- IPSG
- PDSN
- P-GW

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > ACS Configuration > Credit Control Configuration
- `active-charging service service_name > credit-control`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-dcca)#
```

**Syntax**

```
diameter disable-final-reporting-in-ccru

{ default | no } diameter disable-final-reporting-in-ccru
```

<table>
<thead>
<tr>
<th>default</th>
<th>no</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configures this command with the default setting. Default behavior is to send CCR-U with reporting reason as FINAL immediately on receiving 4010/4012 result-code.</td>
<td></td>
</tr>
</tbody>
</table>

**Usage**

As per the current implementation, CCR-U is sent immediately on receiving 4010 or 4012 Result-Code at MSCC level. This new CLI command controls sending of immediate CCR-U with FINAL as Reporting-Reason. All other behaviors remain almost same like a Rating-group being blacklisted.

If this CLI command is configured, on receiving the result-code 4010/4012 at MSCC-level, immediate CCR-U with FINAL as Reporting-Reason will not be sent. All USU corresponding to that rating group is reported in CCR-T message.

**Example**

The following command specifies not to send immediate CCR-U with FINAL as Reporting-Reason:

```
diameter disable-final-reporting-in-ccru
```
diameter dynamic-rules request-quota

This command specifies to request quota immediately in the CCR sent to the Gy interface when the traffic matches the dynamic rules with Online AVP enabled and received over Gx interface.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Credit Control Configuration
active-charging service service_name > credit-control

Entering the above command sequence results in the following prompt:
[local]host_name(config-dcca)#

Syntax

diameter dynamic-rules request-quota { on-traffic-match | on-receiving-rule }

default diameter dynamic-rules request-quota

default
Configures this command with the default setting.
Default: on-receiving-rule

on-traffic-match
Requests quota only when there is traffic matching the dynamic rules with Online AVP enabled.

on-receiving-rule
Requests quota on receiving a dynamic rule with Online AVP enabled.

Usage
Use this command to request quota when the traffic matches the dynamic rules with Online AVP enabled.

Example
The following command specifies to request quota on receiving a dynamic rule with Online AVP enabled:

diameter dynamic-rules request-quota on-receiving-rule
**diameter enable-quota-retry**

This command enables/disables Quota Retry Timer for blacklisted content.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Credit Control Configuration

`active-charging service service_name > credit-control`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-dcca)#
```

**Syntax**

```
[ no ] diameter enable-quota-retry end-user-service-denied
```

- `no`

  Configures this command with the default setting.

**Usage**

Quota-Retry-Time is currently not applicable to a Rating-Group which is blacklisted with 4010 (END_USER_SERVICE_DENIED).

If this CLI command is configured, after the quota-retry timeout, CCR-U including the RSU is sent for blacklisted content also. That is, quota will be requested for 4010 blacklisted content also.

Without the configuration of this CLI command, the old behavior persists that is, after quota retry-timer expiry, CCR-U is not sent for 4010 blacklisted category.

**Example**

The following command allows sending CCR-U requesting quota for blacklisted content:

```
diameter enable-quota-retry end-user-service-denied
```
**diameter exclude-mscc-in-ccr-terminate**

This command enables to exclude Multiple-Services-Credit-Control (MSCC) AVP in CCR-T message.

**Product**
- GGSN
- IPSG

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Credit Control Configuration

active-charging service service_name > credit-control

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-dcca)#
```

**Syntax**

```
[ default | no ] diameter exclude-mscc-in-ccr-terminate
```

- **default**
  Includes MSCC AVP in CCR-T.

- **no**
  Includes MSCC AVP in CCR-T.

**Usage**

Use this command to exclude MSCC AVP in CCR-T, which is included by default. Also, see the `diameter mscc-per-ccr-update` command.

**Example**

The following command specifies to exclude MSCC AVP in CCR-T:

```
diameter exclude-mscc-in-ccr-terminate
```
diameter fui-redirected-flow

This command enables to control the behavior of marking redirected HTTP flow as free-of-charge.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Credit Control Configuration

active-charging service service_name > credit-control

Entering the above command sequence results in the following prompt:

[local]host_name(config-dcca)#

Syntax

[ no ] diameter fui-redirected-flow allow

  no

  Disables the behavior of marking redirected HTTP flow as free-of-charge.
  Default: diameter fui-redirected-flow allow

Usage

Use this command to control the behavior of marking redirected HTTP flow as free-of-charge when the Final-Unit-Indication (FUI) Diameter AVP comes without Filter IDs.

Important: Note that the default value, when configured, does not appear in the output of the show configuration command output; instead appear only in the output of the show configuration verbose command. When the HTTP redirection feature is disabled using the no diameter fui-redirected-flow allow command, it will be appear in the output of the show configuration command.

Example

The following command specifies to allow the packets free of charge, when matching the redirected-flow:

  diameter fui-redirected-flow allow
diameter gsu-with-only-infinite-quota

This command configures whether to accept/reject CCA messages that contain Granted-Service-Unit AVP with only infinite quota grants from the server.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > ACS Configuration > Credit Control Configuration

active-charging service service_name > credit-control

Entering the above command sequence results in the following prompt:

[local]host_name(config-dcca)#

**Syntax**

```plaintext
diameter gsu-with-only-infinite-quota { accept-credit-control-answer | reject-credit-control-answer }

default diameter gsu-with-only-infinite-quota
```

- **default**
  
  Configures this command with the default setting.
  
  Default: `reject-credit-control-answer`

- **accept-credit-control-answer**
  
  Accepts the Credit-Control-Answer message.

- **reject-credit-control-answer**
  
  Rejects the Credit-Control-Answer message.

**Usage**

Use this command to accept/reject CCA messages that contain the Granted-Service-Unit AVP with only infinite quota grants from the server.

**Example**

The following command specifies to accept CCA with the Granted-Service-Unit AVP containing only Infinite quota:

```plaintext
diameter gsu-with-only-infinite-quota accept-credit-control-answer
```
diameter ignore-returned-rulebase-id

This command configures to accept/ignore the rulebase ID in the Rulebase-Id AVP returned by the Diameter server in CCA messages.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Credit Control Configuration

```
active-charging service service_name > credit-control
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-dcca)#
```

**Syntax**

```
[ default | no ] diameter ignore-returned-rulebase-id
```

- **default**
  Configures this command with the default setting.
  Default: Accept

- **no**
  Accepts the rulebase ID received from Diameter server in CCA.

**Usage**

Use this command to ignore/accept rulebase ID returned from the Diameter server in CCA.

**Example**

The following command ignores the rulebase ID returned from the Diameter server in CCA:

```
diameter ignore-returned-rulebase-id
```
diameter ignore-service-id

This command enables to accept/ignore service ID in the Service-Identifier AVP defined in the Diameter dictionaries. This command is applicable to all products that use the Gy interface.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Credit Control Configuration

`active-charging service service_name > credit-control`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-dcca)#
```

**Syntax**

```
[ default | no ] diameter ignore-service-id
```

---

**default**
Configures this command with the default setting.
Default: Accept

---

**no**
Specifies to accepts the service ID.

---

**Usage**
Use this command to ignore/accept service ID value in the Service-Identifier AVP in the Diameter dictionaries for Gy interface implementations.
This command can be used to disable the usage of the Service-Identifier AVP for Gy interface implementations even if any of the Diameter dictionaries support the Service-Identifier AVP, and if this AVP should not be used for Gy interactions but must be present in GCDRs/eGCDRs.

**Example**
The following command specifies to ignore service ID in the Diameter dictionaries:

```
diameter ignore-service-id
```
**diameter mscc-final-unit-action terminate**

This command enables either to terminate a PDP session immediately when the Final-Unit-Action (FUA) in a particular Multiple Service Credit Control (MSCC) is set as TERMINATE and the quota is exhausted for that service, or to terminate the session after all other MSCCs (categories) have used up their available quota.

**Important:** This command is available only in StarOS 10.2 and later releases.

**Product**  
GGSN

**Privilege**  
Security Administrator, Administrator

**Mode**  
Exec > ACS Configuration > Credit Control Configuration

```
active-charging service service_name > credit-control
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-dcca)#
```

**Syntax**

```
diameter mscc-final-unit-action terminate { category | session { on-per-mscc-exhaustion | on-all-mscc-exhaustion } } 

default diameter mscc-final-unit-action terminate
```

**default**  
Configures this command with the default setting.  
**Default:** Same as `diameter mscc-final-unit-action terminate category`

**category**  
This is the standard behavior wherein the category is terminated if the Final-Unit-Indication AVP comes with TERMINATE for a given MSCC.

**session { on-per-mscc-exhaustion | on-all-mscc-exhaustion }**

Terminates the session depending on the quota usage of one MSCC or all the MSCCs.  
**on-per-mscc-exhaustion:** When the FUA in a particular MSCC is set as TERMINATE and the quota is exhausted for that service, the session will be terminated immediately regardless of the state of the other MSCCs.  
**on-all-mscc-exhaustion:** When the FUA in a particular MSCC is set as TERMINATE and the quota is exhausted for that service, the session termination will be initiated after all the other MSCCs (categories) have used up their available quota. There will no more CCR(U) messages sent requesting quota after receiving the FUA as TERMINATE in the MSCC level.
Usage

Use this command to terminate a PDP session immediately when the FUA in a particular MSCC is set as TERMINATE and the quota is exhausted for that service, or to terminate the session after all other MSCCs (categories) have used up their available quota.

Example

The following command terminates the PDP session after quota exhausts for all MSCCs when MSCC FUA is set to TERMINATE:

    diameter mscc-final-unit-action terminate session on-all-mscc-exhaustion
diameter mscc-per-ccr-update

This command configures sending single/multiple Multiple-Services-Credit-Control (MSCC) AVP in CCR-U messages.

**Important:** This command is available only in StarOS 8.3 and later releases.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Credit Control Configuration

```
active-charging service service_name > credit-control
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-dcca)#
```

**Syntax**

```
diameter mscc-per-ccr-update { multiple | single }
```

**Usage**

Use this command to configure sending single/multiple Multiple-Services-Credit-Control AVP in CCR-U messages.

**Example**

The following command configures sending a single Multiple-Services-Credit-Control AVP in CCR-U messages:

```
diameter mscc-per-ccr-update single
```
diameter origin host

This command is obsolete. See the diameter origin endpoint command.
diameter origin endpoint

This command configures the Diameter Credit Control Origin Endpoint.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > ACS Configuration > Credit Control Configuration

active-charging service service_name > credit-control

Entering the above command sequence results in the following prompt:

[local]host_name(config-dcca)#

**Syntax**

```plaintext
diameter origin endpoint  endpoint_name  [ realm  realm_name  ]

no diameter origin endpoint
```

**no diameter origin endpoint**

- **no**
  - Removes the Diameter Credit Control Origin Endpoint configuration.

**endpoint  endpoint_name**

- Specifies the Diameter Credit Control Origin Endpoint name as an alphanumeric string of 1 through 63 characters.

**realm  realm_name**

- Specifies the Diameter Credit Control Realm ID as an alphanumeric string of 1 through 127 characters.

**Usage**

Use this command to configure the Diameter Credit Control Origin Endpoint. The endpoint to configure should be pre-configured. For information on creating and configuring a Diameter endpoint, see the `diameter endpoint` command in the Context Configuration mode.

**Example**

The following command configures a Diameter Credit Control Origin Endpoint named `test`:

```plaintext
diameter origin endpoint test
```
diameter peer-select

This command configures the Diameter credit control primary and secondary hosts for DCCA.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Credit Control Configuration

active-charging service service_name > credit-control

Entering the above command sequence results in the following prompt:

[local]host_name(config-dcca)#

Syntax

In 8.x and earlier releases:

diameter peer-select peer peer_name [ realm realm_name ] [ secondary-peer secondary_peer_name [ realm realm_name ] ] [ imsi-based start-value imsi_start_value end-value imsi_end_value ]

no diameter peer-select [ imsi-based start-value imsi_start_value end-value imsi_end_value ]

In 9.0 and later releases, for UMTS deployments:

diameter peer-select peer peer_name [ realm realm_name ] [ secondary-peer secondary_peer_name [ realm realm_name ] ] [ imsi-based { { prefix | suffix } imsi/prefix/suffix_start_value } [ to imsi/prefix/suffix_end_value ] ] [ msisdn-based { { prefix | suffix } msisdn-based/prefix/suffix_start_value } [ to msisdn-based/prefix/suffix_end_value ] ]

no diameter peer-select [ { prefix | suffix } imsi/prefix/suffix_start_value ] [ to imsi/prefix/suffix_end_value ] | [ msisdn-based { { prefix | suffix } msisdn-based/prefix/suffix_start_value } [ to msisdn-based/prefix/suffix_end_value ] ]

no

Removes previously configured Diameter credit control peer selection setting.

peer peer_name

Specifies the primary host name, as an alphanumeric string of 1 through 63 characters that can contain punctuation characters.

imsi-based start-value imsi_start_value end-value imsi_end_value

Important: This section applies only to 8.3 and earlier releases.
diameter peer-select

Specifies peer selection based on International Mobile Subscriber Identification (IMSI) range.

start-value imsi_start_value specifies the start of range in integer value of IMSI, and end-value
imsi_end_value specifies the end of range in integer value of IMSI.

imsi-based { { prefix | suffix } imsi/prefix/suffix_start_value } [ to
imsi/prefix/suffix_end_value ]

Important: This section applies only to 9.0 and later releases for UMTS deployments.

Selects peer based on IMSI prefix or suffix or IMSI range.

prefix: Specifies the prefix range
suffix: Specifies the suffix range

imsi/prefix/suffix_start_value: Specifies the IMSI/prefix/suffix start value. prefix/suffix must be an IMSI prefix/suffix, and must be an integer from 1 through 15 characters.
imsi/prefix/suffix_end_value: Specifies the IMSI/prefix/suffix end value. prefix/suffix must be an IMSI prefix/suffix, and must be an integer from 1 through 15 characters that must be greater than the start value.

Important: If prefix/suffix is used, the lengths of both start and end prefix/suffix must be equal. If the prefix or suffix keyword is not specified, it will be considered as suffix.

msisdn-based { { prefix | suffix } msisdn/prefix/suffix_start_value } [ to
msisdn/prefix/suffix_end_value ]

Specifies peer selection based on MSISDN prefix or suffix or MSISDN range.

prefix: Specifies the prefix range
suffix: Specifies the suffix range

msisdn/prefix/suffix_start_value: Specifies the MSISDN/prefix/suffix start value. prefix/suffix must be an MSISDN prefix/suffix, and must be an integer from 1 through 15 characters.
msisdn/prefix/suffix_end_value: Specifies the MSISDN/prefix/suffix end value. prefix/suffix must be an MSISDN prefix/suffix, and must be an integer from 1 through 15 characters that must be greater than the start value.

realm realm_name

The realm_name must be an alphanumeric string of 1 through 127 characters, and can contain punctuation characters. The realm may typically be a company or service name.

secondary-peer secondary_peer_name

Specifies a name for the secondary host to be used for failover processing. When the route-table does not find an AVAILABLE route, the secondary host performs a failover processing if the diameter session failover command is set.

secondary_peer_name must be an alphanumeric string of 1 through 63 characters, and can contain punctuation characters.

Usage

Use this command to configure Diameter credit control host selection.
If the `diameter peer-select` command is not configured, and if multiple peers are configured in the endpoint, the available peers configured in the endpoint are automatically chosen in a load-balanced round-robin manner.

9.0 and later releases support peer selection using prefix or suffix of IMSI or IMSI range. Subscribers are now assigned to a primary OCS instance based on the value of the IMSI prefix or suffix of a length of 1 to 15 digits. If the prefix or suffix keyword is not specified, it will be considered as suffix. Up to 64 peer selects can be configured. At a time either prefix or suffix mode can be used in one DCCA config. If prefix or suffix mode is used, the lengths of all prefix/suffix must be equal.

In 12.2 and later releases, Diameter peer selection can also be performed based on the configurable prefix or suffix of MSISDN or MSISDN range.

Each primary OCS may have a designated secondary OCS in case of failure of the primary. It will be the responsibility of the GGSN to use the appropriate secondary OCS in case of primary failure. The secondary OCS for each primary OCS will be one of the existing set of OCSs.

**Example**

The following command configures a Diameter credit control peer named `test` and the realm `companyx`:

```
diameter peer-select peer test realm companyx
```

The following command configures IMSI-based Diameter credit control peer selection in the IMSI range of 1234567890 to 1234567899:

```
diameter peer-select peer star imsi-based start-value 1234567890 end-value 1234567899
```

The following command configures IMSI-based DCCA peer selection with IMSI suffix of 100 through 200:

```
diameter peer-select peer test_peer realm test_realm secondary-peer test_sec_realm realm test_realm2 imsi-based suffix 100 to 200
```
**diameter pending-timeout**

This command configures the maximum time period to wait for response from a Diameter peer.

**Product**  
All

**Privilege**  
Security Administrator, Administrator

**Mode**  
Exec > ACS Configuration > Credit Control Configuration

`active-charging service service_name > credit-control`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-dcca)#
```

**Syntax**

```
diameter pending-timeout duration

default diameter pending-timeout
```

**default**

Disables DCCA resending message at pending-timeout.

**duration**

Specifies the timeout duration (in seconds). The value must be an integer from 1 through 300.

**after-expiry-try-secondary-host**

This keyword is deprecated. This can now be managed using the `retry-after-tx-expiry` and `go-offline-after-tx-expiry` keywords in the `failure-handling` command.

**Usage**

Use this command to set the maximum time for Diameter credit control to receive a response from its peer. DCCA refers to this as the Tx Timer. Typically, this should be configured to a value smaller than the response-timeout value of Diameter Endpoint Configuration Mode. That value is typically too large for DCCA's purposes.

If DCCA gets a "no available routes" error before pending-timeout expires, then DCCA tries to send to the secondary host (if one has been configured). If DCCA gets no response and pending-timeout expires, then DCCA either tries the secondary host or gives up. This can now be managed using the `failure-handling` command.

If routing has failed, i.e., the attempt to the primary host, as well as, the attempt to the secondary host (if that has been configured), then the processing configured by the `failure-handling` command is performed. The routing (i.e., returning a good response, no response or an error response such as "no available routes") is controlled by Diameter Endpoint Configuration Mode. That uses a watchdog timer (called Tw Timer) to attempt a different route to a host. Multiple routes could be attempted. If there's no response before the endpoint's configured response-timeout expires, then "no available routes" is the routing result. The routing
logic remembers the status of routes, so it can return "no available routes" immediately, without using any timers. The default case will disable DCCA resending message at Tx (pending-timeout). So messages are retried only at Tw (device watchdog timeout) by diabase or at response-timeout by DCCA.

Example

The following command configures a Diameter Credit Control Pending Timeout setting of 20 seconds:

```plaintext
diameter pending-timeout 20
```
**diameter reauth-blacklisted-content**

This command allows reauthorization of blacklisted content (blacklisted with Result-Code like 4012, 4010, etc) when a Rating Group (RG) based Re-Authorization Request (RAR) or generic RAR is received.

**Product**
- GGSN
- HA
- IPSG
- PDSN
- P-GW
- SAEGW

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > ACS Configuration > Credit Control Configuration

```bash
active-charging service service_name > credit-control
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-dccca)#
```

**Syntax**

```bash
diameter reauth-blacklisted-content [ content-based-rar ]

no diameter reauth-blacklisted-content
```

- **no**
  Configures this command with the default setting. That means, the reauthorization of blacklisted RG will not happen.

- **content-based-rar**
  Reauthorizes blacklisted RG only when RG specific RAR is received.

**Usage**

The current Gy implementation does not allow reauthorization of Blacklisted content (blacklisted with Result-Code like 4012, 4010, etc) when Gy receives an RAR (either a RG based RAR or generic RAR). With this CLI based enhancement, it is possible to perform one of the following actions:

- to reauthorize blacklisted RG only when RG specific RAR is received.
- to reauthorize blacklisted RG on any kind of RAR (both RG specific or generic)
- do not reauthorize blacklisted RG (default implementation).

This feature determines if the RAR received from OCS is generic or to any specific rating-group.
If it is a generic RAR:

- If this CLI command “diameter reauth-blacklisted-content” is configured, then reauthorize all the Rating-Groups (RGs) which are blacklisted. CCR-U forced-reauthorization will be triggered all the RGs.

- If this CLI command “diameter reauth-blacklisted-content content-based-rar” is configured, then RG which are blacklisted will not be reauthorized. CCR-U forced-reauthorization will be triggered only for active RGs alone.

If Rating-Group information is received in RAR:

- If either “diameter reauth-blacklisted-content” or “diameter reauth-blacklisted-content content-based-rar” is configured, then RG gets re-authorized even it is blacklisted. CCR-U forced-reauthorization will be triggered for the received RG.

If this CLI command is not configured, then the default behavior which is not to reauthorize blacklisted RG persists.

**Example**

The following command enables reauthorization of blacklisted content on receiving RG specific RAR:

```
diameter reauth-blacklisted-content [ content-based-rar ]
```
**diameter redirect-url-token**

This command allows configuring a token to be used for appending original URL to the redirect address.

**Important:** This command is customer specific. For more information contact your Cisco account representative.

**Product**
- GGSN
- HA
- IPSG
- PDSN
- P-GW
- SAEGW

**Privilege**
Security Administrator, Administrator

**Mode**
- Exec > ACS Configuration > Credit Control Configuration

active-charging service service_name > credit-control

Entering the above command sequence results in the following prompt:

[local]host_name(config-dcca)#

**Syntax**

```
diameter redirect-url-token string
default diameter redirect-url-token
```

**default diameter redirect-url-token**

- **default**
  Configures this command with the default setting.

- **string**
  The redirect url token name must be an alphanumeric string of size 1 through 63 characters.

**Usage**

The chassis should perform dynamic Advice of Charge (AoC) redirections (URL provided by Online Charging System (OCS)) for a particular Service ID/Rating Group combination without affecting the flows mapped to other Service ID/Rating Group combinations. Redirections can be removed by OCS for a particular MSCC (Service ID/Rating Group combination) using a RAR message containing a specific Service ID/Rating Group combination.

As part of redirection to an AoC or Top-UP server (302 Moved HTTP message) the PCEF should be able to append the original HTTP URL to the redirected session. This way, once the subscriber has successfully been redirected (and potentially topped up their prepaid account) they can be presented with an option to be redirected back to their original URL. The OCS can indicate to the PCEF if the original URL is to be
appended to the redirection by specifying a special character to the end of the AoC redirection — for example, a "?" character.

Upon final unit indication a redirect server address will be returned together with the FUI.

On redirection, the redirect URL will be appended with the original URL information using the token name configured with the `diameter redirect-url-token` command so that on completion of AoC, the AoC server may redirect the client back to the original location.

The rules for appending the original URL before redirection are as follows:

1. The “?” character at the end of the AoC page provided by the OCS in the redirect URL will be replaced with the “&” character.
2. A configurable parameter will be appended after the “&” character. The parameter whose name will be defined in a command line in the chassis configuration. The parameter name is case sensitive.
3. An “=” will be appended to the parameter.
4. The subscriber's original URL will be appended to the “=” character.

For example:
When the original URL was `http://homepage/
OCS provided URL:
The text in bold in the following sample indicates the current configuration for implementing the dynamic AoC redirection.

**Example**

The following command configures the redirect-url-token as `returnUrl`:

```
diameter redirect-url-token returnUrl
```
diameter result-code

This command enables sending a GTP Create-PDP-Context-Rsp message with cause code based on the DCCA result code.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Credit Control Configuration

```bash
active-charging service service_name > credit-control
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-dcca) #
```

Syntax

```bash
diameter result-code { authorization-rejected | credit-limit-reached | end-user-service-denied | user-unknown } use-gtp-cause-code { authentication-failure | no-resource-available | system-failure }

default diameter result-code { authorization-rejected | credit-limit-reached | end-user-service-denied | user-unknown } use-gtp-cause-code
```

- **default**
  Configures this command with the default setting.
  In 12.1 and earlier releases: `no-resource-available`
  In 12.2 and later releases: `system-failure`

- **authorization-rejected**
  Result code received as DIAMETER_AUTHORIZATION_REJECTED(5003).

- **credit-limit-reached**
  Result code received as DIAMETER_CREDIT_LIMIT_REACHED(4012).

- **end-user-service-denied**
  Result code received as DIAMETER_END_USER_DENIED(4010).

- **user-unknown**
  Result code received as DIAMETER_USER_UNKNOWN(5030).

- **use-gtp-cause-code**
  Cause code to be sent in GTP response.
**authentication-failure**

Sends the GTP cause code GTP_USER_AUTHENTICATION_FAILED in GTP response.

**no-resource-available**

Sends the GTP cause code GTP_NO_RESOURCES_AVAILABLE in GTP response.

**system-failure**

Sends the GTP cause code GTP_SYSTEM_FAILURE in GTP response.

---

**Usage**

On receiving result-code as AUTHORIZATION-REJECTED, CREDIT_LIMIT_REACHED, END_USER_DENIED or USER_UNKNOWN from DCCA server, based on this CLI configuration, in GTP Create-PDP-Context Response message the cause code can either be sent as GTP_NO_RESOURCE_AVAILABLE or GTP_AUTHENTICATION_FAILED or GTP_SYSTEM_FAILURE.

**Example**

The following command sets the deny cause as user authentication failure when the CCA-Initial has the result code DIAMETER_AUTHORIZATION_REJECTED(5003):

```
diameter result-code authorization-rejected use-gtp-cause-code authentication-failure
```
diameter send-ccri

This command configures when to send an initial Credit Control Request (CCR-I) for the subscriber session.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Credit Control Configuration

active-charging service service_name > credit-control

Entering the above command sequence results in the following prompt:

[local]host_name(config-dcca)#

Syntax

diameter send-ccri { session-start | traffic-start }

default diameter send-ccri

- default
  
  Configures this command with the default setting.
  Default: session-start

- session-start
  
  Sends CCR-I when the PDP context is being established (on receiving Create-PDP-Context-Request).

- traffic-start
  
  Delays sending CCR-I until the first data packet is received from the subscriber.

**Important:** Please note that the CCR-I will be sent only with the default rulebase and not with Rulebase list even if the rulebase-list configuration is enabled. When the rulebase-list command is used in conjunction with diameter send-ccri traffic-start command, the former one's function is invalidated. The rulebase-list is used to allow the OCS to select one of the rulebases from the list configured during the session setup. But in case of send-ccri traffic-start the CLI causes the session setup to complete without OCS interaction. For more information on rulebase-list command, please see the ACS Configuration Mode Commands chapter of the Command Line Interface Reference.

Usage

Use this command to configure when to send CCR-Initial for the subscriber session.

Example

The following command configures to send CCR-I on traffic detection and not on context creation:

```
diameter send-ccri traffic-start
```
**diameter service-context-id**

This command configures the value to be sent in the Service-Context-Id AVP, which identifies the context in which DCCA is used.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > ACS Configuration > Credit Control Configuration

```
active-charging service service_name > credit-control
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-dcca)#
```

**Syntax**

```
diameter service-context-id service_context_id

default diameter service-context-id
```

**default diameter service-context-id**

- **default**
  
  Configures this command with the default setting. Currently, the default value is encoded based on the dictionary wherever applicable; when not applicable, it is not encoded.

- **service_context_id**
  
  Specifies the service context as an alphanumeric string of 1 through 63 characters that can contain punctuation characters.

**Usage**

If Service-Context-Id is applicable and configured using this command, it will be sent in the AVP Service-Context-Id in the Diameter CCR message.

**Example**

The following command specifies the value `version@customer.com` to be sent in the Service-Context-Id AVP in the Diameter CCR message:

```
diameter service-context-id version@customer.com
```
diameter session failover

This command enables/disables Diameter Credit Control Session Failover. When enabled, the secondary peer is used in the event the main peer is unreachable.

**Product**
- GGSN
- HA
- IPSG
- PDSN
- P-GW

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > ACS Configuration > Credit Control Configuration

```plaintext
active-charging service service_name > credit-control
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-dcca)#
```

**Syntax**

```
[ default | no ] diameter session failover
```

- **default**
  - Configures this command with the default setting.
  - Default: Depends on the failure-handling configuration

- **no**
  - If the primary server is not reachable, failover is not triggered and the session is torn down. No failover action is taken.

**Usage**

Use this command to enable/disable Diameter Credit Control Session Failover. The failure-handling configuration comes into effect only if `diameter session failover` is present in the configuration. The failover can be overridden by the server in the response message, and it takes precedence.

**Example**

The following command enables Diameter Credit Control Session Failover:

```
diameter session failover
```
diameter update-dictionary-avps

This command enables dictionary control of the AVPs that need to be added based on the version of the specification with which the Online Charging System (OCS) is compliant. This command is applicable to all products that use the dcca-custom8 dictionary for Gy interface implementation.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Credit Control Configuration

active-charging service service_name > credit-control

Entering the above command sequence results in the following prompt:

[local]host_name(config-dcca)#

Syntax

diameter update-dictionary-avps { 3gpp-rel8 | 3gpp-rel9  }

[ default | no ] diameter update-dictionary-avps

<table>
<thead>
<tr>
<th>default</th>
<th>no</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configures this command with the default setting.</td>
<td></td>
</tr>
<tr>
<td>Default: Compliant with the oldest release (Rel. 7) and send only Rel. 7 AVPs</td>
<td></td>
</tr>
</tbody>
</table>

3gpp-rel8

Select the 3GPP Rel. 8 AVPs for encoding.

3gpp-rel9

Selects the 3GPP Rel. 9 AVPs for encoding.

Usage

⚠️ Important: This command is applicable ONLY to the dcca-custom8 dictionary. If, for any dictionary other than dcca-custom8, this command is configured with a value other than the default, configuration errors will be indicated in the output of the show configuration errors section active-charging command.

Use this command to encode the AVPs in the dictionary based on the release version of the specification to which the OCS is compliant with.

Example

The following command enables encoding of AVPs in the dictionary based on 3GPP Rel. 9:

diameter update-dictionary-avps 3gpp-rel9
end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

der

Usage

Use this command to return to the Exec mode.
event-based-session

This command configures the parameters for event-based Gy session.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Credit Control Configuration

`active-charging service service_name > credit-control`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-dcca)#
```

Syntax

```
[ no ] event-based-session trigger type { location-any | mcc | mnc | timezone } +
```

default event-based-session trigger type

```
default
Configs this command with the default setting.
Default: No triggers.
```

```
no
Removes the previously configured trigger type.
```

```
location-any
Sets the trigger based on change in user location.
```

```
mcc
Sets the trigger based on change in Mobile Country Code (MCC) of the serving node (for e.g. SGSN, S-GW).
```

```
mnc
Sets the trigger based on change in Mobile Network Code (MNC) of the serving node (for e.g. SGSN, S-GW).
```

```
timezone
Sets the trigger based on change in the timezone of UE.
```

```
+
Indicates that more than one of the previous keywords can be entered within a single command.
```
**Usage**

Use this command to enable the credit control reauthorization triggers for event-based-session in the credit-control group.

**Example**

The following command selects a credit control trigger as mcc:

```
event-based-session trigger type mcc
```
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Use this command to return to the parent configuration mode.
failure-handling

This command configures Diameter Credit Control Failure Handling (CCFH) behavior in the event of communication failure with the prepaid server or on reception of specific error codes from prepaid server.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Credit Control Configuration

active-charging service service_name > credit-control

Entering the above command sequence results in the following prompt:

[local]host_name(config-dcca)#

Syntax


default failure-handling [ initial-request | terminate-request | update-request ]

default failure-handling [ initial-request | terminate-request | update-request ]

Configures the default CCFH setting.

initial-request: The default setting is terminate.
update-request: The default setting is retry-and-terminate.
terminate-request: The default setting is retry-and-terminate.

initial-request

Specifies the message type as CCR-Initial.

terminate-request

Specifies the message type as CCR-Terminate.

update-request

Specifies the message type as CCR-Update.

continue

Specifies the CCFH setting as continue. The online session is converted into an offline session. The associated PDP Context is established (new sessions) or not released (ongoing sessions).
### retry-and-terminate

Specifies the CCFH setting as retry-and-terminate. The user session will continue for the duration of one retry attempt with the prepaid server. If there is no response from both primary and secondary servers, the session is torn down.

### terminate

Specifies the CCFH setting as terminate. All type of sessions (initial or update) are terminated in case of failure.

### go-offline-after-tx-expiry

Starts offline charging after Tx expiry.

### retry-after-tx-expiry

Retries after Tx expiry. Enables secondary-host, if up, to take over after Tx expiry.

### Usage

Use this command to select the CCFH behavior. The specified behavior is used for sessions when no behavior is specified by the prepaid server. By default, the CCFH is taken care at response-timeout except for terminate setting.

If the Credit-Control-Failure-Handling AVP is received from the server, the received setting will be applied to all the message types.

The following table indicates the CCFH behavior for the combination of different CCFH settings, and the corresponding CLI commands.

<table>
<thead>
<tr>
<th>CCFH Setting</th>
<th>CLI Command</th>
<th>Behavior at Tx</th>
<th>Behavior at RT</th>
<th>Secondary is Up</th>
<th>Secondary is Down</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Initial-request Message Type</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Continue</td>
<td>initial-request continue</td>
<td>N/A</td>
<td>Continue</td>
<td>Secondary takes over after RT</td>
<td>Offline after another RT. No more quota requests are performed for any rating group within the session after DCCA failure (even if connectivity to DCCA is restored)</td>
</tr>
<tr>
<td></td>
<td>initial-request continue go-offline-after-tx-expiry</td>
<td>Offline</td>
<td>N/A</td>
<td>Offline at Tx</td>
<td>Offline at Tx</td>
</tr>
<tr>
<td></td>
<td>initial-request continue retry-after-tx-expiry</td>
<td>Continue</td>
<td>N/A</td>
<td>Secondary takes over after Tx</td>
<td>Offline after another Tx</td>
</tr>
<tr>
<td>Retry-and-terminate</td>
<td>initial-request retry-and-terminate</td>
<td>N/A</td>
<td>Retry</td>
<td>Secondary takes over after RT</td>
<td>Terminate after another RT</td>
</tr>
<tr>
<td></td>
<td>initial-request retry-and-terminate retry-after-tx-expiry</td>
<td>Retry</td>
<td>N/A</td>
<td>Secondary takes over after Tx</td>
<td>Terminate after another Tx</td>
</tr>
</tbody>
</table>
### Credit Control Configuration Mode Commands

**Failure-handling**

<table>
<thead>
<tr>
<th>CCFH Setting</th>
<th>CLI Command</th>
<th>Behavior at Tx</th>
<th>Behavior at RT</th>
<th>Secondary is Up</th>
<th>Secondary is Down</th>
</tr>
</thead>
<tbody>
<tr>
<td>Terminate</td>
<td>initial-request terminate</td>
<td>Terminate</td>
<td>N/A</td>
<td>Terminate after Tx</td>
<td>Terminate after Tx</td>
</tr>
</tbody>
</table>

**Update-request Message Type**

<table>
<thead>
<tr>
<th>Continue</th>
<th>update-request continue</th>
<th>N/A</th>
<th>Continue</th>
<th>Secondary takes over after RT</th>
<th>Offline after another RT</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>update-request continue go-offline-after-tx-expiry</td>
<td>Offline</td>
<td>N/A</td>
<td>Offline at Tx</td>
<td>Offline at Tx</td>
</tr>
<tr>
<td></td>
<td>update-request continue retry-after-tx-expiry</td>
<td>Continue</td>
<td>N/A</td>
<td>Secondary takes over after Tx</td>
<td>Offline after another Tx</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Retry-and-terminate</th>
<th>update-request retry-and-terminate</th>
<th>N/A</th>
<th>Retry</th>
<th>Secondary takes over after RT</th>
<th>Sends CCR-T after another RT</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>update-request retry-and-terminate retry-after-tx-expiry</td>
<td>Retry</td>
<td>N/A</td>
<td>Secondary takes over after Tx</td>
<td>Sends CCR-T after another Tx</td>
</tr>
</tbody>
</table>

**Terminate-request Message Type**

<table>
<thead>
<tr>
<th>Continue</th>
<th>terminate-request continue</th>
<th>N/A</th>
<th>Retry</th>
<th>CCR-T is sent to secondary after RT</th>
<th>Terminate after another RT</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>terminate-request continue go-offline-after-tx-expiry</td>
<td>Retry</td>
<td>N/A</td>
<td>CCR-T is sent to secondary after Tx</td>
<td>Terminate after another Tx</td>
</tr>
<tr>
<td></td>
<td>terminate-request continue retry-after-tx-expiry</td>
<td>Retry</td>
<td>N/A</td>
<td>CCR-T is sent to secondary after Tx</td>
<td>Terminate after another Tx</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Retry-and-terminate</th>
<th>terminate-request retry-and-terminate</th>
<th>N/A</th>
<th>Retry</th>
<th>CCR-T is sent to secondary after RT</th>
<th>Terminate after another RT</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>terminate-request retry-and-terminate retry-after-tx-expiry</td>
<td>Retry</td>
<td>N/A</td>
<td>CCR-T is sent to secondary after Tx</td>
<td>Terminate after another Tx</td>
</tr>
</tbody>
</table>

**Example**

<table>
<thead>
<tr>
<th>Terminate</th>
<th>terminate-request terminate</th>
<th>Terminate</th>
<th>N/A</th>
<th>Terminate after Tx</th>
<th>Terminate after Tx</th>
</tr>
</thead>
</table>

---

Cisco ASR 5x00 Command Line Interface Reference

2670
The following command sets the Credit Control Failure Handling behavior for initial request message type to **retry-and-terminate**:

```
failure-handling initial-request retry-and-terminate
```
imsi-imeisv-encode-format

This command configures the encoding format of IMSI/IMEISV in the User-Equipment-Info, 3GPP-IMSI and 3GPP-IMEISV AVPs.

Product
- GGSN
- HA
- IPSG
- PDSN
- P-GW

Privilege
- Security Administrator, Administrator

Mode
- Exec > ACS Configuration > Credit Control Configuration
- active-charging service service_name > credit-control

Entering the above command sequence results in the following prompt:

[local]host_name(config-dcca)#

Syntax

[ default | no ] imsi-imeisv-encode-format { ascii | tbc }d

- ascii
  Sends IMSI/IMEISV as an octet string in ASCII encoded format. By default, the IMSI/IMEISV will be encoded in ASCII format.

- tbc
  Sends IMSI/IMEISV as an octet string in Telephony Binary Coded Decimal (TBCD) format, i.e. the nibbles in an octet are inter-changed.

Usage

Use this command to configure the encoding format of IMSI/IMEISV in User-Equipment-Info, 3GPP-IMSI and 3GPP-IMEISV AVPs.

Example

The following command specifies the encoding format of IMSI/IMEISV as ASCII:

imsi-imeisv-encode-format ascii
mode

This command configures the Prepaid Credit Control mode to RADIUS or Diameter.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Credit Control Configuration

active-charging service service_name > credit-control

Entering the above command sequence results in the following prompt:

[local]host_name(config-dcca)#

Syntax

mode { diameter | radius }

default mode

---

default
Configures the default prepaid credit control mode.
Default: diameter

---

diameter
Enables Diameter Credit Control Application (DCCA) for prepaid charging.

---

radius
Enables RADIUS Credit Control for prepaid charging.

Usage
Use this command to configure the prepaid charging application mode to Diameter or RADIUS credit control.

Example
The following command specifies to use RADIUS prepaid credit control application:

mode radius
pending-traffic-treatment

This command controls the pass/drop treatment of traffic while waiting for definitive credit information from the server.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Credit Control Configuration

```
active-charging service service_name > credit-control
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-dcca)#
```

**Syntax**

```
pending-traffic-treatment { { { forced-reauth | trigger | validity-expired } drop | pass } } | { noquota { buffer | drop | limited-pass volume | pass } } | { quota-exhausted { buffer | drop | pass } } }

default pending-traffic-treatment { forced-reauth | noquota | quota-exhausted | trigger | validity-expired }
```

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Configures this command with the default setting.</td>
</tr>
<tr>
<td></td>
<td>Default: drop</td>
</tr>
<tr>
<td>forced-reauth</td>
<td>Sets the Diameter credit control pending traffic treatment to forced reauthorization.</td>
</tr>
<tr>
<td>trigger</td>
<td>Sets the Diameter credit control pending traffic treatment to trigger.</td>
</tr>
<tr>
<td>validity-expired</td>
<td>Sets the Diameter credit control pending traffic treatment to validity expired.</td>
</tr>
<tr>
<td>noquota</td>
<td>Sets the Diameter credit control pending traffic treatment to no quota.</td>
</tr>
<tr>
<td>quota-exhausted</td>
<td>Sets the Diameter credit control pending traffic treatment to quota exhausted.</td>
</tr>
</tbody>
</table>
buffer

Specifies to tentatively count/time traffic, and then buffer traffic pending arrival of quota. Buffered traffic will be forwarded and fully charged against the quota when the quota is eventually obtained and the traffic is passed.

drop

Drops any traffic when there is no quota present.

limited-pass volume

Enables limited access for subscribers when the OCS is unreachable. 

`volume` specifies the Default Quota size (in bytes) and must be an integer from 1 through 4294967295. This feature allows the subscriber to use the network when the OCS response is slow. This configuration enables to set a Default Quota size from which the subscriber can consume quota until response from the OCS arrives. The traffic consumed by the subscriber from the Default Quota at the beginning of the session is reported and counted against the quota assigned from the OCS.

**Important:** Default Quota is used only for `noquota` case (Rating Group (RG) seeking quota for the first time) and not for `quota-exhausted`. Default Quota is not used for subsequent credit requests.

If the Default Quota is NOT exhausted before the OCS responds with quota, traffic is allowed to pass. Initial Default Quota usage is counted against initial quota allocated. If quota allocated is less than the actual usage, the actual usage and request additional quota are reported. If no additional quota is available, the traffic is denied.

If the Default Quota is NOT exhausted before the OCS responds with denial of quota, traffic is blocked after the OCS response. The gateway will report usage on Default Quota even in for CCR-U (FINAL) or CCR-T until the OCS responds.

If the Default Quota is exhausted before the OCS responds, the session is dropped.

The default pending-traffic-treatment for `noquota` is drop. The default `pending-traffic-treatment noquota` command removes any Default Quota limit configured.

pass

Passes all traffic more or less regardless of quota state.

Usage

Use this command to set the Diameter credit control pending traffic treatment while waiting for definitive credit information from the server.

This CLI command is different than the `failure-handling` command, which specifies behavior in the case of an actual timeout or error, as opposed to the behavior while waiting. See also the `buffering-limit` command in the Active Charging Service Configuration Mode.

Example

The following command sets the Diameter credit control pending traffic treatment to drop any traffic when there is no quota present:

```
pending-traffic-treatment noquota drop
```
quota

This command sets various time-based quotas in the prepaid credit control service.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Credit Control Configuration

active-charging service service_name > credit-control

Entering the above command sequence results in the following prompt:

[local]host_name(config-dcca)#

Syntax

quota holding_time | validity-time validity_time }

{ default | no } quota { holding-time | validity-time }

holding-time holding_time

Specifies the Quota Holding Time (QHT) in seconds. The value must be an integer from 1 through 4000000000.

validity-time validity_time

Specifies the validity lifetime of the quota, in seconds. The value must be an integer from 1 through 4000000.

Usage
Use this command to set the prepaid credit control quotas.

Example
The following command sets the prepaid credit control request holding time to 30000 seconds:

quota holding-time 30000
**quota request-trigger**

This command configures the action on the packet that triggers the credit control application to request quota.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Credit Control Configuration

```
active-charging service service_name > credit-control
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-dcca)#
```

**Syntax**

```
quota request-trigger { exclude-packet-causing-trigger | include-packet-causing-trigger }
{ default | no } quota request-trigger

default quota request-trigger
```

**Important:** In 10.0 and later releases, this keyword is deprecated.

```
exclude-packet-causing-trigger
```

Excludes the packet causing threshold limit violation trigger.

```
include-packet-causing-trigger
```

Includes the packet causing the threshold limit violation trigger.

**Usage**

Use this command to configure action on the packet that triggers the credit control application to request quota, whether the packet should be excluded/included in the utilization information within the quota request.

**Example**

The following command sets the system to exclude the packets causing threshold limit triggers from accounting of prepaid credit of a subscriber:

```
quota request-trigger exclude-packet-causing-trigger
```
**quota time-threshold**

This command configures the time threshold limit for subscriber quota in the prepaid credit control service.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Credit Control Configuration

Example:

```
active-charging service service_name > credit-control
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-dcca)#
```

**Syntax**

```
quota time-threshold { abs_time_value | percent percent_value } 
{ default | no } quota time-threshold
```

- **default**
  Configures this command with the default setting.
  Default: Disabled

- **no**
  Disables time threshold for prepaid credit control quota.

- **abs_time_value**
  Specifies the absolute threshold time (in seconds) for configured time quota in prepaid credit control charging. abs_time_value must be an integer from 1 through 86400. To disable this assign 0. Default: 0 (Disabled)

- **percent_value**
  Specifies the time threshold value as a percentage of the configured time quota in DCCA. percent_value must be an integer from 1 through 100.

**Usage**

Use this command to set the time threshold for prepaid credit control quotas.

**Example**

The following command sets the prepaid credit control time threshold to 400 seconds:

```
quota time-threshold 400
```
quota units-threshold

This command sets the unit threshold limit for subscriber quota in the prepaid credit control service.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Credit Control Configuration

active-charging service service_name > credit-control

Entering the above command sequence results in the following prompt:

[local]host_name(config-dcca)#

Syntax

quota unit-threshold { abs_unit_value | percent percent_value }

{ default | no } quota units-threshold

default

Configures this command with the default setting.
Default: Disabled

no

Disables unit threshold for DCCA quota.

abs_unit_value

Specifies the absolute threshold value (in units) for the configured units quota in prepaid credit control application. abs_unit_value must be an integer from 1 through 400000000. To disable this assign 0.
Default: 0 (Disabled)

percent_value

Specifies the time threshold value as a percentage of the configured units quota in DCCA. percent_value must be an integer from 1 through 100.

Usage

Use this command to set the units threshold for prepaid credit control quotas.

Example

The following command sets the prepaid credit control time threshold to 160400 units:

    quota units-threshold 160400
quota volume-threshold

This command sets the volume threshold limit for subscriber quota in the prepaid credit control service.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Credit Control Configuration

active-charging service service_name > credit-control

Entering the above command sequence results in the following prompt:

[local]host_name(config-dca)#

Syntax

```plaintext
quota volume-threshold { abs_vol_value | percent percent_value }

{ default | no } quota volume-threshold
```

- `default`
  Configures this command with the default setting.
  Default: Disabled

- `no`
  Disables volume threshold for prepaid credit control quota.

- `abs_vol_value`
  Specifies the absolute threshold volume (in bytes) to the configured volume quota in prepaid credit control.
  `abs_vol_value` must be an integer from 1 through 400000000. To disable this assign 0. Default: 0 (Disabled)
  If configured, the Credit Control client will seek re-authorization from the server for the quota when the quota contents fall below the specified threshold.

- `percent percent_value`
  Specifies the volume threshold value as a percentage of the configured volume quota in prepaid credit control.
  `percent_value` must be an integer from 1 through 100.

Usage
Use this command to set the volume threshold for prepaid credit control quotas.

Example
The following command sets the prepaid credit control volume threshold to \textit{160400} bytes:

```plaintext
quota volume-threshold 160400
```
radius usage-reporting-algorithm

This command configures the usage reporting algorithm for RADIUS prepaid using the Diameter Credit-Control Application (DCCA).

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Credit Control Configuration

active-charging service service_name > credit-control

Entering the above command sequence results in the following prompt:

[local]host_name(config-dcca)#

Syntax

radius usage-reporting-algorithm { cumulative | relative }

default radius usage-reporting-algorithm

default

Configures this command with the default setting.
Default: cumulative

cumulative

Reports the total accumulated usage of quota in every accounting interim.

relative

Reports the quota usage per accounting interim (since the previous usage report).

Usage

Use this command to configure the usage reporting algorithm for RADIUS prepaid using DCCA.

Example

The following command configures the usage reporting algorithm for RADIUS prepaid using DCCA to relative:

radius usage-reporting-algorithm relative
redirect-indicator-received

This command configures the action on buffered packets when a redirect-indicator is received from the RADIUS server.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Credit Control Configuration

active-charging service service_name > credit-control

Entering the above command sequence results in the following prompt:

[local]host_name(config-dcca)#

Syntax

redirect-indicator-received { discard-buffered-packet | reprocess-buffered-packet }

{ default | no } redirect-indicator-received

default
Configures this command with the default setting. Default: discard-buffered-packet

no
Disables the redirect-indicator-received configuration.

discard-buffered-packet
Discards the buffered packet.

reprocess-buffered-packet
Redirects the buffered packet on receiving a redirect-indicator from the RADIUS server.

Usage
Use this command to configure the action taken on buffered packet when redirect-indicator is received. Diameter can return a redirect URL but not a redirect indicator, however RADIUS can return a redirect indicator. In this situation, any subsequent subscriber traffic would match ruledefs configured with cca redirect-indicator, and charging actions that have flow action redirect-url should be configured. However, some handsets do not retransmit, so there will be no subsequent packets. On configuring reprocess-buffered-packet, the ruledefs are reexamined to find a new charging action, which may have flow action redirect-url configured.

Example
The following command configures the action taken on buffered packet when redirect-indicator is received to reprocess-buffered-packet:

```
redirect-indicator-received reprocess-buffered-packet
```
redirect-require-user-agent

This command conditionally verifies the presence of user-agents in the HTTP header, based on which HTTP URL redirection will be applied.

Product
GGSN
HA
IPSG
PDSN
P-GW
SAEGW

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Credit Control Configuration

active-charging service service_name > credit-control

Entering the above command sequence results in the following prompt:

[local]host_name(config-dcca)#

Syntax

[ no ] redirect-require-user-agent

no

Disables the “user-agent” check in the HTTP header.

Usage

Use this command to conditionally verify the presence of configured user-agents in the HTTP header. The user agent is configured using the redirect user-agent command in the ACS Configuration Mode. The user agent could be, for example, Mozilla, Opera, Google Chrome, etc.

The default configuration is to enable the "user-agent" check, and compare it with the configured list of supported user-agents. The packet will be redirected only when the user-agent is matched with one of the configured user-agents.

If no redirect-require-user-agent is configured, the user-agent check is disabled. The packets will be redirected even if it does not contain a "user-agent" information in the HTTP header.
servers-unreachable

This command configures whether to continue or terminate calls when Diameter server or the OCS becomes unreachable.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Credit Control Configuration

`active-charging service service_name > credit-control`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-dcca)#
```

**Syntax**

In 12.1 and earlier releases:

```
servers-unreachable { initial-request { continue [ after-interim-expiry timeout_period ] } | update-request { continue [ after-quota-expiry | after-timer-expiry timeout_period ] } }
```

```
no servers-unreachable { initial-request | update-request }
```

In 12.2 and later releases:

```
```

```
no servers-unreachable { initial-request | update-request }
```

```
default servers-unreachable behavior-triggers { initial-request | update-request }
```

```
no
```

Deletes the current servers-unreachable configuration.

In 15.0 and later releases, to remove the error result code configuration, the `no` command syntax is `no servers-unreachable behavior-triggers { initial-request | update-request } result-code { any-error | result-code [ to end-result-code ] }`. 
behavior-triggers { initial-request | update-request } { result-code { any-error | result-code [ to end-result-code ] } | transport-failure [ response-timeout | tx-expiry ] }

This keyword is used to determine when to apply server-unreachable action. This supports three configurable options to apply server-unreachable action either at transport failure, Tx expiry or at response timeout. Out of these three options, the transport failure is the default option.

- **initial-request**: Specifies the behavior when Diameter server(s)/OCS become unreachable during initial session establishment.
- **update-request**: Specifies the behavior when Diameter server(s)/OCS become unreachable during mid-session.
- **result-code { any-error | result-code [ to end-result-code ] }**: Specifies to configure any Diameter error result code or a range of result codes to trigger entering server unreachable mode.
  - result-code must be an integer ranging from 3000 to 5999.
- **transport-failure [ response-timeout | tx-expiry ]**: This keyword specifies to trigger the behavior either at transport failure or response timeout OR at Transport failure or Tx expiry.

```plaintext
initial-request { continue | terminate [ after timer expiry timeout_period ] }
```

**Important**: This section applies only to 12.1 and earlier releases.

Specifies behavior when Diameter server(s)/OCS become unreachable during initial session establishment.

- **continue**: Specifies to continue call if Diameter server(s) becomes unreachable.
- **terminate**: Specifies to terminate call if Diameter server(s) becomes unreachable.

  - **after timer expiry timeout_period**: On detecting transport failure, this keyword variable specifies the time limit for which the subscriber session will remain in offline state before the call is terminated.

```plaintext
timeout_period specifies the timeout period, in seconds, and must be an integer from 1 through 4294967295.
```

```plaintext
initial-request { continue { [ [ after-interim-time timeout_period ] [ after-interim-volume quota_value ] } server-retries retry_count ] | terminate { [ [ after-interim-time timeout_period ] [ after-interim-volume quota_value ] } server-retries retry_count ] | after timer expiry timeout_period }
```

**Important**: This section applies only to 12.2 and later releases.

Specifies behavior when Diameter server(s)/OCS become unreachable during initial session establishment.

- **continue**: Specifies to continue call if Diameter server(s) becomes unreachable.
- **terminate**: Specifies to terminate call if Diameter server(s) becomes unreachable.

  - **after-interim-time timeout_period**: Specifies to continue or terminate call after the interim timeout period expires.

  ```plaintext
timeout_period specifies the timeout period, in seconds, and must be an integer from 1 through 4294967295.
  ```
**after-interim-volume** quota_value: Specifies to continue or terminate call on exhaustion of the assigned quota.

quota_value specifies the volume-based quota value, in bytes, and must be an integer from 1 through 4294967295.

The **after-interim-volume** and **after-interim-time** can be configured in one of the following ways:

- **after-interim-volume quota_value server-retries retry_count**
- **after-interim-time timeout_period server-retries retry_count**
- **after-interim-volume quota_value after-interim-time timeout_period server-retries retry_count**
- **after-timer-expiry timeout_period**: On detecting transport failure, this keyword variable specifies the time limit for which the subscriber session will remain in offline state before the call is terminated.

timeout_period specifies the timeout period, in seconds, and must be an integer from 1 through 4294967295.

- **server-retries retry_count**: Specifies the number of retries that should happen to OCS before allowing the session to terminate/offline.

retry_count specifies the retries to OCS, and must be an integer from 0 through 65535. If the value 0 is defined for this keyword, the retry to OCS will not happen instead the configured action will be immediately applied.

```
update-request { continue | terminate [ after-quota-expiry | after-timer-expiry timeout_period ] }
```

**Important**: This section applies only to 12.2 and later releases.

Specifies behavior when Diameter server(s)/OCS become unreachable during mid session.

- **continue**: Specifies to continue call if Diameter server(s) becomes unreachable.
- **terminate**: Specifies to terminate call if Diameter server(s) becomes unreachable.
- **after-quota-expiry**: Specifies to terminate call on exhaustion of all available quota.
- **after-timer-expiry timeout_period**: On detecting transport failure, this keyword variable specifies the time limit for which the subscriber session will remain in offline state before the call is terminated.

timeout_period specifies the timeout period, in seconds, and must be an integer from 1 through 4294967295.

```
update-request { continue [ { [ after-interim-time timeout_period ] [ after-interim-volume quota_value ] } server-retries retry_count ] | terminate [ { { [ after-interim-time timeout_period ] [ after-interim-volume quota_value ] } server-retries retry_count ] [ after-quota-expiry | after-timer-expiry timeout_period ] ] }
```

**Important**: This section applies only to 12.2 and later releases.
Specifies behavior when Diameter server(s)/OCS become unreachable during mid session.

- **continue**: Specifies to continue call if Diameter server(s) becomes unreachable.
- **terminate**: Specifies to terminate call if Diameter server(s) becomes unreachable.

  - **after-interim-time** `timeout_period`**: Specifies to continue or terminate call after the interim timeout period expires.
    
    `timeout_period` specifies the timeout period, in seconds, and must be an integer from 1 through 4294967295.

  - **after-interim-volume** `quota_value`**: Specifies to continue or terminate call on exhaustion of the assigned quota.
    
    `quota_value` specifies the volume-based quota value, in bytes, and must be an integer from 1 through 4294967295.

The **after-interim-volume** and **after-interim-time** can be configured in one of the following ways:

- **after-interim-volume** `quota_value` **server-retries** `retry_count`
- **after-interim-time** `timeout_period` **server-retries** `retry_count`
- **after-interim-volume** `quota_value` **after-interim-time** `timeout_period` **server-retries** `retry_count`

- **after-quota-expiry**: Specifies to terminate call on exhaustion of all available quota.

- **after-timer-expiry** `timeout_period`: On detecting transport failure, this keyword variable specifies the time limit for which the subscriber session will remain in offline state before the call is terminated.

  `timeout_period` specifies the timeout period, in seconds, and must be an integer from 1 through 4294967295.

- **server-retries** `retry_count`: Specifies the number of retries that should happen to OCS before allowing the session to terminate/offline.

  `retry_count` specifies the retries to OCS, and must be an integer from 0 through 65535. If the value 0 is defined for this keyword, the retry to OCS will not happen instead the configured action will be immediately applied.

### Usage

Use this command to configure whether to continue/terminate calls when Diameter server(s)/OCS are unreachable. This command can be used to verify the functionality of the configurable action if the OCS becomes unreachable.

In 12.1 and earlier releases, the OCS is considered down/unreachable when all transport/TCP connections are down for that OCS.

In 12.2 and later releases, the OCS is declared unreachable when all transport connections are down OR message timeouts happen (for example, a Tx expiry or response timeout, for all available OCS servers) owing to slow response from the OCS (may be due to network congestion or other network related issues).

The following set of actions are performed if the servers become unreachable:

- **During initial session establishment**:
  - Block traffic: Terminate the session.
  - Continue call: Continue by making the session offline.
  - Pass traffic until timer expiration post which terminates the call: Session would be offline while the timer is running.
Credit Control Configuration Mode Commands

- Pass traffic until interim time expiration post which continues or terminates the call.
- Pass traffic until interim volume expiration post which continues or terminates the call.

- During mid session:
  - Block traffic: Terminate the session.
  - Continue call: Continue by making the session offline.
  - Run out of session quota post which terminates the call.
  - Pass traffic until timer expiration post which terminates the call: Session would be offline while the timer is running.
  - Pass traffic until interim time expiration post which continues or terminates the call.
  - Pass traffic until interim volume expiration post which continues or terminates the call.

This command works on the same lines as the failure-handling command, which is very generic for each of the xxx-requests.

The servers-unreachable CLI command is specifically for TCP connection error. In the event of TCP connection failure, the failure-handling and/or servers-unreachable commands can be used. This way, the operator has the flexibility to configure CCFH independent of OCS-unreachable feature, that is having two different failure handlings for same request types.

**Important:** Please note that the flexibility to configure CCFH independent of OCS-unreachable feature is applicable only to 12.1 and earlier releases. In 12.2 and later releases, if configured, the servers-unreachable takes precedence over the failure-handling command.

This command can also be used to control the triggering of behavior based on transport failure, response message timeouts or Tx expiry when OCS becomes unreachable. The OCS could be unreachable due to no TCP connection and the message timeout could be due to network congestion or any other network related issues.

The following are the possible and permissible configurations with respect to behavior triggering:

- servers-unreachable behavior-triggers { initial-request | update-request } transport-failure
- servers-unreachable behavior-triggers { initial-request | update-request } transport-failure response-timeout
- servers-unreachable behavior-triggers { initial-request | update-request } transport-failure tx-expiry

Of these configurations, the first one is considered to be the default configuration and it will take care of backward compatibility with 12.0 implementation.

If the server returns the CC-Failure-Handling AVP, it would apply for transport-failure/response-timeout/tx-expiry when the CLI command servers-unreachable is not configured. If the servers-unreachable is configured for a set of behavior-triggers, then servers-unreachable configuration will be applied for them.

For those behavior-triggers for which servers-unreachable is not configured, the CC-Failure-Handling value provided by the server will be applied.

By default, Result-Code such as 3002 (Unable-To-Deliver), 3004 (Too-Busy) and 3005 (Loop-Detected) falls under delivery failure category and will be treated similar to response-timeout configuration.

**Example**

The following command configures the duration of 1111 seconds, for the subscriber session to be in offline state, after which the initial request calls will be terminated.

```plaintext
servers-unreachable initial-request terminate after-timer-expiry 1111
```
subscription-id service-type

This command enables required Subscription-Ids for various service types.

**Product**

GGSN
HA
IPSG
PDSN
P-GW

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > ACS Configuration > Credit Control Configuration

active-charging service service_name > credit-control

Entering the above command sequence results in the following prompt:

[local]host_name(config-dcca)#

**Syntax**

subscription-id service-type { closedrp | ggsn | ha | ipsg | l2tplns | mipv6ha | pdsn | pgw } { e164 | imsi | nai }

[ no ] subscription-id service-type { closedrp | ggsn | ha | ipsg | l2tplns | mipv6ha | pdsn | pgw }

**Usage**

Currently, Subscription-Id AVP is encoded in the Gy CCRs based on dictionary and service-type checks. With the new CLI command, customers will have the provision of enabling required Subscription-Id types for various services.
Each service can have a maximum of three Subscription-Id types (e164, imsi & nai) that can be configured through this CLI command. The DCCA specific changes are made in such a way that, if the CLI command is configured for any particular service, then the CLI takes precedence. Else, it falls back to default (hard-coded) values configured for that service.

The advantage of this CLI command is that any further dictionary additions in DCCA can be minimized.

**Important:** The CLI configured for any of the service will contain the most recent Subscription-Id-types configured for that service (i.e. overrides the previous values).

For an instance, if a customer wants IMSI value to be encoded in Gy CCRs (along with E164) for MIPv6HA service, then this CLI command `subscription-id service-type mipv6ha e164 imsi` should be configured in the Credit Control Configuration mode.

If only imsi is configured through the CLI, then Gy CCRs will only have imsi value.

**Example**

The following command configures imsi type for ggsn service:

```
subscription-id service-type ggsn imsi
```
timestamp-rounding

This command configures how to convert exact time into the units that are used in quotas.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Credit Control Configuration

**Syntax**
```
timestamp-rounding { ceiling | floor | roundoff }
```

**Usage**
Use this command to configure how to convert exact time into the units that are used in quotas for CCA charging.
The specified rounding will be performed before system attempts any calculation. For example using roundoff, if the start time is 1.4, and the end time is 1.6, then the calculated duration will be 1 (i.e., $2 - 1 = 1$).

**Example**
The following command sets the CCA timestamp to nearest integer value second (for example, 34:12.23 to 34:12.00):
```
timestamp-rounding roundoff
```
trigger type

This command enables/disables triggering a credit reauthorization when the named values in the subscriber session changes.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Credit Control Configuration

active-charging service service_name > credit-control

Entering the above command sequence results in the following prompt:

[local]host_name(config-dcca)#

Syntax

[ no ] trigger type { cellid | lac | mcc | mnc | qos | rat | serving-node | sgsn | timezone } +

default trigger type

<table>
<thead>
<tr>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configures this command with the default setting.</td>
</tr>
<tr>
<td>Default: No triggers.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>no</th>
</tr>
</thead>
<tbody>
<tr>
<td>Removes the previously configured trigger type.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>cellid</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sets the trigger based on change in cell identity or Service Area Code (SAC).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>lac</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sets the trigger based on change in Location Area Code.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>mcc</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sets the trigger based on change in Mobile Country Code (MCC).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>mnc</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sets the trigger based on change in Mobile Network Code (MNC).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>qos</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sets the trigger based on change in the Quality of Service (QoS).</td>
</tr>
</tbody>
</table>
**rat**
Sets the trigger based on change in the Radio Access Technology (RAT).

**serving-node**
Sets the trigger based on change in serving node. The serving node change causes the credit control client to ask for a re-authorization of the associated quota. Typically used as an extension to sgsn trigger in P-GW (SAEGW), however, may also be used alone.

**sgsn**
Sets the trigger based on change in the IP address of SGSN.

**timezone**
Sets the trigger based on change in the timezone of UE.

**+**
Indicates that more than one of the previous keywords can be entered within a single command.

---

**Usage**

Use this command to set the credit control reauthorization trigger.

**Example**

The following command selects a credit control trigger as lac:

```
trigger type lac
```
usage-reporting

This command configures the ACS Credit Control usage reporting type.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Credit Control Configuration

active-charging service service_name > credit-control

Entering the above command sequence results in the following prompt:

[local]host_name(config-dcca)#

Syntax

usage-reporting quotas-to-report based-on-grant { report-only-granted-volume }

default usage-reporting quotas-to-report

  default
  Configures this command with the default setting.
  Default: Disabled

  report-only-granted-volume
  Suppresses the input and output octets. If the Granted-Service-Unit (GSU) AVP comes with CC-Total-Octets, then the device will send total, input and output octets in Used-Service-Unit (USU) AVP. If it comes with Total-Octets, the device will send only Total-Octets in USU.

Usage

Use this command to configure reporting usage only for granted quota. On issuing this command, the Used-Service-Unit AVP will report quotas based on grant i.e, only the quotas present in the Granted-Service-Unit AVP.

With this command only the units for which the quota was granted by the DCCA server will be reported irrespective of the reporting reason.

Example

The following command configures to report usage based only on granted quota:

  usage-reporting quotas-to-report based-on-grant
Chapter 57
Crypto Group Configuration Mode Commands

The Crypto Group Configuration Mode is used to configure crypto (tunnel) groups that provide fail-over redundancy for IPSec tunnels to packet data networks (PDNs).

Mode

Exec > Global Configuration > Context Configuration > Crypto Group Configuration

`configure > context context_name > crypto group group_name`

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-crypto-grp)#`

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
**end**

Exits the current configuration mode and returns to the Exec mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**

Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

exit

Usage
Use this command to return to the parent configuration mode.
match address

Associates an access control list (ACL) with the crypto group.

Product

ePDG
FA
GGSN
HA
HeNBGW
HNBGW
HSGW
MME
P-GW
PDSN
S-GW
SAEGW
SCM
SecGW
SGSN

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > Context Configuration > Crypto Group Configuration

configure > context context_name > crypto group group_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-crypto-grp)#

Syntax

[ no ] match address acl_name [ preference ]

no

Deletes a previously configured ACL association.

match address acl_name

Specifies the name of the ACL being matched to the crypto group entered as an alphanumeric string of 1 through 47 characters.
**preference**

The priority of the ACL. The ACL preference is factored when a single packet matches the criteria of more than one ACL. `preference` is an integer from 0 through 4294967295; 0 is the highest priority. If multiple ACLs are assigned the same priority, the last one entered will be used first.

---

**Important:** The priorities are only compared for ACLs matched to other groups or to policy ACLs (those applied to the entire context).

---

**Usage**

IP ACLs are associated with crypto groups using this command. Both the crypto group and the ACLs must be configured in the same context. ISAKMP crypto maps can then be associated with the crypto group. This allows user traffic matching the rules of the ACL to be handled according to the policies configured as part of the crypto map.

**Example**

The following command associates an ACL called `corporate_acl` to the crypto group:

```plaintext
match address corporate_acl
```
match ip pool

Matches the specified IP pool to the current crypto group. This command can be used multiple times to match more than one IP pool.

**Important:** The `match ip pool` command is not supported within a crypto group on the ASR 5500 platform.

**Syntax**

```
[ no ] match ip pool pool-name pool_name
```

- **no**
  - Deletes the matching statement for the specified IP pool from the crypto group.
match ip pool

match ip pool pool-name pool_name

Specifies the name of an existing IP pool that should be matched entered as an alphanumeric string of 1 through 31 characters.

Usage

Use this command to set the names of IP pools that should be matched in the current crypto group.

Example

The following command sets a rule for the current crypto group that will match an IP pool named ippool1:

    match ip pool pool-name ippool1
**switchover**

Configures the fail-over properties for the crypto group as part of the Redundant IPSec Fail-Over feature.

**Product**
- ePDG
- FA
- GGSN
- HA
- HeNBGW
- HNBGW
- HSGW
- MME
- P-GW
- PDSN
- S-GW
- SAEGW
- SCM
- SecGW
- SGSN

**Privilege**
- Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Crypto Group Configuration

```plaintext
configure > context context_name > crypto group group_name
```

Entering the above command sequence results in the following prompt:

```
[context_name] host_name(config-crypto-grp) #
```

**Syntax**

```
[ no ] switchover auto [ do-not-revert ]
```

- **no**
  Disables the automatic switchover of tunnels. This applies to switching primary-to-secondary and secondary-to-primary.

- **switchover auto**
  Allows the automatic switchover of tunnels. Default: Enabled

- **do-not-revert**
  Disables the automatic switchover of secondary tunnels to primary tunnels. Default: Disabled
Usage

This command configures the fail-over options for the Redundant IPSec Fail-over feature. If the automatic fail-over options are disabled, tunneled traffic must be manually switched to the alternate tunnel (or manually activated if no alternate tunnel is configured and available) using the following command in the Exec Mode:

```
crypto-group group_name activate { primary | secondary }
```

For a definition of this command, see the `crypto-group` section of the Exec Mode Commands chapter of this guide.

Example

The following command disables the automatic secondary-to-primary switchover:

```
switchover auto do-not-revert
```
Chapter 58
Crypto IPSec Transform Set Configuration Mode Commands

The Crypto IPSec Transform Set Configuration Mode is used to configure properties for system transform sets. Transform Sets are used to define IPSec security associations (SAs). IPSec SAs specify the IPSec protocols to use to protect packets.

Mode

Exec > Global Configuration > Context Configuration > Crypto IPSec Transform Set Configuration

configure > context context_name > crypto ipsec transform-set transform_set_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-crypto-trans)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
```
exit
```

**Usage**
Use this command to return to the parent configuration mode.
**mode**

Configures the IPSec encapsulation mode for an existing or new transform set. For a new transform set, you must specify transform set parameters as described for the `crypto ipsec transform-set` command in the *Context Configuration Mode Commands* chapter.

**Product**
PDSN
HA
GGSN
PDIF

**Privilege**
Security Administrator

**Syntax**

```
mode { transport | tunnel }
```

**transport**

Specifies that the transform set only protects the upper layer protocol data portions of an IP datagram, leaving the IP header information unprotected. Default: Disabled

**Important:** This mode should only be used if the communications end-point is also the cryptographic end-point.

**tunnel**

Specifies that the transform set protects the entire IP datagram. This mode should be used if the communications end-point is different from the cryptographic end-point as in a VPN. Default: Enabled

**Usage**

This command specifies the encapsulation mode for the transform set.

**Example**

The following command configures the transforms set’s encapsulation mode to transport:

```
    mode transport
```
Chapter 59
Crypto Map IKEv2-IPv4 Configuration Mode Commands

The Crypto Map IKEv2-IPv4 Configuration Mode is used to configure an IKEv2 IPsec policy for secure X3 interface tunneling between a P-GW and a lawful intercept server.

Mode

Exec > Global Configuration > Context Configuration > Crypto Map IKEv2-IPv4 Configuration

configure > context context_name > crypto map template_name ikev2-ipv4

Entering the above command sequence results in the following prompt:

[context_name]host_name(cfg-crypto-ikev2-ipv4-map)#

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
allow-cert-enc cert-hash-url

Enables support for a certificate encoding type other than the default. When enabled hash and URL encoding type are supported in CERT and CERTREQ payloads.

Product
Security gateway products

⚠️ Important: This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

Privilege
Security Administrator

Syntax

allow-cert-enc cert-hash-url
no allow-cert-enc cert-hash-url

Usage
Enable support for a certificate encoding type other than the default. When enabled hash and URL encoding type are supported in CERT and CERTREQ payloads.

Example
The following command enables hash and URL encoding type in CERT and CERTREQ payloads:

allow-cert-enc cert-hash-url
authentication

Configures the subscriber authentication method used for this crypto map.

Product
- ePDG
- FA
- GGSN
- HA
- HeNBGW
- HNBGW
- HSGW
- MME
- P-GW
- PDSN
- S-GW
- SAEGW
- SCM
- SecGW
- SGSN

Privilege
Security Administrator

Syntax

```
authentication { local | remote } ( certificate | pre-shared-key { encrypted key value | key value }
```

- **local | remote**
  Specifies which authentication method will be used by the crypto map – local or remote.

- **certificate**
  Specifies that a certificate will be used by this crypto map for authentication.

- **pre-shared-key { encrypted key value | key value }**
  Specifies that a pre-shared key will be used by this crypto map for authentication.
  - **encrypted key value**: Specifies that the pre-shared key used for authentication is encrypted and expressed as an alphanumeric string of 1 through 255 characters for releases prior to 15.0, or 16 to 496 characters for release 15.0 and higher.
  - **key value**: Specifies that the pre-shared key used for authentication is clear text and expressed as an alphanumeric string of 1 through 32 characters for releases prior to 14.0 or 1 through 255 characters for release 14.0 and higher.
**Usage**

Use this command to specify the type of authentication performed for IPSEC peers attempting to access the system via this crypto map.

**Example**

The following command sets the authentication method to an open key value of `6d797061737377647264`:

```plaintext
authentication pre-shared-key key 6d7970617377647264
```
blacklist

Enables or disables a blacklist (access denied) for this map.

**Product**

All products supporting IPSec blacklisting

**Important:** This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

**Privilege**

Security Administrator

**Syntax**

```plaintext
blacklist
no blacklist
```

no blacklist

Disables blacklisting for this crypto map. By default blacklisting is disabled.

**Usage**

Use this command to enable blacklisting for this crypto map. A blacklist is a list or register of entities that are denied a particular privilege, service, mobility, access or recognition. With blacklisting, any peer is allowed to connect as long as it does not appear in the list. For additional information on blacklisting, refer to the *System Administration Guide*.

**Example**

The following command enables blacklisting:

```
blacklist
```
ca-certificate list

Used to bind an X.509 Certificate Authority (CA) certificate to a crypto map.

Product
- ePDG
- FA
- GGSN
- HA
- HeNBGW
- HNBGW
- HSGW
- MME
- P-GW
- PDSN
- S-GW
- SAEGW
- SCM
- SecGW
- SGSN

Privilege
Security Administrator

Syntax

```
ca-certificate list ca-cert-name name [ ca-cert-name name ]
```

no ca-certificate

```
no
```

Unbinds the ca-certificate(s) bound to the crypto map.

```
ca-cert-name name
```

Binds the named X.509 Certificate Authority (CA) certificate to a crypto map. `name` is an alphanumeric string of 1 through 129 characters.
You can chain multiple (max 4) certificates in a single command instance.

Usage
Used to bind an X.509 CA certificate to a map.

Example
Use the following example to add a CA certificate to a list:

```
ca-certificate list CA_list1
```
ca-crl list

Binds one or more Certificate Authority-Certificate Revocation Lists (CA-CRLs) to this crypto map.

Product
- ePDG
- FA
- GGSN
- HA
- HeNBGW
- HNBGW
- HSGW
- MME
- P-GW
- PDSN
- S-GW
- SAEGW
- SCM
- SecGW
- SGSN

Privilege
- Security Administrator

Syntax
```
ca-crl list ca-crl-name name [ ca-crl-name name ] +
```
```
no ca-crl
```

**no**
Removes the CA-CRL configuration from this map.

**ca-crl-name name**
Specifies the CA-CRL to associate with this crypto map. name must be the name of an existing CA-CRL expressed as an alphanumeric string of 1 through 129 characters. List od multiple CA-CRL can be configured for a crypto map.
You can chain multiple(max 4) CA-CRLs in a single command instance.

Usage
Use this command to associate a CA-CRL name with this crypto map.
CA-CRLs are configured in the Global Configuration Mode. For more information about configuring CA-CRLs, refer to the ca-crl name command in the Global Configuration Mode Commands chapter.

Example
The following example binds CA-CRLs named $CRL-5$ and $CRL-7$ to this crypto map:

```
ca-crl list ca-crl-name CRL-5 ca-crl-name CRL-7
```
**certificate**

Used to bind a single X.509 trusted certificate to a crypto map.

**Product**
-ePDG
-FA
-GGSN
-HA
-HeNBGW
-HNBGW
-HSGW
-MME
-P-GW
-PDSN
-S-GW
-SAEGW
-SCM
-SecGW
-SGSN

**Privilege**
Security Administrator

**Syntax**

```plaintext
[ no ] certificate name
```

- **no**
  - Unbinds a certificate from crypto map.

- **name**
  - Specifies the name of a X.509 trusted certificate to bind to a crypto map. *name* is an alphanumeric string of 1 through 129 characters.

**Usage**
Use this command to bind an X.509 certificate to a map.

**Example**
Use the following example to prevent a certificate from being included in the Auth Exchange payload:

```plaintext
no certificate
```
control-dont-fragment

Controls the Don’t Fragment (DF) bit in the outer IP header of the IPSec tunnel data packet.

Product
- ePDG
- FA
- GGSN
- HA
- HeNBGW
- HNBGW
- HSGW
- MME
- P-GW
- PDSN
- S-GW
- SAEGW
- SCM
- SecGW
- SGSN

Privilege
Security Administrator

Syntax
```
control-dont-fragment { clear-bit | copy-bit | set-bit }
```

Usage
A packet is encapsulated in IPsec headers at both ends. The new packet can copy the DF bit from the original unencapsulated packet into the outer IP header, or it can set the DF bit if there is not one in the original packet. It can also clear a DF bit that it does not need.

Example
The following command sets the DF bit in the outer IP header:
```
control-dont-fragment set-bit
```
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

exit

Usage
Use this command to return to the parent configuration mode.
ikev2-ikesa

Configures parameters for the IKEv2 IKE Security Associations within this crypto template.

Product
- ePDG
- FA
- GGSN
- HA
- HeNBGW
- HNBGW
- HSGW
- MME
- P-GW
- PDSN
- S-GW
- SAEGW
- SCM
- SecGW
- SGSN

Privilege
- Security Administrator

Syntax


default ikev2-ikesa { allow-empty-ikesa | max-retransmissions | policy error-notification | rekey [ disallow-param-change ] | setup-timer }

no ikev2-ikesa name | policy { error-notification | use-rfc5996-notification } | rekey sec | transform-set list

no ikev2-ikesa

Disables a previously enabled parameter.

allow-empty-ikesa

Default is not to allow-empty-ikesa. Activate to have the IKEv2 stack keep the IKE SA when all the Child SAs have been deleted.
max-retransmissions number

Specifies the maximum number of retransmissions of an IKEv2 IKE Exchange Request if a response has not been received. number must be an integer from 1 through 8. Default: 5


Specifies the default policy for generating an IKEv2 Invalid Message ID error when PDIF receives an out-of-sequence packet.

- error-notification: Sends an Error Notify Message to the MS for Invalid IKEv2 Exchange Message ID and Invalid IKEv2 Exchange Syntax for the IKE_SA_INIT Exchange.
- [invalid-major-version]: Sends an Error Notify Message for Invalid Major Version
- [invalid-message-id]: Sends an Error Notify Message for Invalid IKEv2 Exchange Message ID.
- [invalid-syntax]: Sends an Error Notify Message for Invalid IKEv2 Exchange Syntax.

use-rfc5996-notification: Enables support for TEMPORARY_FAILURE and CHILDSA_NOT_FOUND notify payloads.

rekey [ disallow-param-change ]

Specifies if IKESA rekeying should occur before the configured lifetime expires (at approximately 90% of the lifetime interval). Default is not to re-key.

The disallow-param-change option does not allow changes in negotiation parameters during rekey.

retransmission-timeout msec

Specifies the timeout period (in milliseconds) before a retransmission of an IKEv2 IKE exchange request is sent (if the corresponding response has not been received). msec must be an integer from 300 to 15000. Default: 500

exponential

Specifies that the subsequent retransmission delays are exponentially increased with a maximum limit of 15000ms.

setup-timer sec

Specifies the number of seconds before a IKEv2 IKE Security Association that is not fully established is terminated. sec must be an integer from 1 through 3600. Default: 16

transform-set list name1 ...name6

Specifies the name of a context-level configured IKEv2 IKE Security Association transform set. name1 ...name6 must be an existing IKEv2 IKESA Transform Set expressed as an alphanumeric string of 1 through 127 characters.

The transform set is a space-separated list of IKEv2-IKESA SA transform sets to be used for deriving IKEv2 IKE Security Associations from this crypto template. A minimum of one transform-set is required; maximum configurable is six.

Usage

Use this command to configure parameters for the IKEv2 IKE Security Associations within this crypto template.

Example
The following command configures the maximum number of IKEv2 IKESA request retransmissions to 7:

```
ikev2-ikesa max-retransmissions 7
```

The following command configures the IKEv2 IKESA request retransmission timeout to 400 milliseconds:

```
ikev2-ikesa retransmission-timeout 400
```

The following command configures the IKEv2 IKESA transform set `ikesa43`:

```
ikev2-ikesa transform-set list ikesa43
```
**keepalive**

Configures keepalive or dead peer detection for security associations used within this crypto template.

**Product**
- ePDG
- FA
- GGSN
- HA
- HeNBGW
- HNBGW
- HSGW
- MME
- P-GW
- PDSN
- S-GW
- SAEGW
- SCM
- SecGW
- SGSN

**Privilege**
Security Administrator

**Syntax**

```
keepalive [ interval sec ]
default keepalive [ interval ]
no keepalive
```

**Usage**
Use this command to set parameters associated with determining the availability of peer servers.

**Example**
The following command sets a keepalive interval to three minutes (180 seconds):

```
keepalive interval 180
```
match

Matches or associates the crypto map to an access control list (ACL) configured in the same context.

Product
- ePDG
- FA
- GGSN
- HA
- HeNBGW
- HNBGW
- HSGW
- MME
- P-GW
- PDSN
- S-GW
- SAEGW
- SCM
- SecGW
- SGSN

Privilege
Security Administrator

Syntax

```plaintext
match address acl_name [ priority ]

no match address acl_name
```

- **no**
  Removes a previously matched ACL.

```plaintext
match address acl_name
```

Specifies The name of the ACL with which the crypto map is to be matched. `acl_name` is an alphanumeric string of 1 through 79 characters that is case sensitive.

```plaintext
priority
```

Specifies the preference of the ACL as integer from 0 through 4294967295. 0 is the highest priority. Default: 0
The ACL preference is factored when a single packet matches the criteria of more than one ACL.

**Important:** The priorities are only compared for ACLs matched to other crypto maps or to policy ACLs (those applied to the entire context).
Usage
ACLs matched to crypto maps are referred to as crypto ACLs. Crypto ACLs define the criteria that must be met in order for a subscriber data packet to routed over an IPSec tunnel. Prior to routing, the system examines the properties of each subscriber data packet. If the packet properties match the criteria specified in the crypto ACL, the system will initiate the IPSec policy dictated by the crypto map.

Example
The following command sets the crypto map ACL to the ACL named acl-list1 and sets the crypto maps priority to the highest level.

```
match address acl-list1 0
```
natt

Configures Network Address Translation - Traversal (NAT-T) for all security associations associated with this crypto template. This feature is disabled by default.

**Product**
All Security Gateway products

**Privilege**
Security Administrator

**Syntax**

```
[ default | no ] natt [ include-header ] [ send-keepalive [ idle-interval idle_secs ] [ interval interval_secs ] ]
```

- **default**
  Disables NAT-T for all security associations associated with this crypto template.

- **no**
  Disables NAT-T for all security associations associated with this crypto template.

- **include-header**
  Includes the NAT-T header in IPSec packets.

- **send-keepalive [ idle-interval idle_secs ] [ interval interval_secs ]**
  Sends NAT-Traversal keepalive messages.

  - **idle-interval idle_secs**: Specifies the number of seconds that can elapse without sending NAT keepalive packets before sending NAT keepalive packets is started. `idle_secs` is an integer from 20 to 86400. Default: 60.

  - **interval interval_secs**: Specifies the number of seconds between the sending of NAT keepalive packets. `interval_secs` is an integer from 20 to 86400. Default: 60.

**Usage**
Use this command to configure NAT-T for security associations within this crypto template.

**Example**
The following command disables NAT-T for this crypto template:

```
no natt
```
ocsp

Enables use of Online Certificate Status Protocol (OCSP) from a crypto template. OCSP provides a facility to obtain timely information on the status of a certificate.

Product
All products supporting IPSec

Important: This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

Privilege
Security Administrator

Syntax

```
ocsp [ nonce | responder-address ipv4_address [ port port_value ] ]
no ocsp [ nonce | responder-address [ port ] ]
default ocsp [ nonce ]
```

- **no**
  - Disables the use of OCSP.

- **default**
  - Sets / Restores default value assigned for ocsp nonce.

- **nonce**
  - Enables sending nonce (unique identifier) in OCSP requests.

- **responder-address ipv4_address**
  - Configures the OCSP responder address (IPv4), used when absent in peer (device) certificate. 
    `ipv4_address` is an IPv4 address specified in dotted decimal format.

- **port port_value**
  - Configures the port for OCSP responder.
    `port_value` is an integer value between 1 and 65535. The default port is 8889.

Usage
This command enables the use of Online Certificate Protocol (OCSP) from a crypto map/template. OCSP provides a facility to obtain timely information on the status of a certificate. OCSP messages are exchanged between a gateway and an OCSP responder during a certificate transaction. The responder immediately provides the status of the presented certificate. The status can be good, revoked or unknown. The gateway can then proceed based on the response.

Example
ocsp
payload

Creates a new, or specifies an existing, crypto map payload and enters the Crypto Map Payload Configuration Mode.

**Product**
- ePDG
- FA
- GGSN
- HA
- HeNBGW
- HNBGW
- HSGW
- MME
- P-GW
- PDSN
- S-GW
- SAEGW
- SCM
- SecGW
- SGSN

**Privilege**
Security Administrator

**Syntax**

```payload name match ipv4```

```no payload name```

---

**payload name**

Specifies the name of a new or existing crypto template payload as an alphanumeric string of 1 through 127 characters.

**match ipv4**

Filters IPSec IPv4 Child Security Association creation requests for subscriber calls using this payload. Further filtering can be performed by applying the following:

**Usage**

Use this command to create a new or enter an existing crypto template payload. The payload mechanism is a means of associating parameters for the Security Association (SA) being negotiated. Two payloads are required: one each for MIP and IKEv2. The first payload is used for establishing the initial Child SA Tunnel Inner Address (TIA) which will be torn down. The second payload is used for establishing
the remaining Child SAs. Note that if there is no second payload defined with home-address as the \textit{ip-address-allocation} then no MIP call can be established, just a Simple IP call. Currently, the only available match is for ChildSA, although other matches are planned for future releases. Entering this command results in the following prompt:

\texttt{[ctxt\_name]\,hostname(cfg-crypto-<name>-ikev2-tunnel-payload)#

Crypto Template IKEv2-IPv4 Payload Configuration Mode commands are defined in the Crypto Template IKEv2-IPv4 Payload Configuration Mode Commands chapter.

\textbf{Example}

The following command configures a crypto template payload called \texttt{payload5} and enters the Crypto Template IKEv2-IPv6 Payload Configuration Mode:

\texttt{payload payload5 match ipv4}
peer

Configures the IP address of a peer IPSec.

Product

ePDG
FA
GGSN
HA
HeNBGW
HNBGW
HSGW
MME
P-GW
PDSN
S-GW
SAEGW
SCM
SecGW
SGSN

Privilege

Security Administrator

Syntax

**peer** ip_address

**no peer**

---

**no**

Removes the configured peer IP address.

**peer ip_address**

Specifies the IP address of a peer IPSec server in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

---

Usage

Use this command to specify a peer IPsec peer server. The IPsec peer server can also be the Lawful Intercept server.

Example

The following command configures the system to recognize an IPsec peer server with an IPv6 address of `fe80::200:f8ff:fe21:67cf`. 
peer fe80::200:ff:fe21:67cf
remote-secret-list

Enables the use of a Remote Secret List containing up to 1000 pre-shared keys.

Product
All Security Gateway products

Important: This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

Privilege
Security Administrator

Syntax
remote-secret-list list_name
no remote-secret-list

- list_name
  Specifies the name of an existing Remote Secret List as an alphanumeric string of 1 through 127 characters.

Usage
Enable the use of a Remote Secret List containing up to 1000 pre-shared keys.
Only one active remote-secret-list is supported per system.
For additional information, refer to the Remote Secret List Configuration Commands chapter of the Command Line Interface Reference and the System Administration Guide.

Example
The following command enables a remote-secret-list named rs-list:

remote-secret-list rs-list
whitelist

Enables or disables a whitelist (access granted) for this crypto map.

**Product**

All products supporting IPSec whitelisting

**Important**: This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

**Privilege**

Security Administrator

**Syntax**

```
whitelist

no whitelist
```

```
no
```

Disables whitelisting for this crypto map. By default whitelisting is disabled.

**Usage**

Use this command to enable whitelisting for this crypto map. A whitelist is a list or register of entities that are being provided a particular privilege, service, mobility, access or recognition. With whitelisting, no peer is allowed to connect unless it appears in the list. For additional information on whitelisting, refer to the *System Administration Guide*.

**Example**

The following command enables whitelisting:

```
whitelist
```
Chapter 60
Crypto Map IKEv2-IPv4 Payload Configuration Mode
Commands

The Crypto Map IKEv2-IPv4 Payload Configuration Mode is used to assign the correct IPSec transform-set from a list of up to four different transform-sets, and to assign Mobile IP addresses.

Exec > Global Configuration > Context Configuration > Crypto Map IKEv2-IPv4 > Crypto Map IKEv2-IPv4 Payload Configuration

```bash
configure > context context_name > crypto map map_name ikev2-ipv4 > payload payload_name
match ipv4
```

Entering the above command sequence results in the following prompt:

```
/context_name/host_name(cfg-crypto-ikev2-ipv4-payload)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
end

**Usage**
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**
Use this command to return to the parent configuration mode.
ipsec

Encrypts and decrypts data across the network using the IPSec protocol.

Configures the IPSec transform set to be used for this crypto template payload.

Product
- ePDG
- FA
- GGSN
- HA
- HeNBGW
- HNBGW
- HSGW
- MME
- P-GW
- PDSN
- S-GW
- SAEGW
- SCM
- SecGW
- SGSN

Privilege
Security Administrator

Syntax

ipsec transform-set list name

no ipsec transform-set list

Specifies the context configured IPSec transform set name to be used in the crypto template payload. This is a space-separated list. From 1 to 4 transform sets can be entered. name is an alphanumeric string of 1 through 127 characters.

Usage
Use this command to list the IPSec transform set(s) to use in this crypto template payload.

Example
The following command configures IPSec transform sets named ipset1 and ipset2 to be used in this crypto template payload:

ipsec transform-set list ipset1 ipset2
lifetime

Configures the number of seconds and/or kilobytes for IPSec Child SAs derived from this crypto template payload to exist.

Product

ePDG
FA
GGSN
HA
HeNBGW
HNBGW
HSGW
MME
P-GW
PDSN
S-GW
SAEGW
SCM
SecGW
SGSN

Privilege

Security Administrator

Syntax

lifetime { sec [ kilo-bytes kbytes ] | kilobytes kbytes }

default lifetime

default

Returns the lifetime value to the default setting of 86400 seconds.

sec

Specifies the number of seconds for IPSec Child Security Associations derived from this crypto template payload to exist. sec must be an integer from 60 through 604800. Default: 86400

kilo-bytes kbytes

Specifies lifetime in kilobytes for IPSec Child Security Associations derived from this Crypto Map. kbytes must be an integer from 1 through 2147483648.
**Usage**

Use this command to configure the number of seconds and/or kilobytes for IPSec Child Security Associations derived from this crypto template payload to exist.

**Example**

The following command configures the IPSec child SA lifetime to be 120 seconds:

```
lifetime 120
```
rekey

Configures child security association rekeying.

**Product**
- ePDG
- FA
- FNG
- GGSN
- HA
- HNBGW
- P-GW
- PDSN
- SAEGW
- SCM
- SGSN

**Privilege**
Security Administrator

**Syntax**

```
rekey [ keepalive ]
```

```
[ default | no ] rekey
```

- **default**
  Returns the feature to the default setting of disabled.

- **no**
  Disables this feature.

- **keepalive**
  If specified, a session will be rekeyed even if there has been no data exchanged since the last rekeying operation. By default rekeying is only performed if there has been data exchanged since the previous rekey.

**Usage**
Use this command to enable or disable the ability to rekey IPSec Child SAs after approximately 90% of the Child SA lifetime has expired. The default, and recommended setting, is not to perform rekeying. No rekeying means the P-GW will not originate rekeying operations and will not process CHILD SA rekeying requests from the MS.

**Example**
The following command disables rekeying:

```
no rekey
```
Chapter 61
Crypto Map IKEv2-IPv6 Configuration Mode Commands

The Crypto Map IKEv2-IPv6 Configuration Mode is used to configure an IKEv2 IPsec policy for secure X3 interface tunneling between a P-GW and a lawful intercept server.

Mode

Exec > Global Configuration > Context Configuration > Crypto Map IKEv2-IPv6 Configuration

configure > context context_name > crypto map map_name ikev2-ipv6

Entering the above command sequence results in the following prompt:

[context_name]host_name(cfg-crypto-ikev2-ipv6-map)#

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
allow-cert-enc cert-hash-url

Enables support for a certificate encoding type other than the default. When enabled hash and URL encoding type are supported in CERT and CERTREQ payloads.

**Product**
Security gateway products

**Important:** This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

**Privilege**
Security Administrator

**Syntax**

```
allow-cert-enc cert-hash-url
no allow-cert-enc cert-hash-url
```

- `no`
Disables support for hash and URL encoding type in CERT and CERTREQ payloads.

**Usage**
Enable support for a certificate encoding type other than the default. When enabled hash and URL encoding type are supported in CERT and CERTREQ payloads.

**Example**
The following command enables hash and URL encoding type in CERT and CERTREQ payloads:

```
allow-cert-enc cert-hash-url
```
**authentication**

Configures the subscriber authentication method used for this crypto map.

**Product**
- ePDG
- FA
- GGSN
- HA
- HeNBGW
- HNBGW
- HSGW
- MME
- P-GW
- PDSN
- S-GW
- SAEGW
- SCM
- SecGW
- SGSN

**Privilege**
Security Administrator

**Syntax**

```
authentication { local | remote } ( certificate | pre-shared-key { encrypted key value | key value }
```

- **local | remote**
  Specifies which authentication method will be used by the crypto map – local or remote.

- **certificate**
  Specifies that a certificate will be used by this crypto map for authentication.

- **pre-shared-key { encrypted key value | key value }**
  Specifies that a pre-shared key will be used by this crypto map for authentication.
  - **encrypted key value**
    Specifies that the pre-shared key used for authentication is encrypted and expressed as an alphanumeric string of 1 through 255 characters for releases prior to 15.0, or 16 to 444 characters for release 15.0 and higher.
  - **key value**
    Specifies that the pre-shared key used for authentication is clear text and expressed as an alphanumeric string of 1 through 32 characters for releases prior to 14.0 or 1 through 255 characters for release 14.0 and higher.
**Usage**

Use this command to specify the type of authentication performed for subscribers attempting to access the system via this crypto map.

**Example**

The following command sets the authentication method to an open key value of `6d79061737767264`:

```
authentication pre-shared-key key 6d79061737767264
```
blacklist

Enables or disables a blacklist (access denied) for this map.

Product
All products supporting IPSec blacklisting

Important: This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

Privilege
Security Administrator

Syntax

blacklist

no blacklist

Usage
Use this command to enable blacklisting for this crypto map. A blacklist is a list or register of entities that are denied a particular privilege, service, mobility, access or recognition. With blacklisting, any peer is allowed to connect as long as it does not appear in the list. For additional information on blacklisting, refer to the System Administration Guide.

Example
The following command enables blacklisting:

blacklist
ca-certificate list

Used to bind an X.509 Certificate Authority (CA) root certificate to a crypto template.

Product

- ePDG
- FA
- GGSN
- HA
- HeNBGW
- HNBGW
- HSGW
- MME
- P-GW
- PDSN
- S-GW
- SAEGW
- SCM
- SecGW
- SGSN

Privilege

Security Administrator

Syntax

`ca-certificate list ca-cert-name name [ ca-cert-name name ]`

`no ca-certificate`

- `no`
  Removes a CA root certificate from the list.

- `ca-cert-name name`
  Binds the named X.509 Certificate Authority (CA) root certificate to a crypto template. `name` is an alphanumeric string of 1 through 129 characters.
  You can chain multiple certificates in a single command instance.

Usage

Used to bind an X.509 CA root certificate to a template.

Example

Use the following example to add a CA root certificate to a list:

`ca-certificate list CA_list1`
**ca-crl list**

Binds one or more Certificate Authority-Certificate Revocation Lists (CA-CRLs) to this crypto template.

**Product**
- ePDG
- FA
- GGSN
- HA
- HeNBGW
- HNBGW
- HSGW
- MME
- P-GW
- PDSN
- S-GW
- SAEGW
- SCM
- SecGW
- SGSN

**Privilege**
Security Administrator

**Syntax**

```plaintext
ca-crl list ca-crl-name name [ ca-crl-name name ] +

no ca-crl
```

- **no**
  Removes the CA-CRL configuration from this template.

- **ca-crl-name name**
  Specifies the CA-CRL to associate with this crypto template. name must be the name of an existing CA-CRL expressed as an alphanumeric string of 1 through 129 characters. Multiple lists can be configured for a crypto template. You can chain multiple CA-CRLs in a single command instance.

**Usage**

Use this command to associate a CA-CRL name with this crypto template. CA-CRLs are configured in the Global Configuration Mode. For more information about configuring CA-CRLs, refer to the **ca-crl name** command in the *Global Configuration Mode Commands* chapter.

**Example**
The following example binds CA-CRLs named CRL-5 and CRL-7 to this crypto template:

```
ca-crl list ca-crl-name CRL-5 ca-crl-name CRL-7
```
**certificate**

Used to bind a single X.509 trusted certificate to a crypto template.

**Product**

ePDG  
FA  
GGSN  
HA  
HeNBGW  
HNBGW  
HSGW  
MME  
P-GW  
PDSN  
S-GW  
SAEGW  
SCM  
SecGW  
SGSN

**Privilege**

Security Administrator

**Syntax**

```
[ no ] certificate name
```

---

**no**

Removes any applied certificate or prevents the certificate from being included in the Auth Exchange response payload.

---

**name**

Specifies the name of a X.509 trusted certificate to bind to a crypto template. *name* is an alphanumeric string of 1 through 127 characters.

---

**Usage**

Can be used to bind an X.509 certificate to a template, or include or exclude it from the Auth Exchange response payload.

**Example**

Use the following example to prevent a certificate from being included in the Auth Exchange payload:

```
no certificate
```
control-dont-fragment

Controls the Don’t Fragment (DF) bit in the outer IP header of the IPSec tunnel data packet.

Product

ePDG
FA
GGSN
HA
HeNBGW
HNBGW
HSGW
MME
P-GW
PDSN
S-GW
SAEGW
SCM
SecGW
SGSN

Privilege

Security Administrator

Syntax

color-dont-fragment { clear-bit | copy-bit | set-bit }

{ clear-bit | copy-bit | set-bit }

clear-bit: Clears the DF bit from the outer IP header (sets it to 0).
copy-bit: Copies the DF bit from the inner IP header to the outer IP header. This is the default action.
set-bit: Sets the DF bit in the outer IP header (sets it to 1).

Usage

A packet is encapsulated in IPsec headers at both ends. The new packet can copy the DF bit from the original unencapsulated packet into the outer IP header, or it can set the DF bit if there is not one in the original packet. It can also clear a DF bit that it does not need.

Example

The following command sets the DF bit in the outer IP header:

    control-dont-fragment set-bit
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**
Use this command to return to the Exec mode.
**exit**

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
```plaintext
exit
```

**Usage**
Use this command to return to the parent configuration mode.
ikev2-ikesa

Configures parameters for the IKEv2 IKE Security Associations within this crypto map.

**Product**
- ePDG
- FA
- GGSN
- HA
- HeNFBGW
- HNBGW
- HSGW
- MME
- P-GW
- PDSN
- S-GW
- SAEGW
- SCM
- SecGW
- SGSN

**Privilege**
- Security Administrator

**Syntax**

```
ikev2-ikesa { allow-empty-ikesa | max-retransmissions number | policy { error-notification | use-rfc5996-notification } | rekey [ disallow-param-change ] | retransmission-timeout msec | setup-timer sec | transform-set list name }

default ikev2-ikesa { allow-empty-ikesa | max-retransmissions | policy error-notification | rekey | setup-timer }

no ikev2-ikesa { allow-empty-ikesa | policy { error-notification | use-rfc5996-notification } | rekey | transform-set list }

default
  Restores the selected keyword to its default value.

no
  Disables a previously enabled parameter.
```
allow-empty-ikesa
Default is not to allow-empty-ikesa. Activate to have the IKEv2 stack keep the IKE SA when all the Child SAs have been deleted.

max-retransmissions number
Specifies the maximum number of retransmissions of an IKEv2 IKE exchange request if a response has not been received.
number must be an integer from 1 to 8.
Default: 5

policy { error-notification | use-rfc5996-notification }
Notifies error policy.
error-notification: Error Notify Messages will be sent to MS for Invalid IKEv2 Exchange Message ID and Invalid IKEv2 Exchange Syntax for the IKE_SA_INIT Exchange.
use-rfc5996-notification: Enables sending and receive processing for RFC 5996 notifications - TEMPORARY_FAILURE and CHILD_SA_NOT_FOUND.

rekey [ disallow-param-change ]
Specifies if IKESA rekeying should occur before the configured lifetime expires (at approximately 90% of the lifetime interval).
Default is not to re-key.
The disallow-param-change option prevents changes in negotiation parameters during rekey.

retransmission-timeout msec
Specifies the timeout period in milliseconds before a retransmission of an IKEv2 IKE exchange request is sent (if the corresponding response has not been received).
msec must be an integer from 300 to 15000.
Default: 500

setup-timer sec
Specifies the number of seconds before an IKEv2 IKE Security Association that is not fully established is terminated.
sec must be an integer from 16 to 3600.
Default: 60

transform-set list name
A space-separated list of context-level configured IKEv2 IKE Security Association transform sets to be used for deriving IKEv2 IKE Security Associations from this crypto map.
name must be an existing IKEv2 IKESA Transform Set expressed as an alphanumeric string of 1 through 127 characters. A minimum of one transform set is required; maximum configurable is six.

Usage
Use this command to configure parameters for the IKEv2 IKE Security Associations within this crypto map.

Example
The following command configures the maximum number of IKEv2 IKESA request retransmissions to 7:

ikev2-ikesa max-retransmissions 7
keepalive

Configures keepalive or dead peer detection for security associations used within this crypto template.

Product

ePDG
FA
GGSN
HA
HeNBGW
HNBGW
HSGW
MME
P-GW
PDSN
S-GW
SAEGW
SCM
SecGW
SGSN

Privilege

Security Administrator, Administrator

Syntax

keepalive [ interval sec ]
default keepalive [ interval ]
no keepalive

no
Disables keepalive messaging.

interval sec
Specifies the amount of time (in seconds) that must elapse before the next keepalive request is sent. sec must be an integer from 10 through 3600. Default: 10

Usage

Use this command to set parameters associated with determining the availability of peer servers.

Example

The following command sets a keepalive interval to three minutes (180 seconds):

```
keepalive interval 180
```
**match**

Matches or associates the crypto map to an access control list (ACL) configured in the same context.

**Product**
- ePDG
- FA
- GGSN
- HA
- HeNBGW
- HNBGW
- HSGW
- MME
- P-GW
- PDSN
- S-GW
- SAEGW
- SCM
- SecGW
- SGSN

**Privilege**
Security Administrator

**Syntax**

```
match address acl_name [ priority ]
```

```
no match address
```

**no**
Removes a previously matched ACL.

```
match address acl_name
```

Specifies The name of the ACL with which the crypto map is to be matched. `acl_name` is an alphanumeric string of 1 through 79 characters that is case sensitive.

```
priority
```

Specifies the preference of the ACL as integer from 0 through 4294967295. 0 is the highest priority. Default: 0
The ACL preference is factored when a single packet matches the criteria of more than one ACL.

**Important:** The priorities are only compared for ACLs matched to other crypto maps or to policy ACLs (those applied to the entire context).
Usage

ACLs matched to crypto maps are referred to as crypto ACLs. Crypto ACLs define the criteria that must be met in order for a subscriber data packet to routed over an IPSec tunnel. Prior to routing, the system examines the properties of each subscriber data packet. If the packet properties match the criteria specified in the crypto ACL, the system will initiate the IPSec policy dictated by the crypto map.

Example

The following command sets the crypto map ACL to the ACL named acl-list1 and sets the crypto maps priority to the highest level.

```plaintext
match address acl-list1 0
```
**ocsp**

Enables use of Online Certificate Status Protocol (OCSP) from a crypto template. OCSP provides a facility to obtain timely information on the status of a certificate.

**Product**

All products supporting IPSec

**Important:** This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

**Privilege**

Security Administrator

**Syntax**

```
ocsp [ nonce | responder-address ipv4_address [ port port_value ] ]
no ocsp [ nonce | responder-address [ port ] ]
default ocsp [ nonce ]
```

**no**

Disables the use of OCSP.

**default**

Sets / Restores default value assigned for ocsp nonce.

**nonce**

Enables sending nonce (unique identifier) in OCSP requests.

**responder-address ipv4_address**

Configures the OCSP responder address (IPv4), used when absent in peer (device) certificate. `ipv4_address` is an IPv4 address specified in dotted decimal format.

**port port_value**

Configures the port for OCSP responder. `port_value` is an integer value between 1 and 65535. The default port is 8889.

**Usage**

This command enables the use of Online Certificate Protocol (OCSP) from a crypto map/template. OCSP provides a facility to obtain timely information on the status of a certificate. OCSP messages are exchanged between a gateway and an OCSP responder during a certificate transaction. The responder immediately provides the status of the presented certificate. The status can be good, revoked or unknown. The gateway can then proceed based on the response.

**Example**
ocsp
payload

Creates a new, or specifies an existing, crypto template payload and enters the Crypto Template Payload Configuration Mode.

Product

ePDG
FA
GGSN
HA
HeNBGW
HNBGW
HSGW
MME
P-GW
PDSN
S-GW
SAEGW
SCM
SecGW
SGSN

Privilege

Security Administrator

Syntax

payload name match ipv6

no payload name

payload name

Specifies the name of a new or existing crypto template payload as an alphanumeric string of 1 through 127 characters.

match ipv6

Filters IPSec IPv6 Child Security Association creation requests for subscriber calls using this payload. Further filtering can be performed by applying the following:

Usage

Use this command to create a new or enter an existing crypto template payload. The payload mechanism is a means of associating parameters for the Security Association (SA) being negotiated. Two payloads are required: one each for MIP and IKEv2. The first payload is used for establishing the initial Child SA Tunnel Inner Address (TIA) which will be torn down. The second payload is used for establishing
the remaining Child SAs. Note that if there is no second payload defined with home-address as the `ip-address-allocation` then no MIP call can be established, just a Simple IP call. Currently, the only available match is for ChildSA, although other matches are planned for future releases. Entering this command results in the following prompt:

```
[ctxt_name]hostname(cfg-crypto-<name>-ikev2-tunnel-payload)#
```

Crypto Template IKEv2-IPv6 Payload Configuration Mode commands are defined in the Crypto Template IKEv2-IPv6 Payload Configuration Mode Commands chapter.

**Example**

The following command configures a crypto template payload called `payload5` and enters the Crypto Template IKEv2-IPv6 Payload Configuration Mode:

```
payload payload5 match ipv6
```
peer

Configures the IP address of a peer IPSec server.

Product

- ePDG
- FA
- GGSN
- HA
- HeNBGW
- HNBGW
- HSGW
- MME
- P-GW
- PDSN
- S-GW
- SAEGW
- SCM
- SecGW
- SGSN

Privilege

Security Administrator

Syntax

- `peer ip_address`
- `no peer`

  **no**
  Removes the configured peer server IP address.

  **peer ip_address**
  Specifies the IP address of a peer IPSec server in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

Usage

Use this command to specify a peer IPsec peer server. The IPsec peer server can also be the Lawful Intercept server.

Example

The following command configures the system to recognize an IPsec peer server with an IPv6 address of `fe80::200:f8ff:fe21:67cf`. 
peer fe80::200:ff:fe21:67cf
remote-secret-list

Enables the use of a Remote Secret List containing up to 1000 pre-shared keys.

**Product**
All Security Gateway products

**Important:** This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

**Privilege**
Security Administrator

**Syntax**

```
remote-secret-list list_name
```

```
no remote-secret-list
```

```
no
```

Disables use of a Remote Secret List.

```
list_name
```

Specifies the name of an existing Remote Secret List as an alphanumeric string of 1 through 127 characters.

**Usage**
Enable the use of a Remote Secret List containing up to 1000 pre-shared keys. Only one active remote-secret-list is supported per system. For additional information, refer to the Remote Secret List Configuration Commands chapter of the Command Line Interface Reference and the System Administration Guide.

**Example**
The following command enables a remote-secret-list named rs-list:

```
remote-secret-list rs-list
```
**whitelist**

Enables or disables a whitelist (access granted) for this crypto map.

**Product**

All products supporting IPSec whitelisting

---

**Important:** This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

**Privilege**

Security Administrator

**Syntax**

```
whitelist
```

```
no whitelist
```

```
no
```

Disables whitelisting for this crypto map. By default whitelisting is disabled.

**Usage**

Use this command to enable whitelisting for this crypto map. A whitelist is a list or register of entities that are being provided a particular privilege, service, mobility, access or recognition. With whitelisting, no peer is allowed to connect unless it appears in the list. For additional information on whitelisting, refer to the *System Administration Guide*.

**Example**

The following command enables whitelisting:

```
whitelist
```
Chapter 62
Crypto Map IKEv2-IPv6 Payload Configuration Mode
Commands

The Crypto Map IKEv2-IPv6 Payload Configuration Mode is used to assign the correct IPSec transform-set from a list of up to four different transform-sets, and to assign Mobile IP addresses.

Mode

Exec > Global Configuration > Context Configuration > Crypto Map IKEv2-IPv6 Configuration > Crypto Map IKEv2-IPv6 Payload Configuration

configure > context context_name > crypto map map_name ikev2-ipv6 > payload payload_name match ipv6

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-crypto-map-ikev2-ipv6-payload)#

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Use this command to return to the parent configuration mode.
ipsec

Configures the IPSec transform set to be used for this crypto template payload.

Product

ePDG
FA
GGSN
HA
HeNBGW
HNBGW
HSGW
MME
P-GW
PDSN
S-GW
SAEGW
SCM
SecGW
SGSN

Privilege

Security Administrator

Mode

Exec > Global Configuration > Context Configuration > Crypto Map IKEv2-IPv6 Configuration > Crypto Map IKEv2-IPv6 Payload Configuration

`configure > context context_name > crypto map map_name ikev2-ipv6 > payload payload_name match ipv6`

Entering the above command sequence results in the following prompt:

`[context_name]host_name(cfg-crypto-ikev2-ipv6-payload)#`

Syntax

`ipsec transform-set list name`

`no ipsec transform-set list`

`ipsec transform-set list name`

Specifies the context configured IPSec transform set name to be used in the crypto template payload. This is a space-separated list. From 1 to 4 transform sets can be entered. `name` is an alphanumeric string of 1 through 127 characters.
**Usage**

Use this command to list the IPSec transform set(s) to use in this crypto template payload.

**Example**

The following command configures IPSec transform sets named `ipset1` and `ipset2` to be used in this crypto template payload:

```
ipsec transform-set list ipset1 ipset2```

**lifetime**

Configures the number of seconds and/or kilobytes for IPSec Child SAs derived from this crypto template payload to exist.

**Product**

ePDG
FA
GGSN
HA
HeNBGW
HNBGW
HSGW
MME
P-GW
PDSN
S-GW
SAEGW
SCM
SecGW
SGSN

**Privilege**

Administrator

**Mode**

Exec > Global Configuration > Context Configuration > Crypto Map IKEv2-IPv6 Configuration > Crypto Map IKEv2-IPv6 Payload Configuration

```
configure > context context_name > crypto map map_name ikev2-ipv6 > payload payload_name
match ipv6
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-crypto-ikev2-ipv6-payload) #
```

**Syntax**

```
lifetime { sec [ kilo-bytes kbytes ] | kilobytes kbytes }

default lifetime
```

```
default
```

Returns the lifetime value to the default setting of 86400 seconds.
sec
Specifies the number of seconds for IPSec Child Security Associations derived from this crypto template payload to exist. sec must be an integer from 60 through 604800. Default: 86400

kilo-bytes  kbytes
Specifies lifetime in kilobytes for IPSec Child Security Associations derived from this Crypto Map. kbytes must be an integer from 1 through 2147483648.

Usage
Use this command to configure the number of seconds and/or kilobytes for IPSec Child Security Associations derived from this crypto template payload to exist.

Example
The following command configures the IPSec child SA lifetime to be 120 seconds:

    lifetime 120
rekey

Configures child security association rekeying.

Product
- ePDG
- FA
- GGSN
- HA
- HeNBGW
- HNBGW
- HSGW
- MME
- P-GW
- PDSN
- S-GW
- SAEGW
- SCM
- SecGW
- SGSN

Privilege
Security Administrator

Mode
Exec > Global Configuration > Context Configuration > Crypto Map IKEv2-IPv6 Configuration > Crypto Map IKEv2-IPv6 Payload Configuration

configure > context context_name > crypto map map_name ikev2-ipv6 > payload payload_name
match ipv6

Entering the above command sequence results in the following prompt:

[context_name]host_name(cfg-crypto-ikev2-ipv6-payload)#

Syntax

rekey [ keepalive ]
[ default | no ] rekey

default
Returns the feature to the default setting of disabled.

no
Disables this feature.
keepalive

If specified, a session will be rekeyed even if there has been no data exchanged since the last rekeying operation. By default rekeying is only performed if there has been data exchanged since the previous rekey.

Usage

Use this command to enable or disable the ability to rekey IPSec Child SAs after approximately 90% of the Child SA lifetime has expired. The default, and recommended setting, is not to perform rekeying. No rekeying means the P-GW will not originate rekeying operations and will not process CHILD SA rekeying requests from the MS.

Example

The following command disables rekeying:

    no rekey
Chapter 63
Crypto Map IPSec Dynamic Configuration Mode
Commands

The Crypto Map IPSec Dynamic Configuration Mode is used to configure IPSec tunnels that are created as needed to facilitate subscriber sessions using Mobile IP or L2TP.

Modification(s) to an existing dynamic crypto map configuration will not take effect until the related security association has been cleared. Refer to the description of the `clear crypto security-association` command in the `Exec Mode Commands` chapter for more information.

Mode

```
Exec > Global Configuration > Context Configuration > Crypto Map Dynamic Configuration
configure > context context_name > crypto map policy_name ipsec-dynamic
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-crypto-dynamic-map)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**
Use this command to return to the parent configuration mode.
set

Configures parameters for the dynamic crypto map.

Product

ePDG
FA
GGSN
HA
HeNBGW
HNBGW
HSGW
MME
P-GW
PDSN
S-GW
SAEGW
SCM
SecGW
SGSN

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > Context Configuration > Crypto Map Dynamic Configuration
configure > context context_name > crypto map policy_name ipsec-dynamic

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-crypto-dynamic-map)#

Syntax

set { control-dont-fragment { clear-bit | copy-bit | set-bit } | isakmp natt
[keepalive time ] | pfs { group1 | group2 | group5 } | phase1-idtype { id-key-id |
ipv4-address } [ mode { aggressive | main } ] | phase2-idtype { ipv4-address |
ipv4-address-subnet } | security-association lifetime { keepalive | kilo-bytes
kbytes | seconds secs } | transform-set transform_name [ transform-set
transform_name2 ... transform-set transform_name6 ]
}

no set { pfs | security-association lifetime { keepalive | kilo-bytes | seconds } |
phase1-idtype | phase2-idtype | transform-set transform_name [ transform-set
transform_name2 ... transform-set transform_name6 ]
}

no

Deletes the specified parameter or resets the specified parameter to the default value.
control-dont-fragment { clear-bit | copy-bit | set-bit }

Controls the don’t fragment (DF) bit in the outer IP header of the IPSec tunnel data packet. Options are:
- clear-bit: Clears the DF bit from the outer IP header (sets it to 0).
- copy-bit: Copies the DF bit from the inner IP header to the outer IP header. This is the default action.
- set-bit: Sets the DF bit in the outer IP header (sets it to 1).

isakmp natt [keepalive time ]

Enable IPSec NAT Traversal.
keepalive time: The time to keep the NAT connection alive in seconds. time must be an integer of from 1 through 3600.

pfs { group1 | group2 | group5 }

Specifies the modp Oakley group (also known as the Diffie-Hellman [D-H] group) that is used to determine the length of the base prime numbers that are used for Perfect Forward Secrecy (PFS).
- group1: Diffie-Hellman Group1 (768-bit modp)
- group2: Diffie-Hellman Group2 (1024-bit modp)
- group5: Diffie-Hellman Group5 (1536-bit modp)

phasel-idtype { id-key-id | ipv4-address } [ mode { aggressive | main } ]

Sets the IKE negotiations Phase 1 payload identifier.
Default: ipv4-address
id-key-id: Use ID_KEY_ID as the Phase 1 payload identifier.
ipv4-address: Use IPV4_ADDR as the Phase 1 payload identifier.
mode { aggressive | main }: Specify the IKE mode.

phase2-idtype { ipv4-address | ipv4-address-subnet }

Sets the IKE negotiations Phase 2 payload identifier.
Default: ipv4-address-subnet
ipv4-address: Use IPV4_ADDR as the Phase 2 payload identifier.
ipv4-address-subnet: Use IPV4_ADDR_SUBNET as the Phase 2 payload identifier.

security-association lifetime { keepalive | kilo-bytes kbytes | seconds secs }

Defaults:
- keepalive: Disabled
- kilo-bytes: 4608000 kbytes
- seconds: 28800 seconds

This keyword specifies the parameters that determine the length of time an IKE Security Association (SA) is active when no data is passing through a tunnel. When the lifetime expires, the tunnel is torn down. Whichever parameter is reached first expires the SA lifetime.
- keepalive: The SA lifetime expires only when a keepalive message is not responded to by the far end.
- kilo-bytes: This specifies the amount of data in kilobytes to allow through the tunnel before the SA lifetime expires; entered as an integer from 2560 through 4294967294.
- **seconds**: The number of seconds to wait before the SA lifetime expires; entered as an integer from 1200 through 86400.

**Important**: If the dynamic crypto map is being used in conjunction with Mobile IP and the Mobile IP renewal timer is less than the crypto map’s SA lifetime (either in terms of kilobytes or seconds), then the **keepalive** parameter must be configured.

```
transform-set transform_name [ transform-set transform_name2 ... transform-set transform_name6 ]
```

Specifies the name of a transform set configured in the same context that will be associated with the crypto map. Refer to the command `crypto ipsec transform-set` for information on creating transform sets. You can repeat this keyword up to 6 times on the command line to specify multiple transform sets. `transform_name` is the name of the transform set entered as an alphanumeric string from 1 through 127 characters that is case sensitive.

**Usage**

Use this command to set parameters for a dynamic crypto map.

**Example**

The following command sets the PFS group to Group1:

```
set pfs group1
```

The following command sets the SA lifetime to 50000 KB:

```
set security-association lifetime kilo-bytes 50000
```

The following command sets the SA lifetime to 10000 seconds:

```
set security-association lifetime seconds 10000
```

The following command enables the SA to re-key when the tunnel lifetime expires:

```
set security-association lifetime keepalive
```

The following command defines transform sets `tset1` and `tset2`:

```
set transform-set tset1 transform-set tset2
```
Chapter 64
Crypto Map IPSec IKEv1 Configuration Mode Commands

The Crypto Map IPSec IKEv1 Configuration Mode is used to configure properties for IPSec tunnels that will be created using the Internet Key Exchange (IKE) that operates within the framework of the Internet Key Exchange version 1 (IKEv1).

Modification(s) to an existing IKEv1 crypto map configuration will not take effect until the related security association has been cleared. Refer to the description of the clear crypto security-association command in the Exec Mode Commands chapter for more information.

Mode

Exec > Global Configuration > Context Configuration > Crypto Map IPSec IKEv1 Configuration

configure > context context_name > crypto map policy_name ipsec-ikev1

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-crypto-map)#

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
end

**Usage**
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
exit
```

Usage
Use this command to return to the parent configuration mode.
match address

Matches or associates the crypto map to an access control list (ACL) configured in the same context.

Product
- ePDG
- FA
- GGSN
- HA
- HeNBGW
- HNBGW
- HSGW
- MME
- P-GW
- PDSN
- S-GW
- SAEGW
- SCM
- SecGW
- SGSN

Privilege
Security Administrator

Mode
Exec > Global Configuration > Context Configuration > Crypto Map IPSec IKEv1 Configuration

```
configure > context context_name > crypto map policy_name ipsec-ikev1
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-crypto-map)#
```

Syntax

```
[ no ] match address acl_name priority
```

- **no**
  
  Removes a previously matched ACL.

```
match address acl_name
```

Specifies the name of the ACL with which the crypto map is to be matched as an alphanumeric string of 1 through 79 characters that is case sensitive.
priority

Specifies the preference of the ACL. The ACL preference is factored when a single packet matches the criteria of more than one ACL.
The preference is an integer value from 0 to 4294967295; 0 is the highest priority. Default: 0

Important: The priorities are only compared for ACLs matched to other crypto maps or to policy ACLs (those applied to the entire context).

Usage

ACLs matched to crypto maps are referred to as crypto ACLs. Crypto ACLs define the criteria that must be met in order for a subscriber data packet to routed over an IPSec tunnel.
Prior to routing, the system examines the properties of each subscriber data packet. If the packet properties match the criteria specified in the crypto ACL, the system will initiate the IPSec policy dictated by the crypto map.

Example

The following command sets the crypto map ACL to the ACL named ACLlist1 and sets the crypto maps priority to the highest level.

```
match address ACLlist1 0
```
match crypto group

Matches or associates the crypto map a crypto group configured in the same context.

Product
- ePDG
- FA
- GGSN
- HA
- HeNBGW
- HNBGW
- HSGW
- MME
- P-GW
- PDSN
- S-GW
- SAEGW
- SCM
- SecGW
- SGSN

Privilege
Security Administrator

Mode
Exec > Global Configuration > Context Configuration > Crypto Map IPSec IKEv1 Configuration

configure > context context_name > crypto map policy_name ipsec-ikev1

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-crypto-map)#

Syntax

[ no ] match crypto group  group_name { primary | secondary }

no

Deletes a previously configured crypto group association.

match crypto group  group_name

Specifies the name of the crypto group entered as an alphanumeric string of 1 through 127 characters that is case sensitive.
primary
Specifies that the policies configured as part of this crypto map will be used for the primary tunnel in the Redundant IPSec Tunnel Failover feature.

secondary
Specifies that the policies configured as part of this crypto map will be used for the secondary tunnel in the Redundant IPSec Tunnel Failover feature.

Usage
Use this command to dictate the primary and secondary tunnel policies used for the Redundant IPSec Tunnel Failover feature.
At least two policies must be configured to use this feature. One policy must be configured as the primary, the other as the secondary.

Example
The following command associates the crypto map to a crypto group called group1 and dictates that it will serve as the primary tunnel policy:

    match crypto group group1 primary
match ip pool

Matches the specified IP pool to the current IKEv1 crypto map. This command can be used multiple times to change more than one IP pool.

**Important:** The `match ip pool` command is not supported on the ASR 5500 platform.

**Product**
- ePDG
- FA
- GGSN
- HA
- HeNBGW
- HNBTGW
- HSGW
- MME
- P-GW
- PDSN
- S-GW
- SAEGW
- SCM
- SecGW
- SGSN

**Privilege**
- Security Administrator

**Mode**
- Exec > Global Configuration > Context Configuration > Crypto Map IPSec IKEv1 Configuration
- `configure > context context_name > crypto map policy_name ipsec-ikev1`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-crypto-map)#
```

**Syntax**

```
[ no ] match ip pool pool-name pool_name[ destination-network ip_address { / mask | mask ip_mask } ]
```

- `no`

Delete the matching statement for the specified IP pool from the crypto map.
match ip pool pool-name pool_name

Specifies the name of an existing IP pool that should be matched as an alphanumeric string of 1 through 31 characters.

destination-network ip_address { / mask | mask ip_mask }

Specifies the IP address of the destination network in IPv4 dotted-decimal notation.

/ mask specifies the subnet mask bits (representing the subnet mask) and must be an integer from 1 to 32 (CIDR notation). This variable must be entered in the IPv4 dotted-decimal notation/subnet bits format (for example, 10.1.1.1/24).

mask ip_mask specifies the subnet mask in dotted decimal notation.

An IP pool attached to the crypto map can have multiple IPSec tunnels according to the destination of the packet being forwarded to internet.

**Important:** Each invocation of this command will add another destination network to the IP pool, with a maximum of eight destination networks per crypto map.

**Usage**

Use this command to set the names of IP pools that should be matched in the current crypto map.

**Important:** If an IP address pool that is matched to a IKEv1 crypto map is resized, removed, or added, the corresponding security association must be cleared in order for the change to take effect. Refer to the `clear crypto` command in the Exec mode for information on clearing security associations.

**Example**

The following command sets a rule for the current crypto map that will match an IP pool named `ippool1`:

```
   match ip pool pool-name ippool1
```
set

Configures parameters for the dynamic crypto map.

Product

ePDG
FA
GGSN
HA
HeNBGW
HNBGW
HSGW
MME
P-GW
PDSN
S-GW
SAEGW
SCM
SecGW
SGSN

Privilege

Security Administrator

Mode

Exec > Global Configuration > Context Configuration > Crypto Map IPSec IKEv1 Configuration

configure > context context_name > crypto map policy_name ipsec-ikev1

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-crypto-map)#

Syntax

set { control-dont-fragment { clear-bit | copy-bit | set-bit } | ikev1 natt [ keepalive time ] | pfs { group1 | group2 | group5 } | phasel-idtype { id-key-id | ipv4-address [ mode { aggressive | main } ] | phase2-idtype { ipv4-address | ipv4-address-subnet } | security-association lifetime { disable-phase2-rekey | keepalive | kilo-bytes kbytes | seconds secs } transform-set transform_name [ transform-set transform_name2 ... transform-set transform_name6 ]

no set { ikev1 natt | pfs | phasel-idtype | phase2-idtype | security-association lifetime { disable-phase2-rekey | keepalive | kilo-bytes | seconds } | transform-set transform_name [ transform-set transform_name2 ... transform-set transform_name6 ]

set control-dont-fragment { clear-bit | copy-bit | set-bit }

Controls the don’t fragment (DF) bit in the outer IP header of the IPsec tunnel data packet. Options are:
set clear-bit: Clears the DF bit from the outer IP header (sets it to 0).
set copy-bit: Copies the DF bit from the inner IP header to the outer IP header. This is the default action.
set set-bit: Sets the DF bit in the outer IP header (sets it to 1).

set ikev1 natt [ keepalive time ]
Specifies IKE parameters.
  natt: Enables IPSec NAT Traversal.
  keepalive time: The time to keep the NAT connection alive in seconds. time must be an integer of from 1 through 3600.

set pfs { group1 | group2 | group5 }
Specifies the modp Oakley group (also known as the Diffie-Hellman [D-H] group) that is used to determine the length of the base prime numbers that are used for Perfect Forward Secrecy (PFS).
  group1: Diffie-Hellman Group1 (768-bit modp)
  group2: Diffie-Hellman Group2 (1024-bit modp)
  group5: Diffie-Hellman Group5 (1536-bit modp)

set phase1-idtype { id-key-id | ipv4-address [ mode { aggressive | main } ] }
Sets the IKE negotiations Phase 1 payload identifier. Default: id-key-id
  id-key-id: ID KEY ID
  ipv4-address: ID IPV4 Address
  mode: Configures IKE mode
    aggressive: IKE negotiation mode: AGGRESSIVE
    main: IKE negotiation mode: MAIN

set phase2-idtype { ipv4-address | ipv4-address-subnet }
Sets the IKE negotiations Phase 2 payload identifier.
Default: ipv4-address-subnet
  ipv4-address: Use IPV4_ADDR as the Phase 2 payload identifier.
  ipv4-address-subnet: Use IPV4_ADDR_SUBNET as the Phase 2 payload identifier.

set security-association lifetime { disable-phase2-rekey | keepalive | kilo-bytes kbytes | seconds secs }
Defaults:
  disable-phase2-rekey: Rekeying is enabled by default
  keepalive: Disabled
  kilo-bytes: 4608000 kbytes
  seconds: 28800 seconds
Specifies the parameters that determine the length of time an IKE Security Association (SA) is active when no data is passing through a tunnel. When the lifetime expires, the tunnel is torn down. Whichever parameter is reached first expires the SA lifetime.
  disable-phase2-rekey: If this keyword is specified, the Phase2 SA is not rekeyed when the lifetime expires.
  keepalive: The SA lifetime expires only when a keepalive message is not responded to by the far end.
**set**

- **kilo-bytes**: This specifies the amount of data (n kilobytes) to allow through the tunnel before the SA lifetime expires. *kbytes* must be an integer from 2560 through 4294967294.

- **set seconds**: The number of seconds to wait before the SA lifetime expires. *secs* must be an integer from 1200 through 86400.

**Important**: If the dynamic crypto map is being used in conjunction with Mobile IP and the Mobile IP renewal timer is less than the crypto map’s SA lifetime (either in terms of kilobytes or seconds), then the keepalive parameter must be configured.

```
transform-set transform_name [ transform-set transform_name2 ... transform-set transform_name6 ]
```

Specifies the name of a transform set configured in the same context that will be associated with the crypto map. Refer to the command `crypto ipsec transform-set` for information on creating transform sets. You can repeat this keyword up to 6 times on the command line to specify multiple transform sets. *transform_name* is the name of the transform set entered as an alphanumeric string of 1 through 127 characters that is case sensitive.

**no**

 Deletes the specified parameter or resets the specified parameter to the default value.

**Usage**

Use this command to set parameters for a dynamic crypto map.

**Example**

The following command sets the PFS group to Group1:

```
set pfs group1
```

The following command sets the SA lifetime to 50000 KB:

```
set security-association lifetime kilo-bytes 50000
```

The following command sets the SA lifetime to 10000 seconds:

```
set security-association lifetime seconds 10000
```

The following command enables the SA to re-key when the tunnel lifetime expires:

```
set security-association lifetime keepalive
```

The following command defines transform sets *tset1* and *tset2*.

```
set transform-set tset1 transform-set tset2
```
Chapter 65
Crypto Map IPSec Manual Configuration Mode Commands

The Crypto IPSec Map Manual Configuration Mode is used to configure static IPSec tunnel properties. Modification(s) to an existing crypto map manual configuration will not take effect until the related security association has been cleared. Refer to the description of the `clear crypto security-association` command in the *Exec Mode Commands* chapter for more information.

**Important:** Because manual crypto map configurations require the use of static security keys (associations), they are not as secure as crypto maps that rely on dynamically configured keys. Therefore, they only be used for testing purposes.

Mode

`Exec > Global Configuration > Context Configuration > Crypto Map Manual Configuration`

`configure > context context_name > crypto map map_name map_number ipsec-manual`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-crypto-manual-map) #
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

`end`

**Usage**
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
```
exit
```

**Usage**
Use this command to return to the parent configuration mode.
**match address**

Matches or associates the crypto map to an access control list (ACL) configured in the same context.

**Product**
- ePDG
- FA
- GGSN
- HA
- HeNBGW
- HNBGW
- HSGW
- MME
- P-GW
- PDSN
- S-GW
- SAEGW
- SCM
- SecGW
- SGSN

**Privilege**
- Security Administrator

**Mode**
- Exec > Global Configuration > Context Configuration > Crypto Map Manual Configuration

```bash
configure > context context_name > crypto map map_name map_number ipsec-manual
```

Entering the above command sequence results in the following prompt:

```
[context_name] host_name(config-crypto-manual-map)#
```

**Syntax**

```
[ no ] match address acl_name [ priority ]
```

**no**

Removes a previously matched ACL.

```
match address acl_name
```

Specifies the name of the ACL with which the crypto map is to be matched. `acl_name` is an alphanumeric string of 1 through 47 characters that is case sensitive.
priority

Specifies the preference of the ACL. The ACL preference is factored when a single packet matches the criteria of more than one ACL. `priority` is an integer from 0 through 4294967295. 0 is the highest priority. Default: 0

**Important:** The priorities are only compared for ACLs matched to other crypto maps or to policy ACLs (those applied to the entire context).

**Usage**

ACLs matched to crypto maps are referred to as crypto ACLs. Crypto ACLs define the criteria that must be met in order for a subscriber data packet to routed over an IPSec tunnel. Prior to routing, the system examines the properties of each subscriber data packet. If the packet properties match the criteria specified in the crypto ACL, the system will initiate the IPSec policy dictated by the crypto map.

**Example**

The following command sets the crypto map ACL to the ACL named `ACLlist1` and sets the crypto maps priority to the highest level.

```
match address ACLlist1 0
```
**set control-dont-fragment**

Controls the Don’t Fragment (DF) bit in the outer IP header of the IPSec tunnel data packet.

**Product**
- ePDG
- FA
- GGSN
- HA
- HeNBGW
- HNBGW
- HSGW
- MME
- P-GW
- PDSN
- S-GW
- SAEGW
- SCM
- SecGW
- SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Crypto Map Manual Configuration

```
configure > context context_name > crypto map map_name map_number ipsec-manual
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-crypto-manual-map)#
```

**Syntax**

```
set control-dont-fragment { clear-bit | copy-bit | set-bit }

default set control-dont-fragment { clear-bit | copy-bit | set-bit }
```

**default**
Sets or restores default value assigned to a specified parameter.

```
set control-dont-fragment clear-bit
```

Clears the DF bit from the outer IP header (sets it to 0).
set control-dont-fragment

copy-bit

Copies the DF bit from the inner IP header to the outer IP header. This is the default action.

set control-dont-fragment set-bit

Sets the DF bit in the outer IP header (sets it to 1).

Usage

Use this command to clear, copy, or set the don’t fragment (DF) bit in the outer IP header of the IPSec tunnel data packet.

Example

The following command sets the DF bit in the outer IP header.

```
set control-dont-fragment set-bit
```
set peer

Configures the IP address of the peer security gateway that the system will establish the IPSec tunnel with.

**Product**
- ePDG
- FA
- GGSN
- HA
- HeNBGW
- HNBGW
- HSGW
- MME
- P-GW
- PDSN
- S-GW
- SAEGW
- SCM
- SecGW
- SGSN

**Privilege**
- Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Crypto Map Manual Configuration

```
configure > context context_name > crypto map map_name map_number ipsec-manual
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-crypto-manual-map)#
```

**Syntax**

```
[ no ] set peer gw_address
```

- **no**
  Removes a previously configured peer address.

```
set peer gw_address
```

Specifies the IP address of the peer security gateway with which the IPSec tunnel will be established.

**Usage**

Once the manual crypto map is fully configured and applied to an interface, the system will establish an IPSec tunnel with the security gateway specified by this command.
Because the tunnel relies on statically configured parameters, once created, it never expires; it exists until its configuration is deleted.

**Example**

The following command configures a security gateway address of **192.168.1.100** for the crypto map with which to establish a tunnel.

```
set peer 192.168.1.100
```
set session-key

Configures session key parameters for the manual crypto map.

Product
- ePDG
- FA
- GGSN
- HA
- HeNBGW
- HNBGW
- HSGW
- MME
- P-GW
- PDSN
- S-GW
- SAEGW
- SCM
- SecGW
- SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Crypto Map Manual Configuration

configure > context context_name > crypto map map_name map_number ipsec-manual

Entering the above command sequence results in the following prompt:

[context_name] host_name(config-crypto-manual-map)#

Syntax

set session-key { inbound | outbound } { ah ah_spi { encrypted ] key ah_key | esp
esp_spi { encrypted } cipher encryption_key { encrypted } authenticator auth_key }
no set session-key { inbound | outbound }

no
Removes previously configured session key information.

inbound
Specifies that the key(s) will be used for tunnels carrying data sent by the security gateway.

outbound
Specifies that the key(s) will be used for tunnels carrying data sent by the system.
ah  ah_spi
Configures the Security Parameter Index (SPI) for the Authentication Header (AH) protocol. The SPI is used to identify the AH security association (SA) between the system and the security gateway. ah_spi is an integer from 256 through 4294967295.

encrypted
Indicates the key provided is encrypted. The encrypted keyword is intended only for use by the system while saving configuration scripts. The system displays the encrypted keyword in the configuration file as a flag that the variable following the key, cipher, and/or authenticator keyword is the encrypted version of the plain text key. Only the encrypted key is saved as part of the configuration file.

key  ah_key
Configures the key used by the system to de/encapsulate IP packets using Authentication Header (AH) protocol. ah_key must be entered as either an alphanumeric string or a hexadecimal number beginning with “0x”. The length of the configured key must match the configured algorithm.

esp  esp_spi
Configures SPI for the Encapsulating Security Payload (ESP) protocol. The SPI is used to identify the ESP security association (SA) between the system and the security gateway. esp_spi is an integer from 256 through 4294967295. The length of the configured key must match the configured algorithm.

cipher  encryption_key
Specifies the key used by the system to de/encrypt the payloads of IP packets using the ESP protocol. encryption_key must be entered as either an alphanumeric string or a hexadecimal number beginning with “0x”. The length of the configured key must match the configured algorithm.

authenticator  auth_key
Specifies the key used by the system to authenticate the IP packets once encryption has been performed. auth_key must be entered as either an alphanumeric string or a hexadecimal number beginning with “0x”. The length of the configured key must match the configured algorithm.

Usage
Manual crypto maps rely on the use of statically configured keys to establish IPSec tunnels. This command allows the configuration of the static keys. Identical keys must be configured on both the system and the security gateway in order for the tunnel to be established. The length of the configured key must match the configured algorithm. This command can be entered up to two time for the same crypto map: once to configure inbound key properties, and once to configure outbound key properties.

Example
The following command configures a manual crypto map with the following session key properties:

- Keys are for tunnels initiated by the system to the security gateway.
- ESP will be used with an SPI of 310.
- Encryption key is \textit{sd23r9skd0fi3as}.
- Authentication key is \textit{sfd23408imi9yn}.

```
set session-key outbound esp 310 cipher sd23r9skd0fi3as authenticator sfd23408imi9yn
```
set transform-set

Configures the name of a transform set that the crypto map is associated with.

Product
- ePDG
- FA
- GGSN
- HA
- HeNBGW
- HNBGW
- HSGW
- MME
- P-GW
- PDSN
- S-GW
- SAEGW
- SCM
- SecGW
- SGSN

Privilege
- Security Administrator, Administrator

Mode
- Exec > Global Configuration > Context Configuration > Crypto Map Manual Configuration
- configure > context context_name > crypto map map_name map_number ipsec-manual

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-crypto-manual-map)#

Syntax

[ no ] set transform-set transform_name

  no

  Removes a previously configured transform set association.

  set transform-set transform_name

  Specifies the name of the transform set expressed as an alphanumeric string of 1 through 127 characters that is case sensitive.
Usage
System transform sets contain the IPSec policy definitions for crypto maps. Refer to the `crypto ipsec transform-set` command for information on creating transform sets.

**Important:** Transform sets must be configured prior to configuring session key information for the crypto map.

Example
The following command associates a transform set named `esp_tset` with the crypto map:

```
set transform-set esp_tset
```
Chapter 66
Crypto Template Configuration Mode Commands

The Crypto Template Configuration Mode is used to configure an IKEv2 IPSec policy. It includes most of the IPSec parameters and IKEv2 dynamic parameters for cryptographic and authentication algorithms. A security gateway service will not function without a configured crypto template. Only one crypto template can be configured per service.

Mode
Exec > Global Configuration > Context Configuration > Crypto Template Configuration
configure > context context_name > crypto template template_name ikev2-dynamic

Entering the above command sequence results in the following prompt:

[context_name]host_name(crf-crypto-tmpl-ikey2-tunnel)#

Important: Available commands or keywords/variables vary based on platform type, product version, and installed license(s).
allow-cert-enc cert-hash-url

Enables support for a certificate encoding type other than the default. When enabled hash and URL encoding type are supported in CERT and CERTREQ payloads.

Product
Security gateway products

**Important:** This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

Privilege
Security Administrator

Syntax

```
allow-cert-enc cert-hash-url

no allow-cert-enc cert-hash-url
```

**Usage**
Disables support for hash and URL encoding type in CERT and CERTREQ payloads.

Enable support for a certificate encoding type other than the default. When enabled hash and URL encoding type are supported in CERT and CERTREQ payloads.

Example

The following command enables hash and URL encoding type in CERT and CERTREQ payloads:

```
allow-cert-enc cert-hash-url
```
allow-custom-fqdn-idr

Allows non-standard FQDN (Fully Qualified Domain Name) strings in the IDr (Identification - Responder) payload of IKE_AUTH messages received from the UE with the payload type as FQDN.

Product
All services using IKEv2 IPSec

Privilege
Security Administrator

Syntax

allow-custom-fqdn-idr

no allow-custom-fqdn-idr

default allow-custom-fqdn-idr

no

Does not allow non-standard FQDN strings in the IDr payload of IKE_AUTH messages received from the UE with the payload type as FQDN.

default

Restores the default setting, which does not allow non-standard FQDN strings in the IDr payload of IKE_AUTH messages received from the UE with the payload type as FQDN.

You can chain multiple CA-CRLs in a single command instance.

Usage

Use this command to configure the system to skip the syntax check for the IDr payload in IKE_AUTH messages received from the UE with the payload type as FQDN. This allows non-standard FQDN strings such as APN names in the IDr payload.

Example

The following command configures the system to allow non-standard FQDN strings in the IDr payload of IKE_AUTH messages received from the UE with the payload type as FQDN:

allow-custom-fqdn-idr
authentication

Configures the gateway and subscriber authentication methods to be used by this crypto template.

Product
All IPSec-related services

Privilege
Security Administrator

Syntax

```
authentication { eap-profile name [ second-phase eap-profile name ] | local { certificate | pre-shared-key { encrypted key value | key clear_text } | pre-shared-key { encrypted key value | key clear_text [ second-phase eap-profile name ] } | remote { certificate | eap-profile name [ second-phase eap-profile name ] | pre-shared-key { encrypted key value | key clear_text [ second-phase eap-profile name ] } } } } 
```

```
no authentication local { certificate | pre-shared-key }
```

default authentication

default

Returns the command to its default setting.

```
no
```

Removes the authentication parameters from the configuration.

```
eap-profile name [ second-phase eap-profile name ]
```

Specifies that authentication is to be performed using a named Extensible Authentication Protocol (EAP) profile. `name` is an alphanumeric string of 1 through 127 characters. Entering this keyword places the CLI in the EAP Authentication Configuration Mode.

The `second-phase eap-profile name` is only required for installations using multiple authentications. `name` must be an alphanumeric string of 1 through 127 characters.

```
local { certificate | pre-shared-key { encrypted key value | key clear_text } }
```

Specifies the local authentication method required for services using the crypto template.

`certificate`: Specifies that the certificate method of authentication must be used for services using the crypto template.

`pre-shared-key { encrypted key value | key clear_text }`: Specifies that a pre-shared key is to be used for services using the crypto template. `encrypted key value` configures an encrypted pre-shared key used for authentication. `value` must be an alphanumeric string of 16 through 255 characters for releases prior to 15.0, or 15 through 444 characters for release 15.0 and higher. `key clear_text` configures a clear text pre-shared key used for authentication. `clear_text` must be an alphanumeric string of 1 through 255 characters.

```
pre-shared-key { encrypted key value | key clear_text }
```

Specifies that a pre-shared key is to be used for services using the crypto template.
encrypted key value: Specifies that the pre-shared key used for authentication is encrypted. value must be an alphanumeric string of 1 through 255 characters for releases prior to 15.0, or 15 through 444 characters for release 15.0 and higher.

key clear_text: Specifies that the pre-shared key used for authentication is clear text. clear_text must be an alphanumeric string of 1 through 255 characters.

remote { certificate | eap-profile name [ second-phase eap-profile name ] | pre-shared-key { encrypted key value | key clear_text } }

Specifies the remote authentication method required for services using the crypto template.

certificate: Specifies that the certificate method of remote authentication must be used for services using the crypto template.

eap-profile name [ second-phase eap-profile name ]: Specifies that remote authentication is to be performed using a named EAP profile. name must be an alphanumeric string of 1 through 127 characters. Entering this keyword places the CLI in the EAP Authentication Configuration Mode. The second-phase eap-profile name is only required for installations using multiple authentications. name must be an alphanumeric string of 1 through 127 characters.

pre-shared-key { encrypted key value | key clear_text }: Specifies that a pre-shared key is to be used for services using the crypto template. encrypted key value configures an encrypted pre-shared key used for authentication. value must be an alphanumeric string of 1 through 255 characters for releases prior to 15.0, or 15 through 444 characters for release 15.0 and higher. key value configures a clear text pre-shared key used for authentication. clear_text must be an alphanumeric string of 1 through 255 characters.

Usage

Use this command to specify the type of authentication performed for subscribers or gateways attempting to access the service using this crypto template.

Entering the authentication eap-profile command results in the following prompt:

```
[context_name]hostname(cfg-crypto-tmpl-eap-key)#
```

EAP Authentication Configuration Mode commands are defined in the EAP Authentication Configuration Mode Commands chapter.

Example

The following command enables authentication via an EAP profile named eap23 for subscribers using the service with this crypto template:

```
authentication eap-profile eap23
```
blacklist

Enables the use of a blacklist (access denied) file to be used by a security gateway.

**Product**
All products supporting IPSec blacklisting

**Important:** This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

**Privilege**
Security Administrator

**Syntax**

blacklist

no blacklist

no

Disables the use of a blacklist.

**Usage**
Enable the use of a previously created blacklist to deny access to prohibited peers via a security gateway. A blacklist is a list or register of entities that are being denied a particular privilege, service, mobility, access or recognition. With blacklisting, any peer is allowed to connect as long as it does not appear in the list. Each entry in the blacklist file should contain the ID type so that the validation is performed for that ID type. In every entry, the ID type and ID value should be separated by a space. Only DOS and UNIX file formatting are supported. For additional information, refer to the *System Administration Guide*.

**Example**

blacklist
**ca-certificate list**

Used to bind an X.509 Certificate Authority (CA) certificate to a crypto template.

**Product**
All IPSec-related services

**Privilege**
Security Administrator, Administrator

**Syntax**

```
ca-certificate list ca-cert-name name [ ca-cert-name name ]
```

```
no ca-certificate
```

**Usage**

Unbinds the ca-certificate(s) bound to the crypto template.

```
ca-cert-name name
```

Binds the named X.509 Certificate Authority (CA) root certificate to a crypto template. `name` is an alphanumeric string of 1 through 129 characters. You can chain multiple certificates(max 4) in a single command instance.

**Example**

Used to bind an X.509 CA certificate to a template.

Use the following example to add a CA certificate to a list:

```
ca-certificate list CA_list1
```
ca-crl list

Binds one or more Certificate Authority-Certificate Revocation Lists (CA-CRLs) to this crypto template.

Product
All IPSec-related services

Privilege
Security Administrator

Syntax

ca-crl list ca-crl-name name [ ca-crl-name name ] +

no ca-crl

no

Removes the CA-CRL configuration from this template.

ca-crl-name name

Specifies the CA-CRL to associate with this crypto template. name must be the name of an existing CA-CRL expressed as an alphanumeric string of 1 through 129 characters. Multiple lists (max 4) can be configured for a crypto template. You can chain multiple CA-CRLs in a single command instance.

Usage

Use this command to associate a CA-CRL name with this crypto template. CA-CRLs are configured in the Global Configuration Mode. For more information about configuring CA-CRLs, refer to the ca-crl name command in the Global Configuration Mode Commands chapter.

Example

The following example binds CA-CRLs named CRL-5 and CRL-7 to this crypto template:

ca-crl list ca-crl-name CRL-5 ca-crl-name CRL-7
**certificate**

Used to bind a single X.509 trusted certificate to a crypto template.

**Product**
All IPSec-related services

**Privilege**
Security Administrator

**Syntax**

```
[ no ] certificate name validate
```

- **no**
  Removes any applied certificate or prevents the certificate from being included in the Auth Exchange response payload.

- **name**
  Specifies the name of a X.509 trusted certificate to bind to a crypto template. *name* is an alphanumeric string of 1 through 129 characters.

- **validate**
  Enable validations for the self-certificate.

**Usage**
Can be used to bind an X.509 certificate to a template, or include or exclude it from the Auth Exchange response payload.

**Example**
Use the following example to prevent a certificate from being included in the Auth Exchange payload:

```
no certificate
```
control-dont-fragment

Controls the Don’t Fragment (DF) bit in the outer IP header of the IPSec tunnel data packet.

**Product**
All IPSec-related services

**Privilege**
Security Administrator

**Syntax**

```markdown
control-dont-fragment { clear-bit | copy-bit | set-bit }

{ clear-bit | copy-bit | set-bit }

Configures the option to perform on the DF bit.
- **clear-bit**: Clears the DF bit from the outer IP header (sets it to 0).
- **copy-bit**: Copies the DF bit from the inner IP header to the outer IP header. This is the default action.
- **set-bit**: Sets the DF bit in the outer IP header (sets it to 1).
```

**Usage**

A packet is encapsulated in IPSec headers at both ends. The new packet can copy the DF bit from the original unencapsulated packet into the outer IP header, or it can set the DF bit if there is not one in the original packet. It can also clear a DF bit that it does not need.

**Example**

The following command sets the DF bit in the outer IP header:

```markdown
control-dont-fragment set-bit
```
default

Restores the default values for the selected parameter.

**Product**
All IPSec-related services

**Privilege**
Security Administrator

**Syntax**

default { allow-custom-fqdn-idr | authentication | certificate | control-dont-fragment |
dns-handling | dos { cookie-challenge detect-dos-attack } | ikev2-ikesa { allow-empty- |
ikesa | cert-sign | ignore-notify-protocol-id | ignore-rekeying-requests | keepalive- |
user-activity | max-retransmission | mobike | policy | rekey | retransmission-timeout |
setup-timer } | keepalive | nai idr | natt { include-header | send-keepalive } |

**Usage**
Use these commands to restore default parameters.

**Example**
Use the following command to disable MOBIKE by default:

default mobike
dns-handling

Adds a custom option to define the ways a DNS address is returned based on prescribed circumstances described below.

**Product**
PDIF

**Privilege**
Security Administrator

**Syntax**

```
[ default ] dns-handling { custom | normal }
```

- **default**
  Configures the default condition as `normal`. By default, PDIF always returns the DNS address in the config payload in the second authentication phase if one is received from either the configuration or the HA.

- **dns-handling custom**
  Configures the PDIF to behave as described in the Usage section below.

- **dns-handling normal**
  This is the default action. The service always returns the DNS address in the config payload in the second authentication phase if one is received from either the configuration or the HA.

**Usage**

During IKEv2 session setup, MS may or may not include INTERNAL_IP4_DNS in the Config Payload (CP). PDIF may obtain one or more DNS addresses for the subscriber in DNS NVSE from a proxy-MIP Registration Reply message. If Multiple Authentication is used, these DNS addresses may be also received in Diameter AVPs during the first authentication phase, or in RADIUS attributes in the Access Accept messages during the second authentication phase.

In `normal` mode, by default PDIF always returns the DNS address in the config payload in the second authentication phase if one is received from either the configuration or the HA.

In `custom` mode, depending on the number of INTERNAL_IP4_DNS, PDIF supports the following behaviors:

- If MS includes no INTERNAL_IP4_DNS in Config Payload: PDIF does not return any INTERNAL_IP4_DNS option to MS, whether or not PDIF has received one in DNS NVSE from HA or from local configurations.

- If MS requests one or more INTERNAL_IP4_DNS(s) in Config Payload, and if P-MIP NVSE doesn't contain any DNS address or DNS address not present in any config, PDIF omits INTERNAL_IP4_DNS option to MS in the Config Payload.

- And if P-MIP NVSE includes one DNS address (a.a.a.a / 0.0.0.0), then PDIF sends one INTERNAL_IP4_DNS option in Config Payload back to the MS.

- If the Primary DNS is a.a.a.a and the Secondary DNS is 0.0.0.0, then a.a.a.a is returned (only one instance of DNS attribute present in the config payload).

- If the Primary DNS is 0.0.0.0 and the Secondary DNS is a.a.a.a, then a.a.a.a is returned (only one instance of DNS attribute present in the config payload). PDIF does not take 0.0.0.0 as a valid DNS address that can be assigned to the MS.
And if P-MIP NVSE includes two DNS addresses (a.a.a and b.b.b) or configurations exists for these two addresses, then PDIF sends two INTERNAL_IP4_DNSs in the CP for the MS (typically known as primary and secondary DNS addresses).

Example

The following configuration applies the `custom` dns-handling mode:

```
dns-handling custom
```
dos cookie-challenge notify-payload

Configure the cookie challenge parameters for IKEv2 INFO Exchange notify payloads for the given crypto template.

**Product**
All IPSec-related services

**Privilege**
Security Administrator

**Syntax**

```

dos cookie-challenge notify-payload [ half-open-sess-count { start integer | stop integer } ]

[ default | no ] cookie-challenge detect-dos-attack

**default**
Default is to disabled condition.

**no**
Prevents Denial of Service cookie transmission. This is the default condition.

**half-open-sess-count**

The **half-open-sess-count** is the number of half-open sessions per IPSec manager.
A session is considered half-open if a PDIF has responded to an IKEv2 INIT Request with an IKEv2 INIT Response, but no further message was received on that particular IKE SA.

- **start**: Starts when the current half-open-sess-count exceeds the start count. The start count is an integer from 0 to 100000.
- **stop**: Stops when the current half-open-sess-count drops below the stop count. The stop count number is an integer from 0 to 100000. It is always less than or equal to the start count number.

**Important**: The start count value 0 is a special case whereby this feature is always enabled. In this event, both **Start** and **Stop** must be 0.

**Usage**
This feature (which is disabled by default) helps prevent malicious Denial of Service attacks against the server by sending a challenge cookie. If the response from the sender does not incorporate the expected cookie data, the packets are dropped.

**Example**

The following example configures the cookie challenge to begin when the half-open-sess-count reaches 50000 and stops when it drops below 20000:

```
dos cookie-challenge notify-payload half-open-sess-count start 50000 stop 20000
```

end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
exit

**Usage**
Use this command to return to the parent configuration mode.
**identity local**

Configures the identity of the local IPSec Client (IKE ID).

**Product**

All Security Gateway products

**Important:** This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

**Privilege**

Security Administrator

**Syntax**

```
identity local id-type type id name

no identity local
```

**no**

Resets the ID to the IP address of the interface to which the crypto template is associated (type = IPv4 or IPv6).

**id-type type**

Configures the IKE identity that the local client uses when authenticating to the gateway. Valid values are:

- `der-asn1-dn`: configures NAI Type DER_ASN1_DN (Distinguished Encoding Rules, ASN.1 encoding, Distinguished Name)
- `fqdn`: configures NAI Type ID_FQDN (Internet Fully Qualified Domain Name).
- `ip-addr`: configures NAI Type ID_IP_ADDR (IP Address).
- `key-id`: configures NAI Type ID_KEY_ID (opaque octet string).
- `rfc822-addr`: configures NAI Type ID_RFC822_ADDR (RFC 822 email address).

**id name**

Specifies the identifier for the local IKE client as an alphanumeric string of 1 through 127 characters.

**Usage**

Use this command to configure the identity of the local IPSec Client.

**Example**

The following command configures the local IPSec Client.

```
identity local id-type der-asn1-dn id system14
```
ikev2-ikesa

Configures parameters for the IKEv2 IKE Security Associations within this crypto template.

**Product**
All IPSec-related services

**Privilege**
Security Administrator

**Syntax**

```plaintext
ikev2-ikesa { allow-empty-ikesa | cert-sign { pkcs1.5 | pkcs2.0 } | ignore-notify-protocol-id | ignore-rekeying-requests | keepalive-user-activity | max-retransmissions number | policy { congestion-rejection { notify-status-value value } | error-notification [ invalid-major-version ] [ invalid-message-id { invalid-major-version | invalid-syntax } ] | invalid-syntax { invalid-major-version } | use-rfc5996-notification } | rekey [ disallow-param-change ] | retransmission-timeout msec | setup-timer sec | transform-set list name1 name2 name3 name4 name5 name6 }

default ikev2-ikesa { allow-empty-ikesa | cert-sign | ignore-notify-protocol-id | ignore-rekeying-requests | keepalive-user-activity | max-retransmissions | mobike | policy error-notification | rekey [ disallow-param-change ] | retransmission-timeout | setup-timer }

no ikev2-ikesa { allow-empty-ikesa | ignore-notify-protocol-id | ignore-rekeying-requests | keepalive-user-activity | list name | mobike | policy error-notification | rekey }

no ikev2-ikesa

Disables a previously enabled parameter.

**allow-empty-ikesa**
Default is not to allow-empty-ikesa. Activate to have the IKEv2 stack keep the IKE SA when all the Child SAs have been deleted.

**cert-sign { pkcs1.5 | pkcs2.0 }**
Specifies the certificate sign to be used. Default: pkcs1.5

**pkcs1.5**
Use the Public-Key Cryptography Standards (PKCS) version 1.5, RSA Encryption Standard.

**pkcs2.0**
Use the PKCS version 2.0, RSA Encryption Standard.

**ignore-notify-protocol-id**
Ignores IKEv2 Informational Exchange Notify Payload Protocol-ID values for strict RFC 4306 compliance.

**ignore-rekeying-requests**
Ignores received IKE_SA Rekeying Requests.

**keepalive-user-activity**
Default is no keepalive-user-activity. Activate to reset the user inactivity timer when keepalive messages are received from peer.
max-retransmissions number

Specifies the maximum number of retransmissions of an IKEv2 IKE Exchange Request if a response has not been received. number must be an integer from 1 through 8. Default: 5

mobike

IKEV2 Mobility and Multihoming Protocol: MOBIKE allows the IP addresses associated with IKEv2 and tunnel mode IPSec Security Associations to change. A mobile Virtual Private Network (VPN) client could use MOBIKE to keep the connection with the VPN gateway active while moving from one address to another. Similarly, a multihomed host could use MOBIKE to move the traffic to a different interface if, for instance, the one currently being used stops working. Default: disable


Specifies the default policy for generating an IKEv2 Invalid Message ID error when PDIF receives an out-of-sequence packet.

congestion-rejection: Sends an Error Notify Message to the MS as a reply to an IKE_SA_INIT Exchange when no more IKE_SA sessions can be established.

notify-status-value value: Notify Message will be sent to MS as a reply to an IKE_SA_INIT Exchange when no more IKE_SA sessions can be established. value is RFC 4306 IKEv2 Private Use Status Range - integer 40960..65535.

error-notification: Sends an Error Notify Message to the MS for Invalid IKEv2 Exchange Message ID and Invalid IKEv2 Exchange Syntax for the IKE_SA_INIT Exchange.

[invalid-major-version]: Sends an Error Notify Message for Invalid Major Version
[invalid-message-id]: Sends an Error Notify Message for Invalid IKEv2 Exchange Message ID.
[invalid-syntax]: Sends an Error Notify Message for Invalid IKEv2 Exchange Syntax.

use-rfc5996-notification: Enable sending and receive processing for RFC 5996 notifications - TEMPORARY_FAILURE and CHILD_SA_NOT_FOUND

rekey [ disallow-param-change ]

Specifies if IKESA rekeying should occur before the configured lifetime expires (at approximately 90% of the lifetime interval). Default is not to re-key.

The disallow-param-change option prevents changes in negotiation parameters during rekey.

retransmission-timeout msec

Specifies the timeout period (in milliseconds) before a retransmission of an IKEv2 IKE exchange request is sent (if the corresponding response has not been received). msec must be an integer from 300 to 15000. Default: 500

setup-timer sec

Specifies the number of seconds before a IKEv2 IKE Security Association that is not fully established is terminated. sec must be an integer from 1 through 3600. Default: 16

transform-set list name1

Specifies the name of a context-level configured IKEv2 IKE Security Association transform set. name1 ...name6 must be an existing IKEv2 IKESA Transform Set expressed as an alphanumeric string of 1 through 127 characters.
The transform set is a space-separated list of IKEv2-IKESA SA transform sets to be used for deriving IKEv2 IKE Security Associations from this crypto template. A minimum of one transform-set is required; maximum configurable is six.

Usage
Use this command to configure parameters for the IKEv2 IKE Security Associations within this crypto template.

Example
The following command configures the maximum number of IKEv2 IKESA request retransmissions to 7:

```
ikev2-ikesa max-retransmissions 7
```

The following command configures the IKEv2 IKESA request retransmission timeout to 400 milli seconds:

```
isv2-ikesa retransmission-timeout 400
```

The following command configures the IKEv2 IKESA list, consisting of a transform set named as ikesa43:

```
isv2-ikesa transform-set list ikesa43
```
keepalive

Configures keepalive or dead peer detection for security associations used within this crypto template.

**Product**
All products supporting IPSec

**Privilege**
Security Administrator

**Syntax**

```plaintext
keepalive [ interval sec ]

default keepalive [ interval ]

no keepalive
```

- **no**
  Disables keepalive messaging.

- **interval sec**
  Specifies the amount of time (in seconds) that must elapse before the next keepalive request is sent. `sec` must be an integer from 10 through 3600. Default: 10

**Usage**

Use this command to set parameters associated with determining the availability of peer servers.

**Example**

The following command sets a keepalive interval to three minutes (180 seconds):

```plaintext
keepalive interval 180
```
**max-childsa**

Defines a soft limit for the number of child Security Associations (SAs) per IKEv2 policy.

**Product**
All products supporting IPSEcv2

**Privilege**
Security Administrator

**Syntax**

```
max-childsa <numbr> [ overload-action { ignore | terminate } ]
```

```
max-childsa <numbr>
```

Specifies a soft limit for the maximum number of Child SAs per IKEv2 policy. `<numbr>` can be an integer from 1 to 4 for releases prior to 15.0, or 1 to 5 for 15.0 and higher. Default = 2.

```
overload-action { ignore | terminate }
```

The action taken when the specified soft limit for the maximum number of Child SAs is reached, as follows:

- **ignore**: The IKEv2 stack ignores the specified soft limit for Child SAs.
- **terminate**: The IKEv2 stack rejects any new Child SAs if the specified soft limit is reached.

**Usage**
The FNG maintains two maximum Child SA values per IKEv2 policy. The first is a system-enforced maximum value, which is four Child SAs per IKEv2 policy. The second is a configurable soft maximum value, which can be a value between one and four. This command defines the soft limit for the maximum number of Child SAs per IKEv2 policy.

**Example**
The following command specifies a soft limit of four Child SAs with the overload action of terminate.

```
max-childsa 4 overload action terminate
```
nai

Configures the Network Access Identifier (NAI) parameters to be used for the crypto template IDr (recipient’s identity).

**Important:** This command is deprecated from 15.0 and later releases.

**Product**
All Security Gateway products

**Privilege**
Security Administrator

**Syntax**

```
nai { idr name [ id-type { der-asn1-dn | der-asn1-gn | fqdn | ip-addr | key-id | rfc822-addr } ] | use-received-idr }

default nai idr

no nai { idr | use-received-idr }
```

**default**

Configures the default command `no nai idr`. As a result, the default behavior is for the PDIF-service IP address to be sent as the IDr value of type ID_IP_ADDR.

**no**

`no nai idr` configures the value whereby the service IP address is sent as the IDr value with the type ID_IP_ADDR. This is the default condition.

**idr name**

Specifies the name of the IDr crypto template as an alphanumeric string of 1 through 79 characters.

**id-type { der-asn1-dn | der-asn1-gn | fqdn | ip-addr | key-id | rfc822-addr }**

Configures the NAI IDr type parameter. If no id-type is specified, then `rfc822-addr` is assumed.

- `der-asn1-dn`: configures NAI Type DER_ASN1_DN (Distinguished Encoding Rules, ASN.1 encoding, Distinguished Name)
- `der-asn1-gn`: configures NAI Type DER_ASN1_GN (Distinguished Encoding Rules, ASN.1 encoding, General Name)
- `fqdn`: configures NAI Type ID_FQDN (Internet Fully Qualified Domain Name).
- `ip-addr`: configures NAI Type ID_IP_ADDR (IP Address).
- `key-id`: configures NAI Type ID_KEY_ID (opaque octet string).
- `rfc822-addr`: configures NAI Type ID_RFC822_ADDR (RFC 822 email address).

**use-received-idr**

Specifies that the received IDr be used in the crypto template.
Usage
The configured IDr is sent to the MS in the first IKEv2 AUTH response.

Example
The following command configures the NAI IDr to the default condition.

```bash
no naiidr
```
natt

Configures Network Address Translation - Traversal (NAT-T) for all security associations associated with this crypto template. This feature is disabled by default.

Product
All Security Gateway products

Privilege
Security Administrator

Syntax

[ default | no ] natt [ include-header ] [ send-keepalive [ idle-interval idle_secs ] [ interval interval_secs ] ]

- **default**
  - Disables NAT-T for all security associations associated with this crypto template.

- **no**
  - Disables NAT-T for all security associations associated with this crypto template.

- **include-header**
  - Includes the NAT-T header in IPSec packets.

- **send-keepalive [ idle-interval idle_secs ] [ interval interval_secs ]**
  - Sends NAT-Traversal keepalive messages.
    - **idle-interval idle_secs**: Specifies the number of seconds that can elapse without sending NAT keepalive packets before sending NAT keepalive packets is started. **idle_secs** is an integer from 20 to 86400. Default: 60.
    - **interval interval_secs**: Specifies the number of seconds between the sending of NAT keepalive packets. **interval_secs** is an integer from 20 to 86400. Default: 60.

Usage

Use this command to configure NAT-T for security associations within this crypto template.

Example

The following command disables NAT-T for this crypto template:

    no natt
**ocsp**

Enables use of Online Certificate Status Protocol (OCSP) from a crypto template. OCSP provides a facility to obtain timely information on the status of a certificate.

**Product**

All products supporting IPSec

**Important:** This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

**Privilege**

Security Administrator

**Syntax**

```
ocsp [ nonce | responder-address IPv4_address [ port port_value ] ]
no ocsp [ nonce | responder-address [ port ] ]
default ocsp [ nonce ]
```

- **no**
  Disables the use of OCSP.

- **default**
  Sets / Restores default value assigned for ocsp nonce.

- **nonce**
  Enables sending nonce (unique identifier) in OCSP requests.

- **responder-address IPv4_address**
  Configures the OCSP responder address(IPv4), used when absent in peer (device) certificate. 
  *IPv4_address* is an IPv4 address specified in dotted decimal format.

- **port port_value**
  Configures the port for OCSP responder. 
  *port_value* is an integer value between 1 and 65535. The default port is 8889.

**Usage**

This command enables the use of Online Certificate Protocol (OCSP) from a crypto map/template. OCSP provides a facility to obtain timely information on the status of a certificate. OCSP messages are exchanged between a gateway and an OCSP responder during a certificate transaction. The responder immediately provides the status of the presented certificate. The status can be good, revoked or unknown. The gateway can then proceed based on the response.

**Example**

```
ocsp
payload

Creates a new, or specifies an existing, crypto template payload and enters the Crypto Template Payload Configuration Mode.

Product
All Security Gateway products

Privilege
Security Administrator

Syntax

[ no ] payload name match chilrsa [ match { any | ipv4 | ipv6 } ]

no

Removes a currently configured crypto template payload.

payload name

Specifies the name of a new or existing crypto template payload as an alphanumeric string of 1 through 127 characters.

match chilrsa [ match { any | ipv4 | ipv6 } ]

Filters IPSec Child Security Association creation requests for subscriber calls using this payload. Further filtering can be performed by applying the following:

• **match any**: Configures this payload to be applicable to IPSec Child Security Association requests for IPv4 and/or IPv6.
• **match ipv4**: Configures this payload to be applicable to IPSec Child Security Association requests for IPv4 only.
• **match ipv6**: Configures this payload to be applicable to IPSec Child Security Association requests for IPv6 only.

Usage

Use this command to create a new or enter an existing crypto template payload. The payload mechanism is a means of associating parameters for the Security Association (SA) being negotiated. Two payloads are required: one each for MIP and IKEv2. The first payload is used for establishing the initial Child SA Tunnel Inner Address (TIA) which will be torn down. The second payload is used for establishing the remaining Child SAs. Note that if there is no second payload defined with home-address as the ip-address-allocation then no MIP call can be established, just a Simple IP call. Currently, the only available match is for ChildSA, although other matches are planned for future releases. Omitting the second match parameter for either IPv4 or IPv6 will make the payload applicable to all IP address pools.

Crypto Template Payload Configuration Mode commands are defined in the *Crypto Template IKEv2-Dynamic Payload Configuration Mode Commands* chapter.

Example

The following command configures a crypto template payload called *payload5* and enters the Crypto Template Payload Configuration Mode:
payload payload5 match childsa
peer network

Configures a list of allowed peer addresses on this crypto template.

Product
All IPSec-related services

Privilege
Security Administrator

Syntax

```
peer network ip_address {/mask | mask ip_mask} [ encrypted pre-shared-key key | pre-shared-key key ]
```

```
no peer network ip_address mask ip_mask
```

no

Removes the specified peer network IP address from this crypto template.

```
peer network ip_address {/mask | mask ip_mask}
```

Specifies the IP address of the peer network in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

`/mask` specifies the subnet mask bits. `mask` must be an integer value from 1 to 32 for IPv4 addresses and 1 to 128 for IPv6 addresses (CIDR notation).

`mask ip_mask` specifies the subnet mask in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notations.

```
[ encrypted pre-shared-key key | pre-shared-key key ]
```

`encrypted preshared key key` : Specifies that an encrypted pre-shared key is to be used for IPSec authentication for the address range. `key` must be an alphanumeric string or hexadecimal sequence from 16 to 64.

`preshared key key` : Specifies that a clear text pre-shared key is to be used for IPSec authentication for the address range. `key` must be an alphanumeric string or hexadecimal sequence from 1 to 32.

Usage

Use this command to configure a list or range of allowed peer network IP addresses for this template.

Example

The following command configures a set of IP addresses with starting address of `10.2.3.4` and a bit mask of 8:

```
peer network 10.2.3.4/8
```
remote-secret-list

Enables the use of a Remote Secret List containing up to 1000 pre-shared keys.

Product
All Security Gateway products

Important: This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

Privilege
Security Administrator

Syntax

remote-secret-list  list_name

no remote-secret-list

no

Disables use of a Remote Secret List.

list_name

Specifies the name of an existing Remote Secret List as an alphanumeric string of 1 through 127 characters.

Usage
Enable the use of a Remote Secret List containing up to 1000 pre-shared keys. Only one active remote-secret-list is supported per system. For additional information, refer to the Remote Secret List Configuration Commands chapter of the Command Line Interface Reference and the System Administration Guide.

Example

The following command enables a remote-secret-list named rs-list:

remote-secret-list rs-list
timeout

Sets the OCSP Certificate Server timeout interval in seconds. This is the interval within which the response from an external OCSP or HASH-url server should be received.

Product Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > Crypto Template Configuration
configure > context context_name > crypto template template_name ikev2-dynamic

Entering the above command sequence results in the following prompt:

[context_name]host_name(crf-crypto-tmpl-ikev2-tunnel)#

Syntax

timeout cert-server timeout_value

default timeout cert-server

default

Sets / Restores default value assigned for Certificate Server timeout in seconds. Default is 20 seconds.

timeout_value

Specifies the timeout value in seconds which is an integer between 1 through 60.

Usage

Use this command to configure Certificate Server timeout in seconds.

Example

The following command configures Certificate Server timeout as 50 seconds:

    timeout cert-server 50
whitelist

Enables the use of an existing whitelist (access permitted) file by a security gateway.

Product
All products supporting IPSec whitelisting

Important: This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

Privilege
Security Administrator

Syntax

whitelist

no whitelist

Usage

Enable the use of a previously created whitelist to allow privileged peers access via a security gateway. A whitelist is a list or register of entities that are being provided a particular privilege, service, mobility, access or recognition. With whitelisting, no peer is allowed to connect unless it appears in the list. Each entry in the whitelist file should contain the ID type so that the validation is performed for that ID type. In every entry, the ID type and ID value should be separated by a space. Only DOS and UNIX file formatting are supported. For additional information, refer to the System Administration Guide.

Example

whitelist
Chapter 67
Crypto Template IKEv2-Dynamic Payload Configuration Mode Commands

The Crypto Template IKEv2-Dynamic Payload Configuration Mode is used to assign the correct IPSec transform-set from a list of up to four different transform-sets, and to assign Mobile IP addresses. There should be two payloads configured. The first must have a dynamic addressing scheme from which the ChildSA gets a TIA address. The second payload supplies the ChildSA with a HoA, which is the default setting for \textit{ip-address-allocation}.

**Mode**

Exec > Global Configuration > Context Configuration > Crypto Template Configuration > Crypto Template IKEv2-Dynamic Payload Configuration

\begin{verbatim}
configure > context context_name > crypto template template_name ikev2-dynamic > payload payload_name match childsa match \{ any | ipv4 | ipv6 \}
\end{verbatim}

Entering the above command sequence results in the following prompt:

\texttt{[context_name]host_name(cfg-crypto-tmpl-ikev2-tunnel-payload)#}

\textbf{Important:} The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
default

Sets or restores the default value for the specified parameter.

Product
ePDG
PDIF

Privilege
Security Administrator

Mode
Exec > Global Configuration > Context Configuration > Crypto Template Configuration > Crypto Template IKEv2-Dynamic Payload Configuration

configure > context context_name > crypto template template_name ikev2-dynamic > payload payload_name match childsa match { any | ipv4 | ipv6 }

Entering the above command sequence results in the following prompt:

[context_name]host_name(cfg-crypto-tmpl-ikev2-tunnel-payload)#

Syntax

default { ignore-rekeying-requests | ip-address-allocation lifetime | maximum-child-sa | rekey | tsi | tsr }

ignore-rekeying-requests
Configures the system to ignore IPSec SA rekey requests.

ip-address-allocation
Configures the crypto map payload IP address allocation scheme to be the home address.

lifetime
Configures the default lifetime for IPSec Child SAs derived from this crypto template. lifetime: 86400 seconds.

maximum-child-sa
Configures the maximum number of IPSec Child SAs to be derived from an IKEv2 IKE SA by default.

rekey
Configures the system to disable Child SA rekeying.

tsi
Configures the default TSi payload to be that of the mobile endpoint.

tsr
Configures the default TSr payload option.
Usage

Configures system defaults.

Example

Use the following configuration to set the TSI payload start-address to be that of the mobile endpoint:

```
default tsi
```
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Use this command to return to the parent configuration mode.
ignore-rekeying-requests

Ignores CHILD SA rekey requests from the Packet Data Interworking Function (PDIF).

Product
All Security Gateway products

Privilege
Security Administrator

Mode
Exec > Global Configuration > Context Configuration > Crypto Template Configuration > Crypto Template IKEv2-Dynamic Payload Configuration

```
configure > context context_name > crypto template template_name ikev2-dynamic > payload
payload_name match childsa match { any | ipv4 | ipv6 }
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-crypto-tmpl-ikeyv2-tunnel-payload)#
```

Syntax

```
ignore-rekeying-requests
```

Usage
Prevents creation of a CHILD SA based on this crypto template.

Example
The following command prevents creation of a CHILD SA based on this crypto template:

```
ignore-rekeying-requests
```
ip-address-allocation

Configures IP address allocation for subscribers using this crypto template payload. Configure two payloads per crypto template. The first must have a dynamic address to assign a tunnel inner address (TIA) to the ChildSA. The second payload is configured after a successful MANaged IP (MIP) initiation and can use the default Home Address (HoA) option.

Product
All Security Gateway products

Privilege
Security Administrator

Mode
Exec > Global Configuration > Context Configuration > Crypto Template Configuration > Crypto Template IKEv2-Dynamic Payload Configuration

configure > context context_name > crypto template template_name ikev2-dynamic > payload payload_name match childsa match { any | ipv4 | ipv6 }

Entering the above command sequence results in the following prompt:

[context_name]host_name(cfg-crypto-tmpl-ikev2-tunnel-payload)#

Syntax

ip-address-allocation { dynamic | home-address | }

default ip-address-allocation

---

ip-address-allocation dynamic

Specifies that the IP address for the subscriber is allocated from a dynamic IP pool.

---

ip-address-allocation home-address

The IP address for the subscriber is allocated by the Home Agent. This is the default setting for this command.

Usage

Use this command to configure how ChildSA payloads are allocated IP addresses for this crypto template.

Example

The following command is for the first ChildSA and will ensure that it gets a TIA address from an IP address pool:

    ip-address-allocation dynamic

The following command is for the second ChildSA and will ensure that it gets a HoA address from the HA:

    default ip-address-allocation
ipsec

Configures the IPSec transform set to be used for this crypto template payload.

**Product**
All Security Gateway products

**Privilege**
Security Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Crypto Template Configuration > Crypto Template IKEv2-Dynamic Payload Configuration

```console
configure > context context_name > crypto template template_name ikev2-dynamic > payload payload_name match childsa match { any | ipv4 | ipv6 }
```

Entering the above command sequence results in the following prompt:

`[context_name]host_name(cfg-crypto-tmpl-ikev2-tunnel-payload)#`

**Syntax**

```console
[ no ] ipsec transform-set list name
```

no

Specifies the IPSec transform set to be deleted. This is a space-separated list. From 1 to 4 transform sets can be entered. `name` must be an alphanumeric string of 1 through 127 characters.

ipsec transform-set list name

Specifies the context configured IPSec transform set name to be used in the crypto template payload. This is a space-separated list. From 1 to 4 transform sets can be entered. `name` must be an alphanumeric string of 1 through 127 characters.

**Usage**

Use this command to list the IPSec transform set(s) to use in this crypto template payload.

**Example**

The following command configures IPSec transform sets named `ipset1` and `ipset2` to be used in this crypto template payload:

```console
ipsec transform-set list ipset1 ipset2
```
lifetime

Configures the number of seconds for IPSec Child SAs derived from this crypto template payload to exist.

Product
All Security Gateway products

Privilege
Security Administrator

Mode
Exec > Global Configuration > Context Configuration > Crypto Template Configuration > Crypto Template IKEv2-Dynamic Payload Configuration

configure > context context_name > crypto template template_name ikev2-dynamic > payload payload_name match childsa match { any | ipv4 | ipv6 }

Entering the above command sequence results in the following prompt:

[context_name]host_name(cfg-crypto-tmpl-ikev2-tunnel-payload)#

Syntax

```
lifetime { sec [ kilo-bytes kbytes ] | kilo-bytes kbytes }
```

default lifetime

```
sec
```

Specifies the number of seconds for IPSec Child Security Associations derived from this crypto template payload to exist. `sec` must be an integer from 60 through 604800. Default: 86400

```
kilo-bytes kbytes
```

Specifies lifetime in kilobytes for IPSec Child Security Associations derived from this crypto template payload. `kbytes` must be an integer from 1 through 2147483647.

```
default lifetime
```

Sets the lifetime to its default value of 86400 seconds.

Usage

Use this command to configure the number of seconds and/or kilobytes for IPSec Child Security Associations derived from this crypto template payload to exist.

Example

The following command configures the IPSec child SA lifetime to be 120 seconds:

```
lifetime 120
```
maximum-child-sa

Configures the maximum number of IPSec child security associations that can be derived from a single IKEv2 IKE security association.

**Product**
All Security Gateway products

**Privilege**
Security Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Crypto Template Configuration > Crypto Template IKEv2-Dynamic Payload Configuration

```configure > context context_name > crypto template template_name ikev2-dynamic > payload payload_name match childsa match { any | ipv4 | ipv6 }
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-crypto-tmpl-ikev2-tunnel-payload)#
```

**Syntax**

- `maximum-child-sa num`
- `default maximum-child-sa`

**Usage**

Specifies the maximum number of IPSec child security associations that can be derived from a single IKEv2 IKE security association. `num` must be 1. Default: 1

**Example**

The following command configures the maximum number of child SAs to 1:

```
maximum-child-sa 1
```
rekey

Configures IPSec Child Security Association rekeying.

Product
All Security Gateway products

Privilege
Security Administrator

Mode
Exec > Global Configuration > Context Configuration > Crypto Template Configuration > Crypto Template IKEv2-Dynamic Payload Configuration

configure > context context_name > crypto template template_name ikev2-dynamic > payload payload_name match childsa match { any | ipv4 | ipv6 }

Entering the above command sequence results in the following prompt:

[context_name]host_name(cfg-crypto-tmpl-ikev2-tunnel-payload)#

Syntax

[ no ] rekey [ keepalive ]

no
Disables this feature.

keepalive
If specified, a session will be rekeyed even if there has been no data exchanged since the last rekeying operation. By default, rekeying is only performed if there has been data exchanged since the previous rekey.

Usage

Use this command to enable or disable the ability to rekey IPSec Child SAs after approximately 90% of the Child SA lifetime has expired. The default, and recommended setting, is not to perform rekeying. No rekeying means the PDIF will not originate rekeying operations and will not process CHILD SA rekeying requests from the UE.

Example

The following command disables rekeying:

no rekey
tsi

Configures the IKEv2 Traffic Selector-Initiator (TSi) payload address options.

Product
All Security Gateway products

Privilege
Security Administrator

Mode
Exec > Global Configuration > Context Configuration > Crypto Template Configuration > Crypto Template IKEv2-
Dynamic Payload Configuration

```bash
configure > context context_name > crypto template template_name ikev2-dynamic > payload
payload_name match childsa match { any | ipv4 | ipv6 }
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-crypto-tmpl-ikev2-tunnel-payload)#
```

Syntax

```
    tsi start-address { any end-address any | endpoint end-address endpoint }
```

- **any end-address any**
  - Configures the TSi payload to allow all IP addresses.

- **endpoint end-address endpoint**
  - Configures the TSi payload to allow only the Mobile endpoint address. (Default)

Usage

On receiving a successful IKE_SA_INIT Response from PDIF, the MS sends an IKE_AUTH Request for the
first EAP-AKA authentication. If the MS is capable of doing multiple-authentication, it includes the
MULTI_AUTH_SUPPORTED Notify payload in the IKE_AUTH Request. MS also includes an IDi payload
containing the NAI, SA, TSi, TSr, and CP (requesting IP address and DNS address) payloads.

Example

Use the following example to configure a TSi payload that allows all addresses:

```
tsi start-address any end-address any
```
tsr

Configures the IKEv2 Traffic Selector-Responder (TSr) payload address options.

**Product**
All Security Gateway products

**Privilege**
Security Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Crypto Template Configuration > Crypto Template IKEv2-Dynamic Payload Configuration

```bash
configure > context context_name > crypto template template_name ikev2-dynamic > payload payload_name match childsa match { any | ipv4 | ipv6 }
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-crypto-tmpl-ikev2-tunnel-payload)#
```

**Syntax**

`tsr start-address ip address end-address ip address`

- **start-address ip address**
  
  Configures the TSr payload to include the starting IP address of the TSr range specified in IPv4 dotted-decimal notation.
  
  See the limitations listed in the *Usage* section.

- **end-address ipv4 address**
  
  Configures the TSr payload to include the ending IP address of the TSr range in IPv4 dotted-decimal notation.
  
  See the limitations listed in the *Usage* section.

**Usage**

This command is used to specify an IP address range in the single TSr payload that the PDG/TTG returns in the last IKE_AUTH message. This TSr is Child SA-specific.

This command is subject to the following limitations:

- The configuration is restricted to a maximum of four TSrs per payload and per childsa.
- Overlapping TSrs are not allowed either inside the same payload or across different payloads.

**Example**

Use the following example to configure a TSr payload that specifies an IPv4 address range for the payload:

```bash
tsrf start-address 10.2.3.4 end-address 10.2.3.155
```
Chapter 68
CSCF Access Profile Configuration Mode Commands

The Access Profile Configuration Mode is used to set commands supporting the use of signaling compression, authentication, and SIP timers for subscribers accessing the system from varying network types.

Mode

Exec > Global Configuration > Context Configuration > CSCF Access Profile Configuration

configure > context context_name > cscf access-profile { default | name profile_name }

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-cscf-access-profile)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
**access-security-type**

Sets the type of access security for a P-CSCF/A-BG.

**Product**

SCM (P-CSCF, A-BG)

**Privilege**

Administrator

**Mode**

Exec > Global Configuration > Context Configuration > CSCF Access Profile Configuration

```
configure > context context_name > cscf access-profile { default | name profile_name }
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-access-profile)#
```

**Syntax**

```
[ no ] access-security-type ipsec-3gpp-cscf
```

- **no**
  - Disables the selected access security type.

- **ipsec-3gpp-cscf**
  - Security mechanism 3GPP/3GPP2 IPSec.

**Usage**

Use this command to enable or disable an access security type for a P-CSCF or A-BG.

**Example**

Enables 3GPP/3GPP2 IPSec access security on P-CSCF or A-BG:

```
access-security-type ipsec-3gpp-cscf
```

Disables 3GPP/3GPP2 IPSec access security on P-CSCF or A-BG:

```
no access-security-type ipsec-3gpp-cscf
```
authentication

Sets the authentication method to use for subscribers using this access profile.

**Product**
SCM (P-CSCF, A-BG)

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Access Profile Configuration

```bash
configure > context context_name > cscf access-profile { default | name profile_name }
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-access-profile)#
```

**Syntax**

```bash
[ no ] authentication { aka-v1 | custom-md5 | md5 }
```

- **no**
  Disables the selected authentication type.

- **aka-v1 | custom-md5 | md5**
  - **aka-v1**: Specifies that the AKA-v1 algorithm will be used for subscribers using this access profile.
  - **custom-md5**: Specifies that custom algorithm HTTP-Digest-MD5 will be used for subscribers using this access profile.
  - **md5**: Specifies that the MD5 algorithm will be used for subscribers using this access profile. This is the default setting for this command.

**Usage**

Use this command to set the authentication method used for subscribers using this access profile.

**Example**

The following command sets the authentication type for subscribers using this access profile to **md5**:

```
authentication md5
```
**diameter-selection**

Enables or disables prefix and capability-based CDF server selection for this access profile. By default, this command is disabled.

**Product**
SCM (S-CSCF)

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Access Profile Configuration

```
configure > context context_name > cscf access-profile { default | name profile_name }
```

Entering the above command sequence results in the following prompt:

```
[context_name] host_name(config-cscf-access-profile)#
```

**Syntax**

```
[ no ] diameter-selection cdf
```

- **no**
  
  Disables prefix and capability-based CDF server selection.

**Usage**

Use this command to enable or disable prefix and capability-based CDF server selection per access-type.
end

Ends the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
end

**Usage**
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**
Use this command to return to the parent configuration mode.
pcrf-policy-control

Enables PCRF policy control for this access profile. By default, this command is disabled.

**Product**
SCM (P-CSCF, A-BG)

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Access Profile Configuration

```
configure > context context_name > cscf access-profile { default | name profile_name }
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-access-profile)#
```

**Syntax**

```
[ default | no ] pcrf-policy-control
```

```
default | no

PCRF policy control is disabled.
```

**Usage**

Use this command to enable or disable PCRF policy control for this access profile.

When a subscriber sends a REGISTER message, P-CSCF extracts the access-type mentioned in the P-Access-Network-Info and stores it. When P-CSCF needs to trigger an AAR for a subscriber, either for signaling-loss-detection or media-authorization, it will check if pcrf-policy-control is enabled for that subscriber's stored access-type. If pcrf-policy-control is enabled, AAR will be sent to PCRF for that subscriber.
sigcomp

Enables signalling compression for the Access Profile.

**Product**

SCM (P-CSCF, A-BG)

**Privilege**

Administrator

**Mode**

Exec > Global Configuration > Context Configuration > CSCF Access Profile Configuration

`configure > context context_name > cscf access-profile { default | name profile_name }`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-access-profile)#
```

**Syntax**

```
[ no ] sigcomp [ force ]
```

---

**no**

Disables signalling compression for the Access Profile.

---

**force**

Specifies that signaling compression is to be forced for the access type. When this feature is enabled, messages received by the P-CSCF/A-BG that are not compressed are rejected.

---

**Usage**

Use this command to enable signalling compression for the specific Access Profile.
timeout

Sets timeout values for CSCF and SIP transactions for subscribers using this Access Profile.

Product
SCM (P-CSCF, A-BG)

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > CSCF Access Profile Configuration

configure > context context_name > cscf access-profile { default | name profile_name }

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-cscf-access-profile)#

Syntax

```
timeout sip { 3gpp-d sec | 3gpp-t1 msec | 3gpp-t2 sec | 3gpp-t4 sec | c sec | d sec | invite-expiry sec | t1 msec | t2 sec | t4 sec }

default timeout sip { 3gpp-d | 3gpp-t1 | 3gpp-t2 | 3gpp-t4 | c | d | invite-expiry | t1 | t2 | t4 }
```

Sets transaction and expiry timers for SIP.

- **3gpp-d** **sec**: This time is used to control the retransmission of 200OK messages to INVITEs after an ACK is sent. The ACK transaction is cleared after this period. This timer is applicable only for unreliable transport. **sec** must be an integer from 0 to 2147483646.
  
  Default: 64*T1 (128 seconds, recommended minimum)

- **3gpp-t1** **msec**: This timer is used to control the time interval between each retransmission. The interval doubles after each retransmission. This is used by P-CSCF/A-BG only when it sending message toward the UE. Example: T1, 2T1, 4T2, etc. This timer is applicable only for unreliable transport. **msec** must be an integer from 0 to 2147483646.
  
  Default: 2000 ms (2 secs, recommended minimum).

- **3gpp-t2** **sec**: This timer is used to control the period for which the request continues to get retransmitted. This is used by P-CSCF/A-BG only when it sending message toward the UE. This timer is applicable both for reliable and unreliable transport. **sec** must be an integer from 0 to 2147483646.
  
  Default: 16 seconds (recommended minimum).

- **3gpp-t4** **sec**: This timer is used to control the period for which the final response to non-invite transaction should be buffered. The buffered response for the retransmitted non-invite request should be sent within that interval. This timer is applicable only for unreliable transport. **sec** must be an integer from 0 to 2147483646.
  
  Default: 17 seconds (recommended minimum).

- **c** **sec**: This timer is used for an INVITE transaction; if the response is a provisional response with status codes 101 to 199 inclusive (anything but 100), the proxy must reset timer C for that client transaction. The timer may be reset to a different value, but this value must be greater than 3 minutes (180 seconds). When
timer C in S-CSCF fires first, S-CSCF will send CANCEL request to Terminating P-CSCF and Terminating P-CSCF will send CANCEL request to UAS.

\(sec\) must be an integer from 180 to 2147483646.
Default: 180 seconds

d \(sec\): This time is used to control the retransmission of 200 OK to INVITE after ACK is sent. The ACK transaction will be cleared after this interval. This timer is applicable only for unreliable transport.

\(sec\) must be an integer from 0 to 2147483646.
Default: 64*T1 (32 seconds, recommended minimum)

invite-expiry \(sec\): This timer is used by SIP while acting as UA Role and no final response is received for the INVITE request sent. This timer is applicable for both reliable and unreliable transport.

\(sec\) must be an integer from 0 to 2147483646.
Default: 100 seconds (recommended minimum).

t1 \(msec\): Specifies the time interval (in milliseconds) between each retransmission. The interval doubles after each retransmission, for example: \(T1, 2T1, 4T2, \) etc. This timer is applicable only for unreliable transport.

\(msec\) must be an integer from 0 to 2147483646.
Default: 500 milliseconds (recommended minimum).

t2 \(sec\): This timer is used to control the period for which the request keeps getting retransmitted. This timer is applicable both for reliable and unreliable transport.

\(sec\) must be an integer from 0 to 2147483646. The recommended minimum value for this parameter is 4 seconds.
Default: 64*T1 (32 seconds)

t4 \(sec\): This timer is used to control the period for which the final response to non-invite transaction should be buffered so as to send the buffered response for the retransmitted non-invite request within that interval. This timer is applicable only for unreliable transport.

\(sec\) must be an integer from 0 to 2147483646.
Default: 5 seconds (recommended minimum).

---

default

Sets/restores default value assigned for specified parameter.

---

Usage

Use this command to configure SIP Stack timers and CSCF service specific timers for subscriber traffic using this Access Profile.

Example

The following command sets the SIP \(d\) timer to 64 seconds:

```
  timeout sip d 64
```
The CSCF ACL (Access Control List) Configuration Mode is used to configure session permissions (permit/deny access) within the system.

Mode

Exec > Global Configuration > Context Configuration > CSCF ACL Configuration

configure > context context_name > cscf acl { default | name list_name }

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-cscf-acl)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
after

Places the CSCF ACL entry at the bottom or end of the ACL. Use this command in conjunction with the `permit` and/or `deny` commands.

**Product**
SCM

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF ACL Configuration

```bash
configure > context context_name > cscf acl { default | name list_name }
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-acl)#
```

**Syntax**

```
after
```

**Usage**

Add this command before the `permit` and/or `deny` commands to place the entry at the end of the ACL.
**before**

Places the CSCF ACL entry at the beginning or top of the ACL. Use this command in conjunction with the `permit` and/or `deny` commands.

**Product**
SCM

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF ACL Configuration

```
configure > context context_name > cscf acl { default | name list_name }
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-acl)#
```

**Syntax**
```
before
```

**Usage**
Add this command before the `permit` and/or `deny` commands to place the entry at the beginning of the ACL.
deny

Configures the system to deny subscriber sessions based on criteria matching the received packet.

**Product**
SCM

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF ACL Configuration

```
configure > context context_name > cscf acl { default | name list_name }
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-acl)#
```

**Syntax**

```
deny { any | destination aor aor | log { any | destination aor aor | source { address ip_address | aor aor } | subscriber-capability capability_type | user-agent device-type device_type } | source { address ip_address | aor aor } | subscriber-capability capability_type | user-agent device-type device_type } +
```

```
no deny { any | destination aor aor | source { address ip_address | aor aor } | subscriber-capability capability_type }
```

- **any**
  Filters all CSCF sessions.

- **destination aor aor**
  Filters sessions based on the destination AoR. `aor` must be an existing AoR from 1 to 79 characters in length.

**Important:** AoR regular expressions are supported. Refer to the SCM Engineering Rules Appendix in the Session Control Manager Administration Guide for more information about regular expressions.

```
log { any | destination aor aor | source { address ip_address | aor aor } | subscriber-capability { capability_type } | user-agent device-type device_type }
```

Enables logging for CSCF sessions meeting the criteria specified in the ACL. The logs can be viewed by executing the `logging filter active facility acl-log` command in the Exec mode.

Specifies the criteria that packets will be compared against. The following criteria are supported:

- **any**
- **destination aor aor**
- **source address ip_address**
- **source aor aor**
- **subscriber-capability capability_type**
deny

user-agent device-type device_type

source { address ip_address | aor aor }
Filters session based on the source IP address or AoR.
  • ip_address must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6.
  • aor must be an existing AoR from 1 to 79 characters in length.

Important: AoR regular expressions are supported. Refer to the SCM Engineering Rules Appendix in the Cisco ASR 5000 Series Session Control Manager Administration Guide for more information about regular expressions.

subscriber-capability { capability_type }
Filters session based on one of the following subscriber capability types:
  • at - Custom AT Type
  • audio - Audio Capability Type
  • chat - Custom CHAT Type
  • cs - Custom CS Type
  • ft - Custom FT Type
  • im - Custom IM Type
  • lte-voip - Custom LTE-VOIP Type
  • lte-vt - Custom LTE-VT Type
  • mms - Custom MMS Type
  • msg - Custom MSG Type
  • oma-sip-im - Custom OMA SIP-IM Type
  • rcs-dp - Custom RCS-DP Type
  • rcs-e - Custom RCS-E Type
  • rcs-ft - Custom RCS-FT Type
  • rcs-im - Custom RCS-IM Type
  • rcs-is - Custom RCS-IS Type
  • rcs-sp - Custom RCS-SP Type
  • rcs-vs - Custom RCS-VS Type
  • smart-edu - Custom SMART-EDU Type
  • text - Text Capability Type
  • video - Video Capability Type
  • vt - Custom VT Type
  • vt-ft - Custom VT-FT Type
  • vt-is - Custom VT-IS Type
  • vt-loc - Custom VT-LOC Type
  • vt-memo - Custom VT-MEMO Type
deny

user-agent device-type device_type
Filters session based on device-type in user-agent header.
device_type must be from 1 to 15 characters in length. The following user agent device types are supported.
  • feature_phone
  • smart_phone
  • pad
  • tablet_pc
  • pc
  • soft_phone
  • modem

+ This symbol indicates that the keywords can be entered multiple times within a single command.

no deny { any | destination aor aor | source { address ip_address | aor aor } | subscriber-capability { capability_type } }
Removes specified filter criteria.

Usage
Specifies the subscriber sessions to deny based on the criteria specified.

Example
The following command denies access to subscribers with a source address of 1.2.3.4:

deny source address 1.2.3.4
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**
Use this command to return to the parent configuration mode.
permit

Configures the system to allow subscriber sessions based on criteria matching the received packet.

**Product**
SCM

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF ACL Configuration

```bash
configure > context context_name > cscf acl { default | name list_name }
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-acl)#
```

**Syntax**

```bash
permit { any | destination aor aor | log { any | destination aor aor | source { address ip_address | aor aor } | subscriber-capability capability_type | user-agent device-type device_type } | source { address ip_address | aor aor } | subscriber-capability capability_type | user-agent device-type device_type } +

no permit { any | destination aor aor | source { address ip_address | aor aor } | subscriber-capability capability_type }
```

**any**
Filters all CSCF sessions.

**destination aor aor**
Filters sessions based on the destination AOR.
*aor* must be an existing AOR from 1 to 79 characters in length.

**Important:** AoR regular expressions are supported. Refer to the *SCM Engineering Rules* Appendix in the *Cisco ASR 5000 Series Session Control Manager Administration Guide* for more information about regular expressions.

```bash
log { any | destination aor aor | source { address ip_address | aor aor } | subscriber-capability { capability_type } | user-agent device-type device_type }
```

Enables logging for CSCF sessions meeting the criteria specified in the ACL. The logs can be viewed by executing the `logging filter active facility acl-log` command in the Exec mode.

Specifies the criteria that packets will be compared against. The following criteria are supported:

*any
*destination aor aor
*source address ip_address
*source aor aor
*subscriber-capability capability_type
permit

• **user-agent device-type** **device_type**

  **source** { **address** **ip_address** | **aor** **aor** }

  Filters session based on the source IP address or AoR.
  • **ip_address** must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6.
  • **aor** must be an existing AoR from 1 to 79 characters in length.

  **Important:** AoR regular expressions are supported. Refer to the SCM Engineering Rules Appendix in the Session Control Manager Administration Guide for more information about regular expressions.

• **subscriber-capability** { **capability_type** }

  Filters session based on one of the following subscriber capability types:
  • **at** - Custom AT Type
  • **audio** - Audio Capability Type
  • **chat** - Custom CHAT Type
  • **cs** - Custom CS Type
  • **ft** - Custom FT Type
  • **im** - Custom IM Type
  • **lte-voip** - Custom LTE-VOIP Type
  • **lte-vt** - Custom LTE-VT Type
  • **mms** - Custom MMS Type
  • **msg** - Custom MSG Type
  • **oma-sip-im** - Custom OMA SIP-IM Type
  • **rcs-dp** - Custom RCS-DP Type
  • **rcs-e** - Custom RCS-E Type
  • **rcs-ft** - Custom RCS-FT Type
  • **rcs-im** - Custom RCS-IM Type
  • **rcs-is** - Custom RCS-IS Type
  • **rcs-sp** - Custom RCS-SP Type
  • **rcs-vs** - Custom RCS-VS Type
  • **smart-edu** - Custom SMART-EDU Type
  • **text** - Text Capability Type
  • **video** - Video Capability Type
  • **vt** - Custom VT Type
  • **vt-ft** - Custom VT-FT Type
  • **vt-is** - Custom VT-IS Type
  • **vt-loc** - Custom VT-LOC Type
  • **vt-memo** - Custom VT-MEMO Type
**user-agent device-type** device_type

Filters session based on device-type in user-agent header. 
*device_type* must be from 1 to 15 characters in length. The following user agent device types are supported.
- feature_phone
- smart_phone
- pad
- tablet_pc
- pc
- soft_phone
- modem

+ This symbol indicates that the keywords can be entered multiple times within a single command.

**no permit { any | destination aor aor | source { address ip_address | aor aor } | subscriber-capability { capability_type } }

Removes specified filter criteria.

---

**Usage**

Specifies the subscriber sessions to permit based on the criteria specified.

**Example**

The following command permits access to subscribers with a destination AoR of $.@abc123.com:

```
permit destination aor $.@abc123.com
```
**redirect**

Configures the system to redirect subscriber sessions to another CSCF based on criteria matching the received packet.

**Product**  
SCM

**Privilege**  
Administrator

**Mode**  
Exec > Global Configuration > Context Configuration > CSCF ACL Configuration

```bash
configure > context context_name > cscf acl { default | name list_name }
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-acl)#
```

**Syntax**

```bash
redirect { address ip_address | host host_name } [ port port_number ] { any | destination aor aor | log { any | destination aor aor | source { address ip_address | aor aor } | subscriber-capability capability_type | user-agent device-type device_type } | source { address ip_address | aor aor } | subscriber-capability capability_type | user-agent device-type device_type } +

no redirect { address ip_address | host host_name } [ port port_number ] { any | destination aor aor | source { address ip_address | aor aor } | subscriber-capability capability_type }
```

- **address ip_address**  
The address to which UE should be redirected.  
*ip_address* must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6.

- **host host_name**  
The host to which UE should be redirected.  
*host_name* must be an existing name from 1 to 79 characters in length.

- **port port_number**  
The port at which request should be redirected.  
*port_number* must be an integer from 1 to 65535.

- **any**  
Redirect UE to address/host.

- **destination aor aor**  
Redirect UE to address/host if destination AoR matches.  
*aor* must be an existing AoR from 1 to 79 characters in length.
Important: AoR regular expressions are supported. Refer to the SCM Engineering Rules Appendix in the Session Control Manager Administration Guide for more information about regular expressions.

```
log { any | destination aor aor | source { address ip_address | aor aor } | subscriber-capability { capability_type } | user-agent device-type device_type }
```

Enables logging for redirect ed UE meeting the criteria specified in the ACL. The logs can be viewed by executing the `logging filter active facility acl-log` command in the Exec mode.

Specifies the criteria that packets will be compared against. The following criteria are supported:

- `any`
- `destination aor aor`
- `source address ip_address`
- `source aor aor`
- `subscriber-capability capability_type`
- `user-agent device-type device_type`

```
source { address ip_address | aor aor }
```

Redirect UE to address/host if source IP address or AoR matches.

- `ip_address` must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6.
- `aor` must be an existing AoR from 1 to 79 characters in length.

Important: AoR regular expressions are supported. Refer to the SCM Engineering Rules Appendix in the Session Control Manager Administration Guide for more information about regular expressions.

```
subscriber-capability { capability_type }
```

Redirect UE to address/host if contact has one of the following subscriber capability types:

- `at` - custom AT type
- `audio` - audio capability type
- `chat` - custom CHAT type
- `cs` - custom CS type
- `ft` - custom FT type
- `im` - custom IM type
- `lte-voip` - Custom LTE-VOIP Type
- `lte-vt` - Custom LTE-VT Type
- `mms` - custom MMS type
- `msg` - Custom MSG Type
- `oma-sip-im` - Custom OMA SIP-IM Type
- `rcs-dp` - Custom RCS-DP Type
- `rcs-e` - Custom RCS-E Type
- `rcs-ft` - Custom RCS-FT Type
- `rcs-im` - Custom RCS-IM Type
**redirect**

- **rcs-is** - Custom RCS-IS Type
- **rcs-sp** - Custom RCS-SP Type
- **rcs-vs** - Custom RCS-VS Type
- **smart-edu** - Custom SMART-EDU Type
- **text** - Text Capability Type
- **video** - Video Capability Type
- **vt** - Custom VT Type
- **vt-ft** - Custom VT-FT Type
- **vt-is** - Custom VT-IS Type
- **vt-loc** - Custom VT-LOC Type
- **vt-memo** - Custom VT-MEMO Type

**User-Agent device-type device_type**

Redirect UE to address/host according to device-type in user-agent header.

*device_type* must be from 1 to 15 characters in length. The following user agent device types are supported.

- feature_phone
- smart_phone
- pad
- tablet_pc
- pc
- soft_phone
- modem

+ This symbol indicates that the keywords can be entered multiple times within a single command.

**no redirect** { address ip_address | host host_name } [ port port_number ] { any | destination aor aor | source { address ip_address | aor aor } | subscriber-capability { capability_type } }

Removes specified redirect location and filter criteria.

**Usage**

Specifies the subscriber sessions to redirect based on the criteria specified.

**Example**

The following command redirects subscribers with a destination AoR of $.@abc123.com to host scscf.com:

```
redirect host scscf.com destination aor $.@abc123.com
```
Chapter 70
CSCF AoR Policy Rules Configuration Mode Commands

The CSCF AoR Policy Rules Configuration Mode is used to manage AoR policy profiles within the system. Both default and user-defined profiles can be managed in this mode.

Mode

Exec > Global Configuration > Context Configuration > CSCF Policy Configuration > AoR Policy Rules Configuration

configure > context context_name > cscf policy { default | name policy_name } > aor-policy-rules

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-policy_name-aor)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
after

Places the CSCF policy entry at the bottom or end of the policy list. Use this command in conjunction with the `aor` command.

**Product**
SCM

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Policy Configuration > AoR Policy Rules Configuration
`configure > context context_name > cscf policy { default | name policy_name } > aor-policy-rules`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-policy_name-aor)#
```

**Syntax**

```
after
```

**Usage**

Add this command before the `aor` command to place the entry at the end of the policy list.
**aor**

Configures an AoR profile and enters the CSCF Policy Rules Configuration Mode.

**Product**
SCM

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Policy Configuration > AoR Policy Rules Configuration

```bash
configure > context context_name > cscf policy { default | name policy_name } > aor-policy-rules
```

Entering the above command sequence results in the following prompt:

```
[context_name]hostname(config-policy_name-aor)#
```

**Syntax**

```bash
[ no ] aor aor_name
```

- **no**
  Removes the AoR profile from the system.

- **aor_name**
  Specifies a name for the AoR profile.
  *aor_name* must be from 1 to 79 alpha and/or numeric characters in length.

**Usage**

Use this command to create or modify an AoR profile and enter the CSCF Policy Rules Configuration Mode. Entering this command results in the following prompt:

```
[context_name]hostname(config-policy_name-aor)#
```

CSCF Policy Rules Configuration Mode commands are defined in the *CSCF Policy Rules Configuration Mode Commands* chapter of this guide.

**Example**

The following command creates an AoR profile named *aor5* and enters the CSCF Policy Rules Configuration Mode:

```
aor aor5
```
before

Places the CSCF policy entry at the top or beginning of the policy list. Use this command in conjunction with the `aor` command.

**Product**
SCM

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Policy Configuration > AoR Policy Rules Configuration

```
configure > context context_name > cscf policy { default | name policy_name } > aor-policy-rules
```

Entering the above command sequence results in the following prompt:

```
[context_name] host_name(config-policy_name-aor)#
```

**Syntax**

```
before
```

**Usage**

Add this command before the `aor` command to place the entry at the beginning of the policy list.
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
end
```

**Usage**
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

```bash
exit
```

**Usage**

Use this command to return to the parent configuration mode.
Chapter 71
CSCF ATCF-ATGW Configuration Mode Commands

The CSCF ATCF (Access Transfer Control Function)/ATGW (Access Transfer Gateway) Configuration Mode is used to configure the ATCF-ATGW functionality in the Proxy-CSCF service.

Mode

Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration > CSCF ATCF-ATGW Configuration

configure > context context_name > cscf service service_name > proxy-cscf > atcf-atgw

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-cscf-atcf-atgw)#

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
**call-linger-timer**

This command configures the timeout value after call termination request for ATCF service.

**Product**

SCM: P-CSCF, A-BG

**Privilege**

Administrator

**Mode**

Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration > CSCF ATCF-ATGW Configuration

```bash
configure > context context_name > cscf service service_name > proxy-cscf > atcf-atgw
```

Entering the above command sequence results in the following prompt:

```bash
[context_name]host_name(config-cscf-atcf-atgw)#
```

**Syntax**

```bash
call-linger-timer timer_seconds
```

**Usage**

Use this command to enable or disable call linger timer after call termination request. This determines the timeout value of session for abnormal procedure parameters in ATCF service.

**Example**

The following command sets the call linger timer value to 20 seconds:

```bash
call-linger-timer 20
```
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Use this command to return to the parent configuration mode.
mgmt-uri

This command supports PSI-based routing mode in I-CSCF.

**Product**
SCM: P-CSCF, A-BG, I-CSCF

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration > CSCF ATCF-ATGW Configuration

```bash
configure > context context_name > cscf service service_name > proxy-cscf > atcf-atgw
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-atcf-atgw)#
```

**Syntax**

```bash
mgmt-uri mgmt_uri
default mgmt-uri
```

**default mgmt-uri**

- Configures this command with its default setting.

**mgmt_uri**

- Specifies the ATCF management URI, and indicates SIP URI or hostname with domain.

  - `mgmt_uri` must be an alphanumeric string of 1 to 127 characters.

  Example format of management URI:
  - `sip:xyz@abc.com` for SIP URI
  - `sip:atcf.xyz.net` for hostname with domain

**Usage**

Use this command to configure ATCF management URI for PSI based routing in I-CSCF.

**Example**

The following command configures the ATCF management URI for hostname with domain `sip:atcf.xyz.net`

```bash
mgmt-uri sip:atcf.xyz.net
```
**policy name**

This command assigns or removes an existing ATCF policy.

**Product**

SCM: P-CSCF, A-BG

**Privilege**

Administrator

**Mode**

Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration > CSCF ATCF-ATGW Configuration

```bash
configure > context context_name > cscf service service_name > proxy-cscf > atcf-atgw
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-atcf-atgw)#
```

**Syntax**

```
[ no ] policy name policy_name
```

- **no**
  If previously configured, disables the configuration.

- **policy_name**
  Specifies the name of the ATCF policy list.
  `policy_name` must be an alphanumeric string of 1 to 127 characters.

**Usage**

Use this command to assign or remove an existing ATCF policy.

**Example**

The following command sets the ATCF policy named `access`:

```bash
policy name access
```
**stn-sr**

This command specifies a Session Transfer Number for Single Radio (STN-SR) for the ATCF service.

**Product**
SCM: P-CSCF, A-BG

**Privilege**
Administrator

**Mode**

Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration > CSCF ATCF-ATGW Configuration

```
configure > context context_name > cscf service service_name > proxy-cscf > atcf-atgw
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-atcf-atgw)#
```

**Syntax**

```
stn-sr stnsr_num
no stn-sr
```

**no**

If previously configured, disables the configuration.

```
stnsr_num
```

Specifies the STN-SR.

`stnsr_num` must be a string of up to 15 digits.

**Usage**

Use this command to configure the STN-SR number for ATCF service. The same STN-SR number will be used for all subscribers.

**Example**

The following command sets STN-SR number to `1005002115000`:

```
stn-sr 1005002115000
```
trusted scc-as

This command allows you to configure trusted Service Centralization and Continuity - Application Server (SCC-AS) addresses in ATCF service.

Product
SCM: P-CSCF, A-BG

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration > CSCF ATCF-ATGW Configuration

configure > context context_name > cscf service service_name > proxy-cscf > atcf-atgw

Entering the above command sequence results in the following prompt:

[context_name] host_name(config-cscf-atcf-atgw) #

Syntax

[ no ] trusted scc-as scc_as

  no
  If previously configured, disables the configuration.

  scc_as
  Specifies the list of trusted SCC-AS.
  scc_as must be an alphanumerical string of 1 to 79 characters.

Usage
Use this command to add or delete an SCC-AS address in ATCF service.

Example
The following command adds SCC-AS address cscfsc

  trusted scc-as sccl
Chapter 72
CSCF ATCF-ATGW Policy Configuration Mode Commands

The CSCF ATCF-ATGW Policy Configuration Mode is used to configure ATCF (Access Transfer Control Function) policy in the context.

**Mode**

Exec > Global Configuration > Context Configuration > ATCF Configuration

```
configure > context context_name > atcf policy name policy_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-atcf-atgw-policy)#
```
criteria

This command enables criteria to invoke ATCF functionality.

Product
SCM: P-CSCF, A-BG

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > ATCF Configuration

configure > context context_name > atcf policy name policy_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-atcf-atgw-policy)#

Syntax

criteria { access-type { 3gpp-e-utran-fdd | 3gpp-e-utran-tdd | 3gpp-geran | 3gpp-utran-fdd | 3gpp-utran-tdd | any | cellular | docsis | dsl | ethernet wlan } | all | any | ics-capability | roaming }

default criteria access-type

no criteria { access-type { 3gpp-e-utran-fdd | 3gpp-e-utran-tdd | 3gpp-geran | 3gpp-utran-fdd | 3gpp-utran-tdd | cellular | docsis | dsl | ethernet | wlan } | ics-capability | roaming }

default

Configures this command with its default setting.

no

If previously configured, disables the configuration.

criteria { access-type { 3gpp-e-utran-fdd | 3gpp-e-utran-tdd | 3gpp-geran | 3gpp-utran-fdd | 3gpp-utran-tdd | any | cellular | docsis | dsl | ethernet wlan } | all | any | ics-capability | roaming }

Specifies the access type of UE to invoke ATCF.
The supported access types are:

- **3gpp-e-utran-fdd**: Access type of UE is E-UTRAN-FDD
- **3gpp-e-utran-tdd**: Access type of UE is E-UTRAN-TDD
- **3gpp-geran**: Access type of UE is GERAN
- **3gpp-utran-fdd**: Access type of UE is UTRAN_FDD
- **3gpp-utran-tdd**: Access type of UE is UTRAN_TDD
- **any**: Access type of UE is any of the following: UTRAN, E-UTRAN, GERAN, DSL, ETHERNET, CELLULAR, WLAN or DOCSIS
- **cellular**: Access type of UE is CELLULAR
• **docsis**: Access type of UE is DOCSIS
• **dsl**: Access type of UE is DSL
• **ethernet**: Access type of UE is ETHERNET
• **wlan**: Access type of UE is WLAN

---

**all**
Specifies that all criteria must be met.

---

**any**
Specifies that any criteria must be met.

---

**ics-capability**
Specifies that UE is ICS capable.

---

**roaming**
Specifies that UE is in visited network.

---

**Usage**
Use this command to enable criteria based on UE’s access type to invoke ATCF functionality.

---

**Example**
The following command enables ATCF to be invoked based on UE’s access type of E-UTRAN-TDD:

```
criteria access-type 3gpp-utran-tdd
```
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

end

**Usage**
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Use this command to return to the parent configuration mode.
ps-cs-alerting

This command configures access transfer during alerting support in ATCF service.

Product
SCM: P-CSCF, A-BG

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > ATCF Configuration
configure > context context_name > atcf policy name policy_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-atcf-atgw-policy)#

Syntax

[ no ] ps-cs-alerting

no
If previously configured, disables the configuration.

Usage
Use this command to configure access transfer during alerting support in ATCF service.
Chapter 73
CSCF Charging Configuration Mode Commands

The CSCF Charging Configuration Mode is used to manage CSCF service policy profiles within the system.

Mode

Exec > Global Configuration > Context Configuration > CSCF Service Configuration > CSCF Charging Configuration

configure > context context_name > cscf service service_name > charging

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-cscf-charging)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**

Use this command to return to the Exec mode.
**exclude**

Configures the service to exclude SIP requests from the Rf charging configuration.

**Product**
SCM

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > CSCF Charging Configuration

```
configure > context context_name > cscf service service_name > charging
```

Entering the above command sequence results in the following prompt:

```
<context_name>host_name(config-cscf-charging)#
```

**Syntax**

```
[ no ] exclude { custom sip_method | invite | message | notify | register | subscribe | update }
```

- **no**
  Removes the exclusion of the specified SIP request message type.

- **custom sip_method**
  Specifies CUSTOM SIP requests that are to be excluded from Rf charging.
  `sip_method` can be a name of any SIP method and be from 1 to 31 alpha and/or numeric characters.

- **invite**
  Specifies that INVITE SIP requests are to be excluded from Rf charging.

- **message**
  Specifies that MESSAGE SIP requests are to be excluded from Rf charging.

- **notify**
  Specifies that NOTIFY SIP requests are to be excluded from Rf charging.

- **register**
  Specifies that REGISTER SIP requests are to be excluded from Rf charging.

- **subscribe**
  Specifies that SUBSCRIBE SIP requests are to be excluded from Rf charging.

- **update**
  Specifies that UPDATE SIP requests are to be excluded from Rf charging.
Usage
Use this command to exclude specific SIP requests from Rf charging.

Example
The following command configures the service to exclude SIP REGISTER requests from Rf charging:

```
exclude register
```
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Use this command to return to the parent configuration mode.
Chapter 74
CSCF Crypto Template Configuration Mode Commands

The CSCF Crypto Template Configuration Mode is used to configure a P-CSCF IPsec policy. It includes most of the IPsec parameters and Internet Key Exchange version 1 (IKEv1) parameters for cryptographic and authentication algorithms etc. A P-CSCF service will not support IPsec without a configured crypto template. Only one crypto template can be configured per P-CSCF service.

**Mode**

Exec > Global Configuration > Context Configuration > CSCF Crypto Template Configuration

```
configure > context context_name > crypto template template_name ipsec-3gpp-cscf
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-crypto-tmpl-ims-cscf-tunnel)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Use this command to return to the parent configuration mode.
ipsec

Configures parameters for the 3GPP/3GPP2 P-CSCF security associations within this crypto template.

Product
SCM

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > CSCF Crypto Template Configuration
configure > context context_name > crypto template template_name ipsec-3gpp-cscf

Entering the above command sequence results in the following prompt:

[context_name]host_name(cfg-crypto-tmpl-ims-cscf-tunnel)#

Syntax

ipsec transform-set list list_name

transform-set list name

transform-set: Specifies a context-level IPSec security association transform set to be used for deriving 3GPP/3GPP2 P-CSCF security associations from this crypto template.
list list_name: A space separated list of 3GPP/3GPP2 P-CSCF security association transform sets.
list_name must be an existing 3GPP/3GPP2 P-CSCF transform set and be from 1 to 127 alpha and/or numeric characters.

Important: A minimum of one transform set is required. A maximum of four transform sets may be specified.

Usage

Use this command to configure parameters for the 3GPP/3GPP2 P-CSCF security associations within this crypto template.

Example

The following command configures the 3GPP/3GPP2 P-CSCF transform set list name to ikevlist1:

ipsec transform-set list ikevlist1
Chapter 75
CSCF Diameter Selection Configuration Mode Commands

The Diameter Selection Configuration Mode is used to configure AAA group selection criteria that will be used for all CDF (enabled for a given access type) or HSS interactions for a subscriber.

```
Mode
Exec > Global Configuration > Context Configuration > CSCF Diameter Selection Configuration
configure > context context_name > cscf diameter-selection type { cdf | hss }
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-diameter-selection)>
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
aaa-group

Configures diameter selection entries.

Product
SCM

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > CSCF Diameter Selection Configuration

configure > context context_name > cscf diameter-selection type { cdf | hss }
Entering the above command sequence results in the following prompt:

[context_name]host_name(config-cscf-diameter-selection)#

Syntax

aaa-group name { [ preference value ] [ skiplir ] [ criteria { aor aor_prefix | subscriber-capability capability_type | subscriber-ip-type { v4 | v6 } | user-agent value ] } } +

no aaa-group name preference value

name
Specifies a name for the diameter selection entry. name must be from 1 to 63 alpha and/or numeric characters.

preference value
Configures preference that will be associated with each diameter selection entry. If preference is specified, the entry matching the preference is updated and a new entry is created in the prefix table. If preference is not specified, it is assigned a preference one greater than the last entry's preference in the diameter selection table. value must be an integer from 1 to 65535.

skiplir
Configures selected AAA group to skip LIR-LIA (Location-Info-Request — Location-Info-Answer). This is applicable only for HSS.

criteria
Specifies AAA group selection criteria.

aor aor_prefix
Filters based on the source or destination AoR. aor_prefix must be an existing AoR from 1 to 79 characters in length.
AoR regular expressions are supported. Refer to the SCM Engineering Rules Appendix in the Cisco ASR 5000 Series Session Control Manager Administration Guide for more information about regular expressions.

```
subscriber-capability capability_type
```

Filters based on the capability of the subscriber.

- `at` - Custom AT Type
- `audio` - Audio Capability Type
- `chat` - Custom CHAT Type
- `cs` - Custom CS Type
- `ft` - Custom FT Type
- `im` - Custom IM Type
- `lte-voip` - Custom LTE-VOIP Type
- `lte-vt` - Custom LTE-VT Type
- `mms` - Custom MMS Type
- `msg` - Custom MSG Type
- `oma-sip-im` - Custom OMA SIP-IM Type
- `rcs-dp` - Custom RCS-DP Type
- `rcs-e` - Custom RCS-E Type
- `rcs-ft` - Custom RCS-FT Type
- `rcs-im` - Custom RCS-IM Type
- `rcs-is` - Custom RCS-IS Type
- `rcs-sp` - Custom RCS-SP Type
- `rcs-vs` - Custom RCS-VS Type
- `smart-edu` - Custom SMART-EDU Type
- `text` - Text Capability Type
- `video` - Video Capability Type
- `vt` - Custom VT Type
- `vt-ft` - Custom VT-FT Type
- `vt-is` - Custom VT-IS Type
- `vt-loc` - Custom VT-LOC Type
- `vt-memo` - Custom VT-MEMO Type

```
subscriber-ip-type { v4 | v6 }
```

Filters based on the IP type of the subscriber.

- `v4` - IPv4 type
- `v6` - IPv6 type

```
user-agent value
```

Filters based on the User-Agent Header value.
aaa-group

value must be from 1 to 127 alpha and/or numeric characters.

+ This symbol indicates that the keywords can be entered multiple times within a single command.

no Removes configured diameter selection entry.

Usage

This command configures matching criteria for selecting a AAA group name. When a subscriber registers, the selection criteria are compared and the AAA group name from the matching entry will be picked up. The selected aaa-group will be used for all CDF (enabled for a given access type) or HSS interactions for that subscriber.

Example

The following command creates a diameter selection entry named aaa1, with a destination AoR criteria of $.@abc123.com and preference 125 associated with it:

    aaa-group aaa1 preference 125 criteria aor $.@abc123.com

The following command (immediately following in the configuration file) creates a diameter selection entry named aaa2, with a destination AoR criteria of user@cisco.com and preference 126 automatically associated with it:

    aaa-group aaa2 criteria aor user@cisco.com
**end**

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**

Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

```bash
exit
```

**Usage**

Use this command to return to the parent configuration mode.
Chapter 76
CSCF EATF Configuration Mode Commands

The CSCF EATF Configuration Mode is used to set commands for enabling service continuity of IMS emergency sessions.

Mode

Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Emergency-CSCF Configuration > CSCF EATF Configuration

configure > context context_name > cscf service service_name > emergency-cscf > eatf

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-cscf-eatf)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
**e-stn-sr**

This command adds the Emergency Session Transfer Number for Single Radio (E-STN-SR) to the EATF.

**Product**

SCM: E-CSCF

**Privilege**

Administrator

**Syntax**

```
e-stn-sr estnsr_num
no e-stn-sr
```

- **no**
  
  Removes E-STN-SR number from the E-CSCF.

- **estnsr_num**
  
  Specifies the E-STN-SR. `estnsr_num` must be a string of up to 15 digits (+ prefix may be added).

**Usage**

Use this command to configure E-STN-SR number for EATF service. EATF performs session continuity when the Access Transfer request indicated by the E-STN-SR is received.

**Example**

The following command sets the E-STN-SR number to **5656565**:

```
e-stn-sr 5656565
```
**end**

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
- All

**Privilege**
- Security Administrator, Administrator

**Syntax**

```plaintext
exit
```

**Usage**

Use this command to return to the parent configuration mode.
Chapter 77
CSCF Emergency-CSCF Configuration Mode Commands

The Emergency-CSCF Configuration Mode is used to set commands supporting the role of the CSCF service as an Emergency CSCF.

Mode

Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Emergency-CSCF Configuration

configure > context context_name > csdf service service_name > emergency-cscf

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-cscf-service-emergency-cscf)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
eatf

This command enables Emergency Call Access Transfers (EATF) functionality for the service. Default is disabled.

Product

SCM: E-CSCF

Privilege

Administrator

Mode

Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Emergency-CSCF Configuration

configure > context context_name > cscf service service_name > emergency-cscf

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-cscf-service-emergency-cscf)#

Syntax

[ no ] eatf

no

Removes EATF support from the E-CSCF.

Usage

Use this command to enable or disable EATF functionality in emergency-CSCF service. On entering this command, the CLI prompt changes to:

[context_name]host_name(config-cscf-eatf)#
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Use this command to return to the parent configuration mode.
plani

Sets parameters associated with P-LANI (P-Last-Access-Network-Info) header.

**Product**
SCM: E-CSCF

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Emergency-CSCF Configuration

```
configure > context context_name > cscf service service_name > emergency-cscf
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-service-emergency-cscf)#
```

**Syntax**

```
plani age seconds
```

**Syntax**

```
[ default | no ] plani age
```

---

`default`

Sets the acceptable P-LANI age to 7200 seconds.

---

`no`

Removes the acceptable P-LANI age configured for the E-CSCF.

---

`age seconds`

Specifies the acceptable P-LANI age from registration time.

`seconds` must be an integer from 1 to 65535.

Default: 7200

---

**Usage**

This command is used to identify location aging of subscriber is within acceptable limits.

Two timestamps are included in Emergency SIP INVITES P-LANI header to determine the “location age” of the last known cellular information at registration. The first timestamp shall be the date/time the P-LANI was captured. The second timestamp shall be the data and time of the Initial registration for voice services. The E-CSCF shall calculate the delta between the two timestamps to determine the P-LANI location age at registration. E-CSCF will compare the P-LANI location age to the “p-lani-acceptable-age” specified in this command. E-CSCF will omit/disregard the LDAP query for CGI location when “p-lani-acceptable-age” is exceeded.

**Example**

The following command sets the acceptable P-LANI age for the E-CSCF to 5000 seconds:

```
plani age 5000

The following command sets the acceptable P-LANI age for the E-CSCF to 7200 seconds:

default plani age

The following command removes the acceptable P-LANI age configured for the E-CSCF:

no plani age
privacy

Enables privacy support on the E-CSCF.

Product
SCM

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Emergency-CSCF Configuration

configure > context context_name > cscf service service_name > emergency-cscf

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-cscf-service-emergency-cscf)#

Syntax

[ no | default ] privacy

-----------

no | default

Removes privacy support from the E-CSCF.

Usage

Use this command to enable privacy support for Emergency CSCF service.
psap-file

Sets the location of the PSAP-Database file to maintain and access the ESRK-Ranges provided by the operator for the E-CSCF.

**Product**
SCM

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Emergency-CSCF Configuration

```
configure > context context_name > cscf service service_name > emergency-cscf
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-service-emergency-cscf)#
```

**Syntax**

```
psap-file file_name
no psap-file
```

- **file_name**

  Specifies the PSAP-Database file in one of the following formats:
  - ftp://[username]:[password]@host/[directory]/<filename> - URL
  - file://flash/[directory]/<filename> - URL
  - sftp://[username]:[password]@host/[directory]/<filename> - URL

**Usage**

This command is used by the SRDB proclet for ESRK-PSAP database management for the E-CSCF.

**Example**

The following command specifies a PSAP-Database file for the E-CSCF:

```
psap-file
ftp://[username]:[password]@10.6.2.246/home/nthattil/psap_profile_CSV_new1.csv
```
Chapter 78
CSCF Enforce Codec Policy Configuration Mode Commands

The CSCF Enforce Codec Policy Configuration Mode is used to manage audio and video codec policies within the system. The parameters defined in this chapter are derived from IETF RFC 3551: “RTP Profile for Audio and Video Conferences with Minimal Control”.

Mode

Exec > Global Configuration > Context Configuration > CSCF Policy Configuration > CSCF Policy Rules Configuration > Enforce Codec Policy Configuration

configure > context context_name > cscf policy { default | name policy_name } > service-policy-rules > enforce-codec-policy

—or-


configure > context context_name > cscf policy { default | name policy_name } > aor-policy-rules > aor aor_name > enforce-codec-policy

Entering the above command sequences results in the following prompt:

[context_name]host_name(config-policy-enforce-code)#

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
dynamic-codec

Creates a list of dynamic codecs supported by the system.

Product
SCM

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > CSCF Policy Configuration > CSCF Policy Rules Configuration > Enforce Codec Policy Configuration

configure > context context_name > cscf policy { default | name policy_name } > service-policy-rules > enforce-codec-policy

-or-


configure > context context_name > cscf policy { default | name policy_name } > aor-policy-rules > aor aor_name > enforce-codec-policy

Entering the above command sequences results in the following prompt:

[context_name]host_name(config-policy-enforce-code)#

Syntax

dynamic-codec { audio encoding_name | video encoding_name } [ clock_rate ] [ channels ]

default dynamic-codec

no dynamic-codec [ encoding_name ] [ clock_rate ] [ channels ]

default

Specifies that the default list of dynamic codecs is added to the allowed codecs list. Default dynamic codecs: H263 and AMR.

no

Specifies that all dynamic codecs are removed from the allowed codecs list. If an encoding_name is specified, then only the codec specified by the encoding_name is removed. Furthermore, if a supporting clock_rate and/or channels are specified, then only the encoding_name with the specified clock_rate and/or channels is removed.

audio encoding_name | video encoding_name

audio encoding_name: Specifies the encoding name of the dynamic audio codec added to the allowed codec list. encoding_name must be from 1 to 49 alpha and/or numeric characters.

video encoding_name: Specifies the encoding name of the dynamic video or audio-video codec added to the allowed codec list. encoding_name must be from 1 to 49 alpha and/or numeric characters.
CSCF Enforce Codec Policy Configuration Mode Commands

dynamic-codec

[ clock_rate ] [ channels ]

clock_rate: Specifies the sampling rate of the codec. clock_rate must be an integer from 0 to 1000000.
channels: Specifies the number of channels required by the codec. channels must be an integer from 1 to 1000000.

Valid dynamic audio codecs:

<table>
<thead>
<tr>
<th>Encoding Name</th>
<th>Clock Rate (Hz)</th>
<th>Channels</th>
</tr>
</thead>
<tbody>
<tr>
<td>G726-40</td>
<td>8,000</td>
<td>1</td>
</tr>
<tr>
<td>G726-32</td>
<td>8,000</td>
<td>1</td>
</tr>
<tr>
<td>G726-24</td>
<td>8,000</td>
<td>1</td>
</tr>
<tr>
<td>G726-16</td>
<td>8,000</td>
<td>1</td>
</tr>
<tr>
<td>G729D</td>
<td>8,000</td>
<td>1</td>
</tr>
<tr>
<td>G729E</td>
<td>8,000</td>
<td>1</td>
</tr>
<tr>
<td>GSM-EFR</td>
<td>8,000</td>
<td>1</td>
</tr>
<tr>
<td>L8</td>
<td>Variable</td>
<td>Variable</td>
</tr>
<tr>
<td>RED</td>
<td>See RFC3551</td>
<td></td>
</tr>
<tr>
<td>VDVI</td>
<td>Variable</td>
<td>1</td>
</tr>
</tbody>
</table>

Valid dynamic video codecs:

<table>
<thead>
<tr>
<th>Encoding Name</th>
<th>Clock Rate (Hz)</th>
</tr>
</thead>
<tbody>
<tr>
<td>H263-1998</td>
<td>90,000</td>
</tr>
</tbody>
</table>

Usage

Use this command to create a list of supported dynamic audio and video codecs in the system. When a request is received by the CSCF, the SDP fields in the message are checked to determine the codec being used. The codec in the SDP fields must match a codec in the allowed codec list or the CSCF rejects the request.

Example

The following command adds the GSM-EFR codec to the allowed dynamic codec list:

    dynamic-codec GSM-EFR
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**

Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

exit

Usage
Use this command to return to the parent configuration mode.
static-codec

Creates a list of static codecs supported by the system.

Product
SCM

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > CSCF Policy Configuration > CSCF Policy Rules Configuration > Enforce Codec Policy Configuration

configure > context context_name > cscf policy { default | name policy_name } > service-policy-rules > enforce-codec-policy

--or--


configure > context context_name > cscf policy { default | name policy_name } > aor-policy-rules > aor aor_name > enforce-codec-policy

Entering the above command sequences results in the following prompt:

[context_name]host_name(config-policy-enforce-code)#

Syntax

static-codec { audio payload_type | video payload_type }

default static-codec

no static-codec [ payload_type ]

default

Specifies that the default list of static codecs is added to the allowed codecs list. The default static codec is 5: DVI4.

no

Specifies that all static codecs are removed from the allowed codecs list. If a payload_type is specified, then only the codec specified by the payload_type is removed.

audio payload_type | video payload_type

audio payload_type: Specifies the audio codec added to the allowed codecs list. payload_type must be an integer from 0 to 95. Default value is 5.

Valid static audio codecs:

<table>
<thead>
<tr>
<th>audio payload_type</th>
<th>0: PCMU</th>
<th>7: LPC</th>
<th>14: MPA</th>
<th>21: unassigned</th>
</tr>
</thead>
<tbody>
<tr>
<td>1: reserved</td>
<td>1: reserved</td>
<td>8: PCMA</td>
<td>15: G728</td>
<td>22: unassigned</td>
</tr>
<tr>
<td>2: reserved</td>
<td>9: G722</td>
<td>16: DVI4</td>
<td>23: unassigned</td>
<td></td>
</tr>
</tbody>
</table>
video payload_type: Specifies the video or audio-video codec added to the allowed codecs list. payload_type must be an integer from 0 to 95. Default value is 5.

Valid static video codecs:

<table>
<thead>
<tr>
<th>Payload Type</th>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>24</td>
<td>unassigned</td>
<td>72-76: reserved</td>
</tr>
<tr>
<td>25</td>
<td>CelB</td>
<td>77-95: unassigned</td>
</tr>
<tr>
<td>26</td>
<td>JPEG</td>
<td>35-71: unassigned</td>
</tr>
</tbody>
</table>

Usage

Use this command to create a list of supported static audio and video codecs in the system. When a request is received by the CSCF, the SDP fields in the message are checked to determine the codec being used. The codec in the SDP fields must match a codec in the allowed codec list or the CSCF rejects the request.

Example

The following command adds the G729 audio codec to the allowed codecs list:

```
static-codec 18
```
Chapter 79
CSCF IFC SPT Group Mode Commands

The CSCF iFC SPT Group Configuration Mode is used to associate individual SPT conditions with an Initial Filter Criteria (iFC) Service Point Trigger (SPT) group.

**Mode**

Exec > Global Configuration > Context Configuration > CSCF IFC SPT Group Configuration

`configure > context context_name > cscf ifc-spt-group id group_id`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-ifc-spt-group)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Use this command to return to the parent configuration mode.
spt-condition

Assigns iFC SPT conditions to an existing iFC SPT group.

Product
SCM (S-CSCF, SIP Proxy)

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > CSCF IFC SPT Group Configuration
   configure > context context_name > cscf ifc-spt-group id group_id

Entering the above command sequence results in the following prompt:
   [context_name]host_name(config-cscf-ifc-spt-group)#

Syntax
[ no ] spt-condition id cond_id

   no
   Removes the specified CSCF iFC SPT condition from the iFC SPT group.

   spt-condition id cond_id
   Specifies the name of an existing iFC SPT condition.
   cond_name must be an integer from 1 to 200.

Usage
Use this command to associate individual SPT conditions with an iFC SPT group.

Important: An iFC SPT group may be associated with multiple SPT conditions.

Example
The following command assigns 2 to an iFC SPT group:
   spt-condition id 2
Chapter 80
CSCF IFC Trigger Point Mode Commands

The CSCF iFC Trigger Point Configuration Mode is used to associate an Initial Filter Criteria (iFC) Service Point Trigger (SPT) group with an iFC trigger point.

```
Mode
Exec > Global Configuration > Context Configuration > CSCF IFC Trigger Point Configuration
configure > context context_name > cscf ifc-trigger-point id trigger_point_id condition-
type { cnf | dnf }
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-ifc-trigger-point)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**
Use this command to return to the Exec mode.
**exit**

Exits the current mode and returns to the parent configuration mode.

**Product**  
All

**Privilege**  
Security Administrator, Administrator

**Syntax**  
```
exit
```

**Usage**  
Use this command to return to the parent configuration mode.
**spt-group**

Assigns an existing iFC SPT group to an iFC trigger point.

**Product**
SCM (S-CSCF, SIP Proxy)

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF IFC Trigger Point Configuration

```
configure > context context_name > csf ifc-trigger-point id trigger_point_id condition-type { cnf | dnf }
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-ifc-trigger-point)#
```

**Syntax**

```
[ no ] spt-group id group_id
```

- **no**
  
  Removes the specified CSCF iFC SPT group from the iFC trigger point.

- **spt-group id group_id**
  
  Specifies the ID of an existing iFC SPT group.
  
  `group_id` must be an integer from 1 to 200.

**Important:** An iFC SPT group can be assigned to more than one iFC trigger point.

**Usage**

Use this command to associate an iFC SPT group with an iFC trigger point.

**Example**

The following command assigns iFC SPT group 2 to an iFC trigger point:

```
spt-group id 2
```
Chapter 81
CSCF ISC Template Configuration Mode Commands

The CSCF ISC Template Configuration Mode is used to configure the IMS Service Control (ISC) interface within the system.

Mode

Exec > Global Configuration > Context Configuration > CSCF ISC Template Configuration
configure > context context_name > cscf isc-template id template_id

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-cscf-isc-tmpl)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
**cnsa**

Core Network Service Authorization (CNSA) related commands used to create media profile and service ids.

**Product**  
SCM (S-CSCF)

**Privilege**  
Administrator

**Mode**  
Exec > Global Configuration > Context Configuration > CSCF ISC Template Configuration

```
configure > context context_name > cscf isc-template id template_id
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-isc-tmpl)#
```

**Syntax**

```
cnsa { media-profile-id profile_id | service-id service_id [ service_id ]...[ service_id ] }
```

```
no cnsa { media-profile-id | service-id [ service_id ] [ service_id ]...[ service_id ] }
```

- **media-profile profile_id**
  - Specifies the cnsa media profile id.
  - *profile_id* must be an integer from 0 to 10.
  - The media profile id is assigned to a service policy using the `cnsa-media-profile` command under CSCF Service configuration.

**Important:** You can only create one media profile id per ISC template.

- **service-id service_id**
  - Specifies the cnsa service id(s). These ids represent URN parameters which are ICSI (IMS Communication Service Identifier) values that are mapped to a service profile through a media profile id.
  - *service_id* must be from 1 to 79 alpha and/or numeric characters.

```
no cnsa { media-profile-id | service-id [ service_id ] [ service_id ]...[ service_id ] }
```

Removes a media profile or service id(s).

**Usage**

Use this command to configure cnsa media profile ids and service ids. Information for core network authorization is received from HSS. It contains a list of service ids and a media profile id. Since the media profile id is an integer value, the S-CSCF needs to have a static database that contains the mapping between the integer value and the subscribed media profile. The media profile id is assigned to this service policy using the `cnsa-media-profile` command under CSCF Service configuration.
The S-CSCF selects the service profile based on the media profile id set and the policies, such as enforce-codec-policy and video-sessions, will be matched with the incoming request. Other policies, if configured, will be ignored in this scenario.

**Example**

The following command defines the media profile id as 2:

```
cnsa media-profile-id 2
```

The following command defines several service ids:

```
cnsa service-id xxx:exampletelephony.version1 xxx:abc.com
```
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

exit

Usage
Use this command to return to the parent configuration mode.
**filter-criteria**

Configure the filter criteria to be used by this template.

**Product**

SCM (S-CSCF)

**Privilege**

Administrator

**Mode**

Exec > Global Configuration > Context Configuration > CSCF ISC Template Configuration

```
configure > context context_name > cscf isc-template id template_id
```

Entering the above command sequence results in the following prompt:

```
[context_name] host_name(config-cscf-isc-tmpl)#
```

**Syntax**

```
[ no ] filter-criteria id criteria_id
```

- **no**
  - Removes the specified filter criteria.

- **id criteria_id**
  - Specifies the ID of existing filter criteria to be used by this template. The particular criteria applied to a subscriber will be based on the priority parameter. `criteria_id` must be an integer from 1 to 200.

---

**Important:** Filter criteria can be assigned to more than one ISC template.

**Usage**

Use this command to configure the filter criteria to be used by this template.

**Example**

The following command identifies the filter criteria 1:

```
filter-criteria id 1
```
Chapter 82
CSCF Last Route Profile Criteria Configuration Mode Commands

The CSCF Last Route Profile Criteria Configuration Mode is used to configure county names and assign them Last Routing Option (LRO) numbers to be used by the CSCF last route profile. The S-CSCF forwards emergency call packets to the correct Public Safety Answering Point (PSAP) based on this criteria, which it receives from a peer server.

Mode

Exec > Global Configuration > Context Configuration > CSCF Last Route Profile Criteria Configuration

configure > context context_name > csf last-route-profile name profile_name criteria { county-name | round-robin }

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-criteria_type-lro-profile)#

⚠️ Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
**county-name**

Configure county names and assign them Last Routing Option (LRO) numbers to be used by the CSCF last route profile.

**Product**
SCM (S-CSCF)

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Last Route Profile Criteria Configuration

```bash
configure > context context_name > cscf last-route-profile name profile_name criteria {
 county-name | round-robin }
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-criteria_type-lro-profile)#
```

**Syntax**

```bash
county-name county_name lro-number value

[ no ] county-name county_name
```

- `county-name` specifies the county name. `county_name` must be from 1 to 79 alpha and/or numeric characters in length.

- `lro-number value` specifies an existing LRO number. `value` can be a maximum of ten digits in length.

- `no county-name county_name` removes the specified county name.

**Usage**

Use this command to configure county names and assign them LRO numbers.

**Important:** You may configure up to 100 county names.

**Example**

The following command creates a county name called `norfolk` and assigns it an LRO number of `8884384357`:

```bash
county-name norfolk lro-number 8884384357
```
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.
Chapter 83
CSCF NPDB Client Configuration Mode Commands

The NPDB Client Configuration Mode is used to set various commands supporting the role of the NPDB (Number Portability Data Base) client. The NPDB client in a CSCF service performs query for called subscriber number on NPDB server, which returns the Routing Number for the query.

**Mode**

Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Serving-CSCF Configuration > NPDB Client Configuration

```
configure > context context_name > cscf service service_name > serving-cscf > npdb-client client_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-npdb-client)#
```

**Important**: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
bind

Binds the NPDB client to an IP address.

**Product**
SCM (S-CSCF)

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Serving-CSCF Configuration > NPDB Client Configuration

```
configure > context context_name > cscf service service_name > serving-cscf > npdb-client client_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-npdb-client)#
```

**Syntax**

```
bind address IPv4_address system-id system_id id client_id [ encrypted ] password password
```

```
no bind
```

**address IPv4_address**

Specifies the NPDB client IP address to establish the TCP connection with NPDB server.  
`IPv4_address` must be expressed in dotted decimal notation for IPv4.

**system-id system_id**

Specifies the identifier of the system performing query to NPDB server.  
`system_id` must be an unsigned integer from 0 to 4294962295.

**id client_id**

Specifies the ID of the NPDB client.  
`client_id` must be from 1 to 15 alpha and/or numeric characters.

```
[ encrypted ] password password
```

Specifies the password of the NPDB client and whether it is encrypted.  
`password` must be from 1 to 15 alpha and/or numeric characters.  
`encrypted password` must be from 1 to 132 alpha and/or numeric characters.

**Important:** Normally, encrypted passwords are only used inside configuration files

```
no bind
```

Removes the binding of the NPDB client.
Usage

Use this command to establish the NPDB client parameters for TCP connection with NPDB server.

**Important:** This command can be entered multiple times to identify multiple IP addresses.

In connected state, only NPDB client will able to send query messages to get routing number from NPDB server. When query message is received in non-connected state from core, the NPDB client sends an error message to CSCF core.

Example

The following command binds the NPDB client to an IP address of 1.2.3.4, system ID of 4294, client ID of asdds, and encrypted password A01h4b5t5rojj205dhrete:

```
bind address 1.2.3.4 system-id 4294 id asdds encrypted password A01h4b5t5rojj205dhrete
```
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
end

**Usage**
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Use this command to return to the parent configuration mode.
npdb-primary-server

Configure the NPDB primary server.

Product

SCM (S-CSCF)

Privilege

Administrator

Mode

Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Serving-CSCF Configuration > NPDB Client Configuration

configure > context context_name > cscf service service_name > serving-cscf > npdb-client client_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-npdb-client) #

Syntax

npdb-primary-server { address IPv4_address | domain domain } port port_number

no npdb-primary-server

address IPv4_address | domain domain

Specifies the NPDB primary server.

address IPv4_address: IP addresses must be expressed in dotted decimal notation for IPv4.

domain domain: Domain name must be entered using from 1 to 255 alpha and/or numeric characters.

port port_number

Specifies the port at which NPDB primary server listens.

port_number may be an integer from 1024 to 65534.

no

Removes the NPDB primary server.

Usage

Use this command to configure the NPDB primary server.

Example

The following command adds an NPDB primary server with an IP address of 1.2.3.4 and a port number of 3878:

npdb-primary-server address 1.2.3.4 port 3878
npdb-secondary-server

Configure the NPDB secondary server.

**Product**
SCM (S-CSCF)

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Serving-CSCF Configuration > NPDB Client Configuration

```
configure > context context_name > cscf service service_name > serving-cscf > npdb-client client_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-npdb-client)#
```

**Syntax**

```
npdb-secondary-server { address IPv4_address | domain domain } port port_number
no npdb-secondary-server
```

- **address IPv4_address | domain domain**
  Specifies the NPDB secondary server.
  - **address IPv4_address**: IP addresses must be expressed in dotted decimal notation for IPv4.
  - **domain domain**: Domain name must be entered using from 1 to 255 alpha and/or numeric characters.

- **port port_number**
  Specifies the port at which NPDB secondary server listens.
  - **port_number**: May be an integer from 1024 to 65534.

- **no**
  Removes the NPDB secondary server.

**Usage**
Use this command to configure the NPDB secondary server.

**Example**
The following command adds an NPDB secondary server with an IP address of 1.2.3.5 and a port number of 3878:

```
npdb-secondary-server address 1.2.3.5 port 3878
```
timeout

Sets timeout values for NPDB client.

Product
SCM (S-CSCF)

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Serving-CSCF Configuration > NPDB Client Configuration
configure > context context_name > cscf service service_name > serving-cscf > npdb-client client_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-npdb-client)#

Syntax

```
timeout { bind-response sec | error-response sec | idle sec | ping sec | ping-response sec | query-response sec | release-response sec | tcp-retry sec }
[ default | no ] timeout { bind-response | error-response | idle | ping | ping-response | query-response | release-response | tcp-retry }
```

```
bind-response sec
Default: 30
This timer is used to specify the timeout for connection path creation in seconds.
sec must be an integer from 1 to 5000.
```

```
error-response sec
Default: 30
This timer is used to specify the timeout for error response in seconds.
sec must be an integer from 1 to 5000.
```

```
idle sec
Default: 30
This timer is used to specify the timeout interval for retrying failed NPDB BIND in seconds.
sec must be an integer from 1 to 5000.
```

```
ping sec
Default: 20
This timer is used to specify the timeout to send ping message to make the connection alive in seconds.
sec must be an integer from 1 to 5000.
```

```
ping-response sec
Default: 30
```
This timer is used to specify the timeout for ping response in seconds. 
\( sec \) must be an integer from 1 to 5000.

query-response \( sec \)
Default: 6
This timer is used to specify the timeout for query response in seconds. 
\( sec \) must be an integer from 1 to 5000.

release-response \( sec \)
Default: 30
This timer is used to specify the timeout for release response in seconds. 
\( sec \) must be an integer from 1 to 5000.

tcp-retry \( sec \)
Default: 15
This timer is used to specify the timeout interval for retrying failed TCP connection in seconds. 
\( sec \) must be an integer from 1 to 5000.

default
Returns the command to the default settings. See keywords above for specific defaults.

no
Deletes the value configured for the specified timer.

Usage
Use this command to configure timeout values for NPDB client.
When CSCF service is started, NPDB client establishes TCP connections with NPDB primary and secondary servers (if configured) and sets the connection path by sending Bind message to server. If NPDB client fails to establish TCP connection to either of the servers, it will retry the connection every TCPRetryTimer interval until it is successful. When the connection is successful, NPDB client will go to the connected state and will start PingTimer. Whenever NPDB client receives service request from CSCF core, it sends the request based on the connected state of the server(s); it should always give higher preference to the primary server. When it fails to send a query message to server, NPDB client returns failure to the core. If both servers are not in connected state, NPDB client will send failure message to CSCF core.

Example
The following command sets the release response timeout to 64 seconds:

\[ \text{timeout release-response 64} \]
Chapter 84
CSCF PCRF-Policy-Control Configuration Mode Commands

The PCRF-Policy-Control Configuration Mode is used to enable PCRF policy control within the service.

**Mode**

Exec > Global Configuration > Context Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration > CSCF PCRF-Policy-Control Configuration

`configure > context context_name > cscf service service_name > proxy-cscf > pcrf-policy-control`

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-pcrf-policy-control)#`

**Important**: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
authorization inactive-media

Enables policy authorization for calls with inactive media.

**Product**
SCM (P-CSCF, A-BG)

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration > CSCF PCRF-Policy-Control Configuration

```
configure > context context_name > cscf service service_name > proxy-cscf > pcrf-policy-control
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcrf-policy-control)#
```

**Syntax**

```
[ default | no ] authorization inactive-media
```

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Calls with all media lines in the inactive state are authorized via Rx.</td>
</tr>
<tr>
<td>no</td>
<td>Calls with all media lines in the inactive state will not be authorized via Rx.</td>
</tr>
</tbody>
</table>

**Usage**

Use this command to enable or disable policy authorization for calls with inactive media. The media will be considered inactive when all m lines in SDP are in inactive state.

**Example**

The following command enables policy authorization for calls with inactive media:

```
authorization inactive-media
```
authorization mediatype

Enables media authorization, using external PCRF via Rx, of specific media types (present in the SDP of a SIP message) only.

**Product**
SCM (P-CSCF, A-BG)

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration > CSCF PCRF-Policy-Control Configuration

`configure > context context_name > csf service service_name > proxy-cscf > pcrf-policy-control`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcrf-policy-control)#
```

**Syntax**

```
[ no ] authorization mediatype { application | audio | control | data | message | others | text | video }
```

Enables the external authorization of calls for the following SDP media types:

- application
- audio
- control
- data
- message
- others
- text
- video

**Usage**

Disables external authorization for the specified media type.

**Example**

As Per 3GPP 29.214V8.5, P-CSCF/A-BG will authorize VOIP calls only for the media types enabled via this command. The P-CSCF/A-BG sends all media information for all supported media types present in SDP in AAR message to PCRF via Rx. For the other (unsupported) media types, P-CSCF will not send media information in AAR.

Be default, media authorization for all the media types is enabled.
Enables the P-CSCF to authorize calls for audio media types:

```
authorization mediatype audio
```

Disables the authorization of calls for audio media types:

```
no authorization mediatype audio
```
authorization policy-interworking-failure

Allows/rejects a session based on configuration in case of failure from PCRF.

**Product**
SCM (P-CSCF, A-BG)

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration > CSCF PCRF-Policy-Control Configuration

```
configure > context context_name > cscf service service_name > proxy-cscf > pcrf-policy-control
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcrf-policy-control)#
```

**Syntax**

```
authorization policy-interworking-failure { session-continue | session-reject [ response-code code ] }
```

**default** authorization policy-interworking-failure

```
    session-continue
    P-CSCF continues session in case of failure from PCRF.

    session-reject
    P-CSCF rejects session in case of failure from PCRF.

    response-code code
    Specifies SIP response code for rejected session.
    number must be an integer from 400 to 699. Default is 500.

    default
    By default, session-reject is activated to reject session with default response code 500.
```

**Usage**

Use this command to configure for policy interworking failure. Allow or reject a session based on configuration in case of failure from PCRF.

**Example**

The following command rejects session in case of failure from PCRF with SIP response code 450:

```
authorization policy-interworking-failure session-reject response-code 450
```
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

exit

Usage
Use this command to return to the parent configuration mode.
signaling-bearer-loss

Enables subscription to Notification of Signaling Transmission Path Status, as well as IPCAN Change type notification. This command is enabled by default.

Product
SCM (P-CSCF, A-BG)

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration > CSCF PCRF-Policy-Control Configuration

configure > context context_name > cscf service service_name > proxy-cscf > pcrf-policy-control

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pcrf-policy-control)#

Syntax

[ no ] signaling-bearer-loss subscription

no
Disables subscription to Notification of Signaling Transmission Path Status, as well as IPCAN Change type notification.

subscription
Enables subscription to Notification of Signaling Transmission Path Status, as well as IPCAN Change type notification.

Usage

Use this command to enable or disable subscription to Notification of Signaling Transmission Path Status, as well as IPCAN Change type notification.

When enabled, the P-CSCF/A-BG sends AAR to the external PCRF via the Rx interface after UE registration. When disabled, the P-CSCF/A-BG will not subscribe to any event during Registration with PCRF and no diameter session will be established.

Example

Enables subscription to Notification of Signaling Transmission Path Status, as well as IPCAN Change type notification:

signaling-bearer-loss subscription

Disables subscription to Notification of Signaling Transmission Path Status, as well as IPCAN Change type notification:

no signaling-bearer-loss subscription
Chapter 85
CSCF Peer Servers Configuration Mode Commands

The CSCF Peer Servers Configuration Mode is used to configure peer servers (for next-hop session routes) within the system.

**Mode**

Exec > Global Configuration > Context Configuration > CSCF Peer Servers Configuration

```bash
configure > context context_name > cscf peer-servers server_name type { bgcf | ibcf | icscf | mgcf | mrcf | pcscf | scscf | sip-as }
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-peer-servers-group)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**

Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
\texttt{exit}

Usage
Use this command to return to the parent configuration mode.
hunting-method

Configures the method by which server is contacted.

Product
SCM

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > CSCF Peer Servers Configuration

configure > context context_name > cscf peer-servers server_name type { bgcf | ibcf | icscf | mgcf | mrcf | pcscf | scscf | sip-as }

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-cscf-peer-servers-group)#

Syntax

hunting-method { round-robin | sequence-on-failure | weighed }

default hunting-method

default

Specifies that the server will be used in round-robin fashion.

round-robin | sequence-on-failure | weighed

Specifies the hunting method for the server.

round-robin: Specifies that the server will be used in round-robin fashion. This is the default setting.

sequence-on-failure: Specifies that the server will be used sequentially if a failure occurs on a server (i.e., first peer server is always used, except on failure, during which next peer server in the list will be used).

weighed: Specifies that the peer server has a set “weight” that determines use as compared to the other like-configured peer servers. The actual weight of the peer server is configured in the server command in this mode.

Usage

Use this command to configure the method that is used by the system to connect to the peer server.

Example

The following command sets the hunting method for a server to contact sequentially only when a server fails:

hunting-method sequence-on-failure
server

Configures the name, IP address, and port of servers belonging to this peer server and enters the Server Configuration Mode.

Product
SCM

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > CSCF Peer Servers Configuration

configure > context context_name > cscf peer-servers server_name type { bgcf | ibcf | icscf | mgcf | mrcf | pcscf | scscf | sip-as }

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-cscf-peer-servers-group)#

Syntax

server name { address ip_address | domain domain_name } [ port number ] [ transport { tcp | udp } ] [ weight number ]

no server name

no

Removes the specified server from the group.

name

Specifies a name for the server. name must be from 1 to 79 alpha and/or numeric characters in length.

address ip_address

Specifies the IP address of the server. ip_address is expressed in dotted decimal notation for IPv4 or colon notation for IPv6.

domain domain_name

Specifies the domain name of the peer server. domain_name must be from 1 to 255 alpha and/or numeric characters in length.

port number

Specifies the port number of the server. number must be an integer value from 1 to 65535.

transport { tcp | udp }

Specifies the transport type (TCP or UDP).
weight number

Default: 5
Specifies a weighted number for the specific peer server for load balancing purposes. number must be an integer value from 1 to 10. Higher weight implies larger server capability (and more routed requests).

**Important:** This keyword is only valid if the `weighed` keyword is applied to the `hunting-method` command in this mode.

---

Usage

Use this command to configure servers and enter the Server Configuration Mode.
Entering this command results in the following prompt:

```
[context_name]hostname(config-server_name-peer-server)#
```

Server Configuration Mode commands are defined in the *CSCF Peer Server Monitoring Configuration Mode Commands* chapter.

Example

The following command configures a server named `scscf5` with an IP address of `1.2.3.4` and a port number of `5060`:

```
server scscf5 address 1.2.3.4 port 5060
```
Chapter 86
CSCF Peer Servers Group Configuration Mode Commands

The CSCF Peer Servers Group Configuration Mode is used to configure peer servers lists within a peer servers group.

Mode

Exec > Global Configuration > Context Configuration > CSCF Peer Servers Group Configuration
configure > context context_name > cscf peer-servers-group group_name type sip-as

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-cscf-peer-servers-group)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
dc
```

**Usage**

Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**
Use this command to return to the parent configuration mode.
peer-servers

Configures peer servers lists in the peer servers group.

Product
SCM

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > CSCF Peer Servers Group Configuration

configure > context context_name > csf peer-servers-group group_name type sip-as

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-csf-peer-servers-group)#

Syntax

peer-servers list_name { default | mode { active | standby } }

no peer-servers list_name

list_name
Specifies a name for the peer servers list. list_name must be from 1 to 79 alpha and/or numeric characters in length.

default
Specifies that the peer servers list is default.

mode { active | standby }
Specifies whether the peer servers list is active or standby.

no peer-servers list_name
Removes the specified peer servers list from the group.

Usage
Use this command to manage peer servers lists in a peer servers group.

Important: There can be one active, one standby, and one default peer servers list in a peer servers group.

Example

The following command configures an active peer servers list named active_as_list:

    peer-servers active_as_list mode active
Chapter 87
CSCF Peer Server Monitoring Configuration Mode Commands

The CSCF Peer Server Monitoring Configuration Mode is used to configure an individual peer server’s monitoring parameters and operational mode. It also associates a network session template with the server.

Mode

Exec > Global Configuration > Context Configuration > CSCF Peer Servers Configuration > Server Configuration

```
configure > context context_name > cscf peer-servers server_name type { bgcf | ibcf | icscf | mgcf | mrfc | pcscf | scscf | sip-as } > server server_name { address ip_address | domain domain_name }
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-server_name-peer-server)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
**dummy-as**

Sets a response code for Dummy-AS peer server.

**Product**
SCM (S-CSCF)

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Peer Servers Configuration > Server Configuration

```
configure > context context_name > cscf peer-servers server_name type { bgcf | ibcf | icscf | mgcf | mrscf | pcscf | scscf | sip-as } > server server_name { address ip_address | domain domain_name }
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-server_name-peer-server)#
```

**Syntax**

```
dummy-as custom-response-code SIP_response_code
```

```
default dummy-as custom-response-code
```

```
custom-response-code SIP_response_code
```

If the peer server is configured as dummy-as and it is chosen as per routing table configured, a UMM response message will be formed with the response code configured and sent as reply to incoming MESSAGE/PUBLISH requests.

`SIP_response_code` must be an integer from 200 to 699.

**Important:** The response code can be 2xx/4xx/5xx/6xx; 3xx,401,and 407 are not allowed.

```
default dummy-as custom-response-code
```

Sets the response code to 200.

**Usage**
Use this command to configure a response code for Dummy-AS. If this mode is selected, then MESSAGE/PUBLISH requests will be responded to by S-CSCF with configured response code.

**Example**
The following command configures AS as Dummy-AS with a corresponding response code of 425:

```
dummy-as custom-response-code 425
```
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

`exit`

**Usage**

Use this command to return to the parent configuration mode.
**ims-capable**

Indicates whether the peer server belongs to a 3GPP/IMS network or a non-IMS network such as the Internet. This command is used to determine at the S-CSCF whether SIP signaling inter-working is needed when the calls are forwarded to external networks.

**Product**
SCM (S-CSCF)

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Peer Servers Configuration > Server Configuration

```bash
configure > context context_name > cscf peer-servers server_name type { bgcf | ibcf | icscf | mgcf | mrcf | pcscf | scscf | sip-as } > server server_name { address ip_address | domain domain_name }
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-server_name-peer-server)#
```

**Syntax**

```
[ no ] ims-capable
```

- **no**

  Removes the identification of “IMS capable” from the selected peer server.

**Usage**

Use this command to identify a peer server as IMS capable allowing the S-CSCF to use SIP signalling inter-working when forwarding calls to non-IMS capable networks.
Iro-selection-profile

Binds a CSCF last route profile with the peer server.

**Product**
SCM

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Peer Servers Configuration > Server Configuration

`configure > context context_name > cscf peer-servers server_name type { bgcf | ibcf | icscf | mgcf | mrcf | pcsf | scscf | sip-as } > server server_name { address ip_address | domain domain_name }

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-server_name-peer-server)#
```

**Syntax**

```
Iro-selection-profile name profile_name
no Iro-selection-profile
```

**Iro-selection-profile name profile_name**

`profile_name` must be an existing CSCF last route profile and be from 1 to 79 alpha and/or numeric characters.

**no Iro-selection-profile**

Removes CSCF last route profile from the peer server group.

**Usage**

Use this command to identify a CSCF last route profile to use for finding the correct Public Safety Answering Point (PSAP) during emergency calls.

**Example**

The following command assigns a CSCF last route profile named `lro1` to the peer server group:

```
Iro-selection-profile name lro1
```

The following command removes a CSCF last route profile from the peer server group:

```
no Iro-selection-profile
```
### mode

Sets the peer server mode to either active or standby. By default, peer servers are in active mode.

**Product**
SCM

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Peer Servers Configuration > Server Configuration

```
configure > context context_name > cscf peer-servers server_name type { bgcf | ibcf | icscf | mgcf | mrcf | pcscf | scscf | sip-as } > server server_name { address ip_address | domain domain_name }
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-server_name-peer-server)#
```

**Syntax**

```
mode { active | standby }
```

<table>
<thead>
<tr>
<th>active</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defines the mode of the CSCF peer server as active.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>standby</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defines the mode of the CSCF peer server as standby.</td>
</tr>
</tbody>
</table>

**Usage**

Use this command to set the peer server mode to either active or standby.

**Example**

The following command sets the peer server’s mode to standby:

```
mode standby
```
monitor-status

Sets parameters for monitoring the status of peer servers.

Product
SCM

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > CSCF Peer Servers Configuration > Server Configuration

```
configure > context context_name > cscf peer-servers server_name type { bgcf | ibcf | icscf | mgcf | mrcf | pcscf | scscf | sip-as } > server server_name { address ip_address | domain domain_name }
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-server_name-peer-server)#
```

Syntax

```
monitor-status { max-response-codes negative max | [ monitor-interval seconds ] } [ monitor-message options [ max-forwards max | response-timer seconds ] ] [ monitor-response-timer seconds ] | response-code { positive SIP_response_code | negative SIP_response_code } | timer [ mark-out-of-service seconds ] [ unavailable-monitor-interval seconds ] [ unavailable-notification seconds ] }

no monitor-status { monitor | response-code [ negative | positive ] [ SIP_response_code ] }
```

---

**max-response-codes negative max**

Default: 1
Specifies the maximum number of negative response codes to receive to mark server unavailable.
`max` must be an integer from 1 to 10.

**monitor-interval seconds**

Default: 30
Specifies the interval that peer server monitoring will occur.
`seconds` must be an integer from 1 to 65535.

**monitor-message options [ max-forwards max | response-timer seconds ]**

Specifies that SIP message (OPTIONS) are to be sent periodically after each monitoring interval.
`max-forwards max`: Max-forwards in number of hops. `max` must be an integer from 0 to 70.
`response-timer seconds`: Response wait timer in seconds. `seconds` must be an integer from 1 to 65535.

**monitor-response-timer seconds**

Default: 180
Specifies the interval that the CSCF will wait for responses from the peer server.
`seconds` must be an integer from 1 to 65535.
response-code { positive SIP_response_code | negative SIP_response_code }

Specifies the Options Message response codes.  

**negative**: Negative response codes.  *SIP_response_code* must be an integer from 300 to 699.  

**positive**: Positive response codes.  *SIP_response_code* must be an integer from 200 to 299.

timer mark-out-of-service seconds

Default: 864000

Timer to mark server out-of-service from unavailable state.  

seconds must be an integer from 0 to 2147483646.

timer unavailable-monitor-interval seconds

Periodic monitor interval to be used when server is marked as unavailable.  

seconds must be an integer from 0 to 2147483646.

timer unavailable-notification seconds

Default: 180

Time after which to send notification to operations administrator.  

seconds must be an integer from 0 to 2147483646.

no monitor-status { monitor | response-code [ negative | positive ] [ SIP_response_code ] }

Disables peering server status monitoring.

**Usage**

Use this command to set parameters for monitoring the status of a peer server.

**Example**

The following command sets the monitoring interval to three minutes (*180* seconds) and the response timer to six minutes (*360* seconds):

```
    monitor-status monitor-interval 180 monitor-response-timer 360
```
nw-session-template

Specifies a session template for sessions terminating from the peer server group.

**Product**
SCM

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Peer Servers Configuration > Server Configuration

```
configure > context context_name > cscf peer-servers server_name type { bgcf | ibcf | icscf | mgcf | mrcf | pcscf | scscf | sip-as } > server server_name { address ip_address | domain domain_name }
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-server_name-peer-server)#
```

**Syntax**

```
nw-session-template name template_name

no nw-session-template
```

**Example**

```
nw-session-template name template_name
```

`name template_name`

`template_name` must be an existing session template created in the Session Template Configuration Mode.

```
n
```

Removes session template from the peer server group.

**Usage**

Use this command to identify a session template to use for sessions terminating from the peer server group.

```
Example
```

The following command identifies a session template named `template-25` to use for sessions terminating from the peer server group:

```
nw-session-template template-25
```
**registration**

This command specifies whether the S-CSCF skips third party registration to the Application Server (AS) by a configured time after initial registration.

**Product**
SCM (S-CSCF)

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Peer Servers Configuration > Server Configuration

```
configure > context context_name > cscf peer-servers server_name type { bgcf | ibcf | icscf | mgcf | mrcf | pcscf | scscf | sip-as } > server server_name { address ip_address | domain domain_name }
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-server_name-peer-server)#
```

**Syntax**

```
registration skip-count count
no registration skip-count
```

**skip-count count**

Number of times to skip third party registration.

`count` must be an integer from 0 (default) to 60.

**no registration skip-count**

The S-CSCF does not skip third party registration to the AS by a configured time after initial registration.

**Usage**
Use this command to specify whether the S-CSCF skips third party registration to the Application Server (AS) by a configured time after initial registration. After skipping the configured number of times, the third party register should be sent again to AS to reduce overload on AS.

**Example**

The following command sets the number of times to skip third party registration to 25:

```
registration skip-count 25
```
tps-rate

Controls the rate of messages based on Transactions Per Second (TPS) from S-CSCF towards the peer server application server (AS).

**Product**
SCM (S-CSCF)

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Peer Servers Configuration > Server Configuration

```bash
configure > context context_name > cscf peer-servers server_name type { bgcf | ibcf | icscf | mgcf | mrpf | pcscf | scscf | sip-as } > server server_name { address ip_address | domain domain_name }
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-server_name-peer-server)#
```

**Syntax**

```
tps-rate rate [ exclude Register ]
```

no tps-rate

- **rate**
  TPS from S-CSCF towards the peer server AS.
  *rate* must be an integer from 1 to 1000.

- **exclude Register**
  Specifies that for Register method, TPS rate need not be applied.

no

TPS rate not applied from S-CSCF towards the peer server AS.

**Usage**

Use this command to control the TPS towards the peer server AS. If TPS rate is exceeded, the incoming requests will be rejected with 500 error response; Retry-After Header specifies the number of seconds before UE should retry.

**Example**

The following command sets the TPS rate towards the AS to 25:

```
tps-rate 25
```
Chapter 88
CSCF Policy Configuration Mode Commands

The CSCF Policy Configuration Mode is used to manage AoR policy profiles within the system. User-defined profiles can be managed in this mode.

Mode

Exec > Global Configuration > Context Configuration > CSCF Policy Configuration

configure > context context_name > cscf policy name policy_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-aor-policy)#

⚠️ *Important:* The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
**aor-policy-rules**

Specifies that the newly created policy is an AoR policy and enters the AoR Policy Rules Configuration Mode.

**Product**

SCM

**Privilege**

Administrator

**Mode**

Exec > Global Configuration > Context Configuration > CSCF Policy Configuration

```plaintext
configure > context context_name > cscf policy name policy_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-aor-policy)#
```

**Syntax**

```plaintext
aor-policy-rules
```

**Usage**

Use this command to create an AoR policy group and enter the AoR Policy Rules Configuration Mode. Entering this command results in the following prompt:

```
[context_name]host_name(config-aor-policy)#
```

AoR Policy Configuration Mode commands are defined in the *CSCF AoR Policy Rules Configuration Mode Commands* chapter.
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Use this command to return to the parent configuration mode.
service-policy-rules

Specifies that the newly created policy is a service policy and enters the Service Policy Rules Configuration Mode.

Product
SCM

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > CSCF Policy Configuration

configure > context context_name > cscf policy name policy_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-aor-policy)#

Syntax

service-policy-rules

Usage
Use this command to create a service policy group and enter the CSCF Policy Rules Configuration Mode. Entering this command results in the following prompt:

[context_name]host_name(config-service-policy)#

Service Policy Rule Configuration Mode commands are defined in the CSCF Policy Rules Configuration Mode Commands chapter.
Chapter 89
CSCF Policy Rules Configuration Mode Commands

The CSCF Policy Rules Configuration Mode is used to manage CSCF AoR and service policy profiles within the system.

Mode

Exec > Global Configuration > Context Configuration > CSCF Policy Configuration > CSCF Policy Rules Configuration

configure > context context_name > cscf policy { default | name policy_name } > service-policy-rules

--or--

Exec > Global Configuration > Context Configuration > CSCF Policy Configuration > AoR Policy Configuration > CSCF Policy Rules Configuration

configure > context context_name > cscf policy { default | name policy_name } > aor-policy-rules > aor aor_name

Entering the above command sequences results in the following prompt:

[context_name]host_name(config-policy_name-aor)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
allow-noauth

Configures the policy to allow unauthenticated access. Default is disabled.

**Product**
SCM

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Policy Configuration > CSCF Policy Rules Configuration

configure > context context_name > cscf policy { default | name policy_name } > service-policy-rules

--or--

Exec > Global Configuration > Context Configuration > CSCF Policy Configuration > AoR Policy Configuration > CSCF Policy Rules Configuration

configure > context context_name > cscf policy { default | name policy_name } > aor-policy-rules > aor aor_name

Entering the above command sequences results in the following prompt:

```
[context_name]host_name(config-policy_name-aor)#
```

**Syntax**

```
[ default | no ] allow-noauth
```

<table>
<thead>
<tr>
<th>default</th>
<th>no</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disables the allow-noauth functionality for this policy.</td>
<td></td>
</tr>
</tbody>
</table>

**Usage**

Use this command to allow access to subscribers without authenticating them.
allow-unsecure

Configures the policy to allow access to the system without a security association. Default is disabled.

**Product**
SCM

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Policy Configuration > CSCF Policy Rules Configuration

```
configure > context context_name > cscf policy { default | name policy_name } > service-policy-rules
```

- or -

Exec > Global Configuration > Context Configuration > CSCF Policy Configuration > AoR Policy Configuration > CSCF Policy Rules Configuration

```
configure > context context_name > cscf policy { default | name policy_name } > aor-policy-rules > aor aor_name
```

Entering the above command sequences results in the following prompt:

```
[context_name]host_name(config-policy_name-aor)#
```

**Syntax**

```
[ default | no ] allow-unsecure
```

- **default**
  - **no**

  Disables the allow-unsecure functionality for this policy.

**Usage**

Use this command to enable the policy to provide subscriber access to system without a security association.
authorization

Configures the policy to allow early bandwidth, emergency, or provisional response authorization. Default is disabled.

**Product**
SCM

**Privilege**
Administrator

**Mode**

Exec > Global Configuration > Context Configuration > CSCF Policy Configuration > CSCF Policy Rules Configuration

```
configure > context context_name > cscf policy { default | name policy_name } > service-policy-rules
```

-or-

Exec > Global Configuration > Context Configuration > CSCF Policy Configuration > AoR Policy Configuration > CSCF Policy Rules Configuration

```
configure > context context_name > cscf policy { default | name policy_name } > aor-policy-rules > aor aor_name
```

Entering the above command sequences results in the following prompt:

```
[context_name]host_name(config-policy_name-aor)#
```

**Syntax**

```
[ no ] authorization { early-bandwidth | emergency { all | register | session } | prov-response }
```

- **early-bandwidth**
  Enables early bandwidth policy.

- **emergency { all | register | session }**
  Enables AA-Request (AAR) for emergency.
  - **all**: Enable AAR for emergency Register and Invite.
  - **register**: Enable AAR for emergency Register.
  - **session**: Enable AAR for emergency Invite.

- **prov-response**
  Enables AAR for provisional responses like 18X.

- **no**
  Disables the early bandwidth, emergency, or provisional response authorization functionality for this policy.
Usage

Use this command to enable the policy to provide early bandwidth, emergency, or provisional response authorization.
end

Ends the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**

Use this command to return to the Exec mode.
enforce-codec-policy

Enters the Enforce Codec Policy Command Mode where allowed static and dynamic codec lists are managed.

**Product**
SCM

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Policy Configuration > CSCF Policy Rules Configuration

```
configure > context context_name > cscf policy { default | name policy_name } > service-policy-rules
```

Exec > Global Configuration > Context Configuration > CSCF Policy Configuration > AoR Policy Configuration > CSCF Policy Rules Configuration

```
configure > context context_name > cscf policy { default | name policy_name } > aor-policy-rules > aor aor_name
```

Entering the above command sequences results in the following prompt:

```
[context_name]host_name(config-policy_name-aor)#
```

**Syntax**

```
[ default | no ] enforce-codec-policy
```

<table>
<thead>
<tr>
<th>default</th>
<th>no</th>
</tr>
</thead>
</table>

Disables the codec policy.

**Usage**

Use this command to enter the Enforce Codec Policy Configuration Mode. Entering this command results in the following prompt:

```
[context_name]hostname(config-policy-enforce-codec)#
```

CSCF Enforce Codec Policy Mode commands are defined in the *Enforce Codec Policy Configuration Mode Commands* chapter in this guide.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Use this command to return to the parent configuration mode.
**max-cscf-concurrent-sessions**

Configures the maximum number of concurrent sessions allowed per subscriber.

**Product**
SCM

**Privilege**
Administrator

**Mode**

Exec > Global Configuration > Context Configuration > CSCF Policy Configuration > CSCF Policy Rules Configuration

```bash
configure > context context_name > cscf policy { default | name policy_name } > service-policy-rules
```

-or-

Exec > Global Configuration > Context Configuration > CSCF Policy Configuration > AoR Policy Configuration > CSCF Policy Rules Configuration

```bash
configure > context context_name > cscf policy { default | name policy_name } > aor-policy-rules > aor aor_name
```

Entering the above command sequences results in the following prompt:

```
[context_name]host_name(config-policy_name-aor)#
```

**Syntax**

```
max-cscf-concurrent-sessions number
```

**default max-cscf-concurrent-sessions**

```
number
```

Default: 5

Specifies the number of concurrent sessions allowed per subscriber for this policy. `number` must be an integer from 1 to 100.

```
default
```

 Resets defaults for this command.

**Usage**

Use this command to set the maximum number of allowed sessions per subscriber for this policy. If enabled, the `subscriber-policy-override` command in the CSCF Service Configuration Mode overrides the service-level policy.

**Example**

The following command sets the maximum number of concurrent sessions for a subscriber using this policy to 7:

```
max-cscf-concurrent-sessions 7
```
policy

Configures the overload response for this policy. When the P-CSCF/A-BG becomes congested, this overload policy is used to reject subsequent sessions or redirect them to another server.

Product

SCM (P-CSCF, A-BG)

Privilege

Administrator

Mode

Exec > Global Configuration > Context Configuration > CSCF Policy Configuration > CSCF Policy Rules Configuration

configure > context context_name > cscf policy { default | name policy_name } > service-policy-rules

-or-

Exec > Global Configuration > Context Configuration > CSCF Policy Configuration > AoR Policy Configuration > CSCF Policy Rules Configuration

configure > context context_name > cscf policy { default | name policy_name } > aor-policy-rules > aor aor_name

Entering the above command sequences results in the following prompt:

[context_name]host_name(config-policy_name-aor)#

Syntax

policy overload { redirect address1 [ weight weight1 ] [ address2 [ weight weight2 ] ] ... | reject [ use-reject-code { admin-prohibited | insufficient-resources } ] }

default policy overload

no policy overload redirect address1[address2] ...

redirect address1 [ weight weight1 ] [ address2 [ weight weight2 ] ] ...

Specifies that upon policy overload, the system will redirect the session to another CSCF.
address1 must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6.
weight weight1: Defines the priority of the redirect address.
weight1 must be an integer from 1 to 10. Default is 1.

reject [ use-reject-code { admin-prohibited | insufficient-resources } ]

Specifies that upon policy overload, the system will reject the session. This is the default setting.
use-reject-code: Specifies that a reject code will be returned upon policy overload.
•admin-prohibited: Specifies that the “admin-prohibited” reject code will be returned upon policy overload.
•insufficient-resources: Specifies that the “insufficient resources” reject code will be returned upon policy overload. This is the default reject code.
default policy overload
Resets defaults for this command.

no policy overload redirect address1 [ address2 ] ...
Removes configured policy overload redirect address(es).

Usage
Use this command to define the response to an overload condition on the P-CSCF/A-BG using this AoR policy.

Example
The following command configures the policy overload response to redirect to a series of CSCFs with IP address of 1.2.3.4, 1.2.3.5, and 1.2.3.6 with respective priorities (weights) of 1, 3, and 2:

```
policy overload redirect 1.2.3.4 weight 1 1.2.3.5 weight 3 1.2.3.6 weight 2
```
qos

Configures QoS bandwidth settings for uplink and downlink specific to media types.

Product
SCM

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > CSCF Policy Configuration > CSCF Policy Rules
Configuration

```
configure > context context_name > cscf policy { default | name policy_name } > service-policies-rules
```

-or-

```
configure > context context_name > cscf policy { default | name policy_name } > aor-policies-rules > aor aor_name
```

Entering the above command sequences results in the following prompt:

```
[context_name]host_name(config-policy_name-aor)#
```

Syntax

```
qos bandwidth { media-type { audio | other | video } | { downlink | uplink } } [ peak value ]
```

- `bandwidth { downlink | uplink }`

  - `downlink`: Configures the downlink bandwidth.
  - `uplink`: Configures the uplink bandwidth.

- `peak value`

  Peak value of bandwidth in kilobits per second (kbit/s).

  - `value` must be an integer from 1 to 99999999.

- `media-type { audio | other | video }`

  Configures QoS bandwidth for media types.

  - `audio`: QoS bandwidth for audio media-type.
  - `other`: QoS bandwidth for media-types other than audio and video.
  - `video`: QoS bandwidth for video media-type.

Usage

The P-CSCF/A-BG fills the required bandwidth for downlink and uplink from the Session Description Protocol (SDP) in the message when communicating with an external policy server via Rx/Tx/Gq. Use this
command to configure the peak uplink and downlink bandwidth to be used when the SDP does not contain bandwidth. Bandwidth configuration can now be specified per media type.

Example

Set the media type to **audio** and peak uplink bandwidth to **256** kbit/s:

```
qos bandwidth media-type audio uplink peak 256
```
signalling-bearer-loss

This command enables or disables signalling bearer loss.

Product

SCM

Privilege

Administrator

Mode

Exec > Global Configuration > Context Configuration > CSCF Policy Configuration > CSCF Policy Rules Configuration

configure > context context_name > cscf policy { default | name policy_name } > service-policy-rules

–or–

Exec > Global Configuration > Context Configuration > CSCF Policy Configuration > AoR Policy Configuration > CSCF Policy Rules Configuration

configure > context context_name > cscf policy { default | name policy_name } > aor-policy-rules > aor aor_name

Entering the above command sequences results in the following prompt:

[context_name] host_name(config-policy_name-aor)#

Syntax

[ no ] signalling-bearer-loss de-register

no

Disables signalling bearer loss for this policy.

Usage

Use this command to trigger De-register request from P-CSCF to S-CSCF, and clear the entry of subscriber. When P-CSCF gets ASR for Signalling Bearer, it sends ASA response and triggers STR for same session ID.
video-sessions

Configures the policy to allow video bearers. Default is disabled.

Product
SCM

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > CSCF Policy Configuration > CSCF Policy Rules Configuration

configure > context context_name > cscf policy { default | name policy_name } > service-policy-rules

-or-

Exec > Global Configuration > Context Configuration > CSCF Policy Configuration > AoR Policy Configuration > CSCF Policy Rules Configuration

configure > context context_name > cscf policy { default | name policy_name } > aor-policy-rules > aor aor_name

Entering the above command sequences results in the following prompt:

[context_name]host_name(config-policy_name-aor)#

Syntax

[ default | no ] video-sessions

default | no

Disables the “allow video sessions” feature.

Usage

Use this command to allow video session via this policy.
Chapter 90
CSCF Prefix Table Configuration Mode Commands

The CSCF prefix table is used to configure for each number (or number prefix) whether it is ported and the SIP routing domain. Only one CSCF prefix table can be configured per context.

Mode

Exec > Global Configuration > Context Configuration > CSCF Prefix Table Configuration

configure > context context_name > cscf prefix-table

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-cscf-prefix-table)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
end

Exits the current configuration mode and returns to the Exec mode.

**Product**  
All

**Privilege**  
Security Administrator, Administrator

**Syntax**  
end

**Usage**  
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.
number

Determines for each number (or number prefix) in a prefix table whether it is ported and the SIP routing domain.

Product
SCM

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > CSCF Prefix Table Configuration

configure > context context_name > cscf prefix-table

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-cscf-prefix-table)#

Syntax

```
number number [ ported ] [ routing-domain domain_name ]
```

```
no number number
```

Specifies number or number prefix. `number` must be a string of digits from 1 to 31 and/or special character “$.”

**Important:** If the number is a prefix, it should end with “$.”

```
ported
```

The number (or number prefix) is in ported range and NPDB (Number Portability Data Base) has to be contacted.

```
routing-domain domain
```

Specifies the SIP routing domain for this number (or number prefix). `domain_name` must be from 1 to 79 alpha and/or numeric characters in length.

```
no number number
```

Removes the specified number or number prefix from the prefix table.

Usage

Use this command to determine whether each number (or number prefix) in a prefix table is ported and the SIP routing domain. The S-CSCF service will use the prefix table configured in its source context for the lookup.

Example

The following command specifies a ported number prefix named `821057$` with SIP routing domain `cisco.com`:
number 821057$ ported routing-domain cisco.com
Chapter 91
CSCF Proxy-CSCF Configuration Mode Commands

The Proxy-CSCF Configuration Mode is used to enable Diameter policy control within the service.

Mode

Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration

configure > context context_name > csf service service_name > proxy-csf

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-csf-service-proxy-csf)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
allow rfc3261-ua-interworking

Enables the function to allow IMS interworking with RFC3261 SIP User Agents.

Product
SCM (P-CSCF, A-BG)

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration
configure > context context_name > cscf service service_name > proxy-cscf

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-cscf-service-proxy-cscf)#

Syntax

[ no ] allow rfc3261-ua-interworking

no

Disables the interworking capability.

Usage

Use this command to enable the P-CSCF/A-BG to allow IMS interworking with RFC3261 SIP User Agents.
atcf-atgw

This command enables ATCF functionality for the P-CSCF.

**Product**
SCM (P-CSCF, A-BG)

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration

```
configure > context context_name > cscf service service_name > proxy-cscf
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-service-proxy-cscf)#
```

**Syntax**

```
[ no ] atcf-atgw
```

- **no**
  - Disables ATCF support for P-CSCF.

**Usage**

Use this command to enable or disable ATCF functionality for the P-CSCF. This command is disabled by default.

On entering this command, the CLI prompt changes to:

```
[context_name]host_name(config-cscf-atcf-atgw)#
```

Refer to the *CSCF ATCF-ATGW Configuration Mode Commands* chapter for additional information.
core-reg-expiry-time

Configures Registration Expiry Timer Handling in P-CSCF/A-BG to keep pin holes open in B2BUA mode.

Product
SCM (P-CSCF, A-BG)

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration
configure > context context_name > cscf service service_name > proxy-cscf

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-cscf-service-proxy-cscf)#

Syntax

core-reg-expiry-time sec

[ default | no ] core-reg-expiry-time

default
Sets the core-reg-expiry-time to 3600 seconds.

no
Disables the timer.

sec
Expiry age should be less than or equal to the maximum in seconds. Must be an integer from 300 to 86400.

Usage
Use this command to configure Registration Expiry Timer Handling in P-CSCF/A-BG to keep pin holes open in B2BUA mode.

Example
The following sets the core-reg-expiry-time to 4000 seconds:

core-reg-expiry-time 4000
**diameter**

This command:
- configures the Diameter dictionary used in this function.
- enables the selection of a Diameter host-select-template for PCRF server selection.
- configures the policy control origin endpoint used in this function.
- enables the selection of a Diameter policy control peer server providing Rx/Tx/Gq applications for this service.
- configures the Diameter requested timeout value used in this function.

**Product**
SCM (P-CSCF, A-BG)

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration

```
configure > context context_name > cscf service service_name > proxy-cscf
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-service-proxy-cscf)#
```

**Syntax**

```
diameter location-info { dictionary { e2custom01 | e2custom02 | e2custom03 | e2custom04 | e2custom05 | e2custom06 | e2custom07 | e2custom08 | e2custom09 | e2standard } | origin endpoint endpoint_name | peer-select peer peer_name [ peer-realm realm_name ] [ secondary-peer peer_name [ sec-peer-realm realm_name ] ] | request-timeout sec }
```

In StarOS v12.0 and earlier:

```
diameter policy-control { dictionary { Gq-custom | Gq-standard | Rq-custom | Rx-rel8 | Rx-standard | Tx-standard | custom01 | custom02 | custom03 | custom04 | custom05 | custom06 | custom07 | custom08 | custom09 } | origin endpoint endpoint_name | peer-select peer peer_name [ peer-realm realm_name ] [ secondary-peer peer_name [ sec-peer-realm realm_name ] ] | request-timeout sec }
```

In StarOS v12.2 and later:

```
diameter policy-control { dictionary { dynamic-load | gq-custom | gq-standard | rq-custom | rx-custom01 | rx-custom02 | rx-custom03 | rx-custom04 | rx-custom05 | rx-rel8 | rx-standard | tx-standard } | host-select-template name template_name | origin endpoint endpoint_name | peer-select peer peer_name [ peer-realm realm_name ] [ secondary-peer peer_name [ sec-peer-realm realm_name ] ] | request-timeout sec }
```

```
default diameter { location-info | policy-control } { dictionary | request-timeout }
```

```
no diameter { location-info | policy-control } [ host-select-template | origin endpoint | peer-select ]
```
**diameter**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Sets the Diameter’s location-info or policy control dictionary or requested timeout value as the default.</td>
</tr>
<tr>
<td>no</td>
<td>Removes the Diameter location-info or policy control origin endpoint or Diameter peer from the service.</td>
</tr>
</tbody>
</table>

**location-info**

Defines the E2 interface for location information.

```plaintext
dictionary { e2custom01...e2custom09 | e2standard }
custom01...custom09: Specifies that a customer-specific (custom) dictionary is to be used for expansion and behaviors.
e2standard: Specifies that the E2-Standard-Dictionary is to be used.
```

**Important:** If this keyword is not configured, the system defaults to the default dictionary (e2standard). In the Proxy-CSCF configuration, at any time, the location-info dictionary can either be an explicitly configured dictionary or the default dictionary. Hence, there is no corresponding “no” CLI to disable the location-info dictionary setting.

**policy-control**

Defines external policy control.

```plaintext
dictionary { Gq-custom | Gq-standard | Rq-custom | Rx-rel8 | Rx-standard | Tx-standard | custom01...custom09 }
Gq-custom: Specifies that the Gq Operax dictionary is to be used for Operax-specific behavior.
Gq-standard: Specifies that the Gq standard dictionary is to be used.
Rq-custom: Specifies that the Rq custom dictionary is to be used.
Rx-rel8: Specifies that the Rx Release 8 dictionary is to be used.
Rx-standard: Specifies that the Rx standard dictionary is to be used.
Tx-standard: Specifies that the Tx standard dictionary is to be used.
custom01...custom09: Specifies that a customer-specific (custom) dictionary, for customer-specific expansion and behaviors, is to be used.
```

```plaintext
dictionary { dynamic-load | gq-custom | gq-standard | rq-custom | rx-custom01 | rx-custom02 | rx-custom03 | rx-custom04 | rx-custom05 | rx-rel8 | rx-standard | tx-standard }
dynamic-load: Configures the dynamically loaded Diameter dictionary. The dictionary name must be an alphanumeric string of 1 through 15 characters. For more information on dynamic loading of Diameter dictionaries, see the `diameter dynamic-dictionary` in the Global Configuration Mode Commands chapter of this guide.
gq-custom: Specifies that the Gq Operax dictionary is to be used for Operax-specific behavior.
gq-standard: Specifies that the Gq standard dictionary is to be used.
rq-custom: Specifies that the Rq custom dictionary is to be used.
rx-custom01...rx-custom05: Specifies that a customer-specific (custom) dictionary, for customer-specific expansion and behaviors, is to be used.
rx-rel8: Specifies that the Rx Release 8 dictionary is to be used.
rx-standard: Specifies that the Rx standard dictionary is to be used.
tx-standard: Specifies that the Tx standard dictionary is to be used.
```
**host-select-template name template_name**

Specifies the Diameter host-select-template. The host-select-template has a table of prefix and PCRF peers. When configured, PCRF server is selected using a lookup based on subscriber IMSI prefix from this table. *template_name* must be the template’s name and an alpha and/or numeric string of 1 through 63 characters in length.

**origin endpoint endpoint_name**

Specifies the Diameter location-info or policy control endpoint name. *endpoint_name* must be the endpoint’s name and an alpha and/or numeric string of 1 through 63 characters in length.

**peer-select peer peer_name**

Specifies the name of the Diameter location-info or policy control peer server. *peer_name* must be from 1 to 63 alpha and/or numeric characters in length. Diameter peer servers are configured through the *diameter endpoint* command in the Context Configuration Mode. The *diameter endpoint* command is a generic command and can be found in the Cisco ASR 5000 Series Command Line Interface Reference.

**peer-realm realm_name**

Specifies the realm name for which the Diameter location-info or policy control peer server has responsibility. *realm_name* must be from 1 to 63 alpha and/or numeric characters in length.

> **Important:** If this keyword is not configured, the system defaults to the realm name configured for the selected peer server.

**secondary-peer peer_name**

Specifies the name of the secondary Diameter location-info or policy control peer server. *peer_name* must be from 1 to 63 alpha and/or numeric characters in length.

**sec-peer-realm realm_name**

Specifies the realm name for which the secondary Diameter location-info or policy control peer server has responsibility. *realm_name* must be from 1 to 63 alpha and/or numeric characters in length.

> **Important:** If this keyword is not configured, the system defaults to the realm name configured for the selected peer server.

> **Important:** The “*diameter location-info peer-select peer <primary_peer> peer-realm <primary_peer_realm> secondary-peer <secondary_peer> sec-peer-realm <secondary_peer_realm>*” CLI configures Peer Switching—selecting which peers the Diameter messages are routed to. When the secondary peer is configured, in case the primary fails, request messages are rerouted to the secondary. Note that the “*no diameter location-info peer-select*” CLI command will remove the entire Peer Switching CLI from the configuration.
request-timeout \textit{sec}

Specifies the Diameter location-info or policy control requested timeout value in seconds. \textit{sec} must be an integer from 1 to 300. Default: 10

\textbf{Important:} If this keyword is not configured, the system defaults to the default setting (10 seconds). In the Proxy-CSCF configuration, at any time, the request-timeout setting can either be an explicitly configured value or the default value. Hence, there is no corresponding “no” CLI to disable the request-timeout setting.

\textbf{Usage}

Use this command to:
- define the Diameter dictionary to use for the service.
- specify the Diameter origin endpoint.
- specify a Diameter location-info or policy control peer server to support Rx/Tx/Gq applications.
- specify the Diameter requested timeout value for this service.

\textbf{Example}

The following command configures the system to use the Tx standard Diameter dictionary for this service:

```
diameter policy-control dictionary Tx-standard
```

The following command sets the Diameter location-info origin endpoint to test:

```
diameter location-info origin endpoint test
```

The following command selects a Diameter policy control peer server with a name of \textit{diam-2} and a realm name of \textit{realm-6}:

```
diameter policy-control peer-select peer diam-2 peer-realm realm-6
```
emergency

Configures the function to allow or disallow the emergency-session or emergency-registration of a particular type.

Product
SCM (P-CSCF, A-BG, SIP Proxy)

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration

configure > context context_name > cscc service service_name > proxy-cscf

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-cscf-service-proxy-cscf)#

Syntax

[ default | no ] emergency { registration [ visited-ue ] | session [ 3gpp-ims-xml-body | anonymous | non-emergency-registered | sdp-CS-media | visited-ue ] }

default
Specifies that the emergency-session or emergency-registration of a particular type can be allowed.

no
Disallows the emergency-session or emergency-registration of a particular type.

registration [ visited-ue ]
Allow emergency-registration. By default, it's allowed.

visited-ue: Allow emergency-registration from a visited UE. By default, it's allowed.

session [ 3gpp-ims-xml-body | anonymous | non-emergency-registered | sdp-CS-media | visited-ue ]
Specifies the type of emergency-session to be allowed or disallowed. By default, all are allowed.

3gpp-ims-xml-body: Allow 3GPP IM CN XML body to be added in 380 response messages.
anonymous: Allow anonymous subscribers (unregistered UEs) to initiate emergency sessions.
non-emergency-registered: Allow non-emergency registered subscribers to initiate emergency sessions.
sdp-CS-media: Allow emergency calls with SDP CS Media.
visited-ue: Allow emergency calls from visited UE.

Usage
Use this command to configure the function to allow or disallow the emergency-session or emergency-registration of a particular type.

Example
The following command configures the function to allow non-emergency registered subscribers to initiate emergency sessions:

emergency session non-emergency-registered
emergency-call-mode

Enables the P-CSCF/A-BG service to add “P-Emergency-Call-Mode-Preference” header in 200OK to REGISTER message. By default, this command is disabled.

Product
SCM (P-CSCF, A-BG)

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration

configure > context context_name > cscf service service_name > proxy-cscf

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-cscf-service-proxy-cscf)#

Syntax

emergency-call-mode { 3gpp-cs | 3gpp-ims }

[ default | no ] emergency-call-mode

default
Specifies 3GPP IMS access preference in header.

no
Disables “P-Emergency-Call-Mode-Preference” header insertion for the P-CSCF/A-BG service.

3gpp-cs | 3gpp-ims

3gpp-cs: Specifies 3GPP CS access preference in header.
3gpp-ims (default): Specifies 3GPP IMS access preference in header.

Usage
Enabling this command allows the P-CSCF or A-BG to add a “P-Emergency-Call-Mode-Preference” header in 200OK to REGISTER message.

Example
The following command enables “P-Emergency-Call-Mode-Preference” header insertion with a 3GPP CS access preference defined:

    emergency-call-mode 3gpp-cs
**end**

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**

Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Use this command to return to the parent configuration mode.
**interrogating-cscf-role**

Enables the function to also perform as an Interrogating-CSCF.

**Product**
SCM (P-CSCF, A-BG)

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration

```
configure > context context_name > cscf service service_name > proxy-cscf
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-service-proxy-cscf)#
```

**Syntax**

```
[ no ] interrogating-cscf-role
```

```
no
```

Disables the Interrogating-CSCF role in this function.

**Usage**
Use this command to enable the P-CSCF/A-BG to also perform as an Interrogating-CSCF.

**Important:** All Interrogating-CSCF functions have been moved to the Serving-CSCF exclusively in v10.0 and beyond.
message-max-size

Configures the maximum message body size in MESSAGE method.

Product
SCM (P-CSCF, A-BG)

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration

configure > context context_name > cscf service service_name > proxy-cscf

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-cscf-service-proxy-cscf)#

Syntax

message-max-size limit

[ default | no ] message-max-size

default | no

Returns/sets the maximum SIP message size to 1024 bytes.

limit

Default: 1024

Configures the maximum SIP message size limit in bytes for any SIP message buffer.

limit must be an integer from 512 to 65535.

Important: Message body size should be less than the max-sipmsg-size set in the CSCF Service Configuration Mode.

Usage

Use this command to configure the maximum SIP message size for any SIP message buffer.

Example

The following command limits the SIP message size to 4000 bytes:

message-max-size 4000
network-id

Configures the Network Identifier.

**Product**
SCM (P-CSCF, A-BG)

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration

```bash
configure > context context_name > cscf service service_name > proxy-cscf
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-service-proxy-cscf)#
```

**Syntax**

```
[ no ] network-id id
```

- **no**
  
  Removes the configured Network Identifier of the entity.

- **id**
  
  The Network Identifier of the entity.

  *id* must be from 1 to 79 alpha and/or numeric characters in length.

**Usage**

The Network Identifier is used by the P-CSCF or A-BG to fill the P-Visited-Network-ID header.

**Example**

Sets the Network Identifier to `pcscf01.company.com`:

```
network-id pcscf01.company.com
```
pcrf-policy-control

Enables external policy control via PCRF through the Rx Diameter interface and enters the PCRF-Policy-Control Configuration Mode. Default is disabled.

**Product**
SCM (P-CSCF, A-BG)

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration

```plaintext
configure > context context_name > cscf service service_name > proxy-cscf
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-service-proxy-cscf)>
```

**Syntax**

```
[ no ] pcrf-policy-control
```

- **no**
  Disables external policy control via PCRF for this service. P-CSCF/A-BG will not establish any Diameter session with PCRF, even though the PCRF is configured. This option disables both authorization and subscription to PCRF during Registration and VOIP call.

**Usage**

Use this command to enable PCRF policy control and enter the PCRF-Policy-Control Configuration Mode. It enables authorization and subscription to PCRF during Registration and VOIP calls. If the P-CSCF cannot connect to the PCRF server (due to wrong configuration in CSCF or PCRF unavailability), then P-CSCF/A-BG does not authorize media and VOIP calls will be rejected due to auth failure. Registrations will be handled normally.

Entering this command results in the following prompt:

```
[context_name]host_name(config-pcrf-policy-control)>
```

PCRF-Policy-Control Configuration Mode commands are defined in the *CSCF PCRF-Policy-Control Configuration Mode Commands* chapter in this guide.
peer-sbc

Configures peer Session Border Controller (SBC) addresses from where the P-CSCF/A-BG service can receive requests.

**Product**
SCM (P-CSCF, A-BG)

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration

```bash
configure > context context_name > cscf service service_name > proxy-cscf
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-service-proxy-cscf)#
```

**Syntax**

```
[ no ] peer-sbc ip_address
```

**no**
Removes the IP address of a peer SBC from this P-CSCF/A-BG service.

```
ip_address
```
Specifies the IP address of a peer SBC for this P-CSCF/A-BG service.

*ip_address* is expressed in standard dotted decimal notation for IPv4 or colon notation for IPv6.

**Usage**

Use this command to specify peer Session Border Controller (SBC) addresses from where the P-CSCF/A-BG service can receive requests.

**Important:** This command must be entered multiple times if more than one SBC is present.

**Example**

The following commands identify three peer SBCs for a single P-CSCF/A-BG service:

```
peer-sbc 200.6.2.3
peer-sbc 200.6.2.10
peer-sbc 200.6.2.11
```

The following command removes the peer SBC with IP address 200.6.2.10 from the P-CSCF/A-BG service:

```
no peer-sbc 200.6.2.10
```
plmn-id

Configures location specific mobile network identifiers used to help translate local emergency and service-related numbers. Default is disabled.

**Product**
SCM (P-CSCF, A-BG)

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration

`configure > context context_name > cscf service service_name > proxy-cscf`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-service-proxy-cscf)#
```

**Syntax**

```
plmn-id mcc code mnc code
no plmn-id
```

**Usage**

Use this command to help match location specific emergency/service numbers when configuring translations. The `mcc` and `mnc` values are compared against those received in p-access-network-info headers as per 3GPP TS 24.229. If `mnc` is not provided in the criteria only `mcc` is compared.

**Example**

The following command identifies the mobile network with a MCC of 123 and a MNC of 12:

```
plmn-id mcc 123 mnc 12
```
**reg-preloaded-route**

Enables the function to use the preloaded-route-headers received in REGISTER for routing at P-CSCF.

**Product**
SCM (P-CSCF, A-BG)

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration

```bash
configure > context context_name > cscf service service_name > proxy-cscf
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-service-proxy-cscf)#
```

**Syntax**

```bash
[ default | no ] reg-preloaded-route
```

- **default** | **no**

  Disables the ability to use preloaded-route-headers for routing REGISTER.

**Usage**

Use this command to enable or disable usage of preloaded-route-headers for routing REGISTER.
reg-service-route

Enables the function to use service routes when routing re-registrations.

**Product**
SCM (P-CSCF, A-BG)

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration

```
configure > context context_name > cscf service service_name > proxy-cscf
```

Entering the above command sequence results in the following prompt:

```
[context_name] host_name(config-cscf-service-proxy-cscf)#
```

**Syntax**

```
[ no ] reg-service-route
```

no

Disables the ability to use service routes for re-registration.

**Usage**

Use this command to enable the P-CSCF/A-BG service to use service routes when routing re-registrations.
reliable-prov-resp

Enables/disables the reliability of provisional responses feature.

Product
SCM (P-CSCF, A-BG)

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration
configure > context context_name > cscf service service_name > proxy-cscf

Entering the above command sequence results in the following prompt:
[context_name]host_name(config-cscf-service-proxy-cscf)#

Syntax
reliable-prov-resp { mandatory | optional }

[ no ] reliable-prov-resp

<table>
<thead>
<tr>
<th>no</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disables the reliability of provisional responses feature.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>mandatory</th>
<th>optional</th>
</tr>
</thead>
<tbody>
<tr>
<td>mandatory: Both inbound and outbound will request reliability.</td>
<td></td>
</tr>
<tr>
<td>optional (default): Reliability is imposed by inbound side. Only if inbound call requests reliability will outbound also request reliability.</td>
<td></td>
</tr>
</tbody>
</table>

Usage
Use this command to enable/disable the reliability of provisional responses feature.

Example
The following command sets the reliability of provisional responses feature to mandatory:

```
reliable-prov-resp mandatory
```

The following command disables the reliability of provisional responses feature:

```
no reliable-prov-resp
```
**restoration-procedure**

Enables the P-CSCF/A-BG service to reject with a 504 response when it receives 3xx, 480, or “no response” to service request. This feature is disabled by default.

**Product**
SCM (P-CSCF, A-BG)

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration

`configure > context context_name > cscf service service_name > proxy-cscf`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-service-proxy-cscf)#
```

**Syntax**

```
[ no ] restoration-procedure
```

`no`

Disables restoration procedure on the P-CSCF/A-BG service.

**Usage**

Restoration procedure is intended to handle unreachability of service-route header content. Enabling this command allows the P-CSCF/A-BG service to reject with a 504 response when it receives 3xx, 480, or “no response” to service request.

**Example**

Enables restoration procedure on the P-CSCF/A-BG service:

```
restoration-procedure
```

Disables restoration procedure on the P-CSCF/A-BG service:

```
no restoration-procedure
```
security-parameters

Enters the Security Configuration Mode in which Denial of Service (DOS) prevention commands can be configured.

**Product**
SCM (P-CSCF, A-BG)

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration

```text
configure > context context_name > cscf service service_name > proxy-cscf
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-service-proxy-cscf)#
```

**Syntax**

`security-parameters`

**Usage**

Use this command to enter the Security Configuration Mode.

Entering this command results in the following prompt:

```
[context_name]hostname(config-security-parameters)#
```

Security Configuration Mode commands are defined in the *CSCF Security Configuration Mode Commands* chapter in this guide.
sigcomp

Enables signaling compression for the P-CSCF/A-BG service and enters the Signaling Compression Configuration Mode.

Product
SCM (P-CSCF, A-BG)

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration

configure > context context_name > cscf service service_name > proxy-cscf

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-cscf-service-proxy-cscf)#

Syntax

[ no ] sigcomp

no

Disables signaling compression for the P-CSCF/A-BG service.

Usage

Use this command to enable signaling compression for the P-CSCF/A-BG service and enter the CSCF Signaling Compression Configuration Mode.

Entering this command results in the following prompt:

[context_name]host_name(config-cscf-service-proxy-cscf)#

Signaling Compression Configuration Mode commands are defined in the *CSCF Signaling Compression Configuration Mode Commands* chapter in this guide.
**sip-header**

Enable SIP header insertion for the P-CSCF/A-BG service. SIP header insertion is disabled by default.

**Product**
SCM (P-CSCF, A-BG)

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration

`configure > context context_name > csf service service_name > proxy-cscf`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-service-proxy-cscf)#
```

**Syntax**

```
[ no ] sip-header insert { p-access-network-info | p-cust1-prid-info | p-user-database }
```

- **no**
  
  Disables SIP header insertion for the P-CSCF/A-BG service.

```
insert { p-access-network-info | p-cust1-prid-info | p-user-database }
```

- **p-access-network-info**: Inserts P-Access-Network-Info (PANI) header in received request/response.
- **p-cust1-prid-info**: Inserts a custom header, P-LGUP-Plus-PRID-Info, which contains the private user id of the user sending any dialogue creating request or any standalone requests, to be added in the message toward nexthop. Addition of the header will be done when P-CSCF forwards this message.
- **p-user-database**: Inserts P-User-Database (PUD) header in SIP (REGISTER) message and Invite from I-CSCF to S-CSCF.

**Usage**

Enabling this command allows SIP header insertion on the P-CSCF or A-BG.

**Important:** Use the `access-type` command to configure a ue-ip-address-range per access type. CSCF Service Configuration Mode commands are defined in the `CSCF Service Configuration Mode Commands` chapter in this guide.

**Example**

Enables SIP PANI header insertion for the P-CSCF/A-BG service:

```
sip-header insert p-access-network-info
```
**sip-param**

Enable the addition of “integrity-protected” parameter in the authorization header of a SIP (REGISTER) message for the P-CSCF/A-BG service.

**Product**
SCM (P-CSCF, A-BG)

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration

`configure > context context_name > csf service service_name > proxy-cscf`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-service-proxy-cscf)#
```

**Syntax**

```
[ no ] sip-param insert integrity-protected [ custom-logic | transparent ]
```

- **no**
  Disables the addition of “integrity-protected” parameter in the authorization header of a SIP (REGISTER) message for the P-CSCF/A-BG service.

- **insert integrity-protected**
  Inserts “integrity-protected” parameter in the authorization header of a SIP (REGISTER) message for the P-CSCF/A-BG service.

- **custom-logic**
  Insert “integrity-protected” parameter for custom-logic in Authorization header.

- **transparent**
  Pass the “integrity-protected” parameter received from the previous node unmodified.

**Usage**

Enabling this command allows the P-CSCF or A-BG to add the “integrity-protected” parameter in the authorization header of a SIP (REGISTER) message. The parameter will be used by the S-CSCF to decide which authentication mode to use to authenticate the user.

**Example**

Enables the addition of `integrity-protected` parameter:

```
sip-param insert integrity-protected
```

Disables the addition of `integrity-protected` parameter:

```
no sip-param insert integrity-protected
```
store-session-path

Enables the P-CSCF or A-BG to store and process the session path information, which includes the Route list, Record-Route list, Service-Route list, and ViaList.

Product
SCM (P-CSCF, A-BG)

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration

configure > context context_name > cscf service service_name > proxy-cscf

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-cscf-service-proxy-cscf)#

Syntax

[ no ] store-session-path

no

Disables the storing of session path information by the P-CSCF or A-BG. In addition, the P-CSCF/A-BG will not overwrite the Route list, Record-Route list, Service-Route list, or ViaList in the in-dialog request and responses.

Usage

Enabling this command allows the P-CSCF or A-BG to store and process the session path information.

Example

Enables the storage and processing of session path information:

store-session-path

Disables the storage and processing of session path information:

no store-session-path
Chapter 92
CSCF Routes Configuration Mode Commands

The CSCF Routes Configuration Mode is used to configure session forwarding within the system.

Mode
Exec > Global Configuration > Context Configuration > Routes Configuration

configure > context context_name > cscf routes { default | name list_name }

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-cscf-route)#

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
**after**

Places the CSCF route entry at the bottom or end of the route list. Use this command in conjunction with the `route` command.

**Product**
SCM (P-CSCF, S-CSCF, SIP Proxy)

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Routes Configuration
`configure > context context_name > cscf routes { default | name list_name }`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-route)#
```

**Syntax**
```
after
```

**Usage**
Add this command before the `route` command to place the entry at the end of the route list.
before

Places the CSCF route entry at the top or beginning of the route list. Use this command in conjunction with the `route` command.

**Product**
SCM (P-CSCF, S-CSCF, SIP Proxy)

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Routes Configuration
`configure > context context_name > cscf routes { default | name list_name }`

Entering the above command sequence results in the following prompt:
`[context_name]host_name(config-cscf-route)#`

**Syntax**
`before`

**Usage**
Add this command before the `route` command to place the entry at the beginning of the route list.
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

exit

Usage
Use this command to return to the parent configuration mode.
route

Configure the routing parameters for the context.

**Product**
SCM (P-CSCF, S-CSCF, SIP Proxy)

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Routes Configuration

```bash
configure > context context_name > cscf routes { default | name list_name }
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-route)\# 
```

**Syntax**

```bash
route { domain name | local { icscf | pcscf | scscf } | nexthop-address address | peer-servers server_name | peer-servers-group group_name | route-list group_name | vpn name } 
[ [ mod-req-uri ] base-criteria criteria [ filter-criterial criteria ] [ filter-criteria2 criteria ] ] [ log ]
```

```bash
no route { domain name | local { icscf | pcscf | scscf } | nexthop-address address | peer-servers server_name | peer-servers-group group_name | route-list group_name | vpn name } base-criteria criteria [ filter-criterial criteria ] [ filter-criteria2 criteria ]
```

```bash
no
```

Removes the specified routing parameters for the CSCF service.

**domain name**
Specifies a valid next-hop domain name. *name* must be from 1 to 79 alpha and/or numeric characters in length.

**local { icscf | pcscf | scscf }**
Specifies a local interrogating, serving, or proxy call/session control function to which all calls processed by the context will be routed.

**nexthop-address ip_address**
Specifies a next-hop address. *ip_address* must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6.

**peer-servers server_name**
Specifies a configured peer server. *server_name* must be the name of a configured peer server on this system.
peer-servers-group group_name

Specifies a configured peer servers group. 
*group_name* must be the name of a configured peer servers group on this system.

route-list group_name

Specifies a configured route list group. 
*group_name* must be the name of a configured route list group on this system.

vpn name

Specifies a configured VPN context on the system. 
*name* must be a configured context name.

mod-req-uri

Specifies that a route lookup should be performed and the request URI modified.

base-criteria criteria

Specifies the base criteria that packets will be compared against. The following criteria is supported:

*access-type* type: Filters sessions based on a specific access-type used by the subscriber. Possible access types are:

- 3gpp-geran: 3GPP Access Type
- 3gpp-utran-fdd: 3GPP Access Type
- 3gpp-utran-tdd: 3GPP Access type
- 3gpp2-1x: 3GPP2 Access Type
- 3gpp2-1x-hrpdl: 3GPP2 Access Type
- 3gpp2-cdma-cs: 3GPP2-CDMA-CS
- 3gpp2-umb: 3GPP2-UMB
- adsl1: FixedLine Access Type
- adsl12: FixedLine Access Type
- adsl12p: FixedLine Access Type ADSL2+
- docsis: DOCSIS
- gshdsl: Fixed Line Access Type G.SHDSL
- hds1: Fixed Line Access Type
- hds12: Fixed Line Access Type
- ids1: Fixed Line Access Type
- ieee-80211: WLAN Access Type
- ieee-80211a: WLAN Access Type
- ieee-80211b: WLAN Access Type
- ieee-80211g: WLAN Access Type
- ieee-80216e: Wireless MAN Access Type
- rads1: Fixed Line Access Type
CSCF Routes Configuration Mode Commands

route

*sdsl*: Fixed Line Access Type
*vdsl*: Fixed Line Access Type
*any*: Filters all CSCF sessions.
*carrier-id name*: Filters sessions based on the carrier’s ID. *name* must be from 1 to 79 alpha and/or numeric characters in length.
*destination aor aor*: Filters sessions based on the destination AoR. *aor* must be an existing AoR from 1 to 79 characters in length.

**Important**: The destination aor and carried-id criteria cannot occur in the same route rule.

*nexthop-uri name*: Filters sessions based on Address of Record. *name* must be from 1 to 79 alpha and/or numeric characters in length.
*plmn-id mcc mcc_code mnc mnc_code*: Filters sessions based on the mobile country and network codes. *mcc_code* must be a three-digit integer from 200 to 999. *mnc_code* must be a two or three-digit integer from 00 to 999.
*source address ip_address*: Filters sessions based on source IP address. *ip_address* must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6.
*source aor aor*: Filters sessions based on the source AoR. *aor* must be an existing AoR from 1 to 79 characters in length.
*subscriber-capability capability_type*: Filters sessions based on capability of the subscriber. Possible capability types are:

*at*: Custom AT Type
*audio*: Audio Capability Type
*chat*: Custom CHAT Type
*cs*: Custom CS Type
*ft*: Custom FT Type
*im*: Custom IM Type
*lte-voip*: Custom LTE-VOIP Type
*lte-vt*: Custom LTE-VT Type
*msg*: Custom MSG Type
*oms*: Custom OMA SIP Type
*rscp*: Custom RCS-DP Type
*rsc-e*: Custom RCS-E Type
*rsc-ft*: Custom RCS-FT Type
*rsc-im*: Custom RCS-IM Type
*rsc-is*: Custom RCS-IS Type
*rsc-sp*: Custom RCS-SP Type
*rsc-vs*: Custom RCS-VS Type
**smart-edu** - Custom SMART-EDU Type

**text** - Text Capability Type

**video** - Video Capability Type

**vt** - Custom VT Type

**vt-ft** - Custom VT-FT Type

**vt-is** - Custom VT-IS Type

**vt-loc** - Custom VT-LOC Type

**vt-memo** - Custom VT-MEMO Type

**subscriber-ip-type** { v4 | v6 }: Filters sessions based on IP type of the subscriber. Possible IP types are:

- **v4** - IPV4 Type
- **v6** - IPV6 Type

**time-of-day**: Filters sessions based on the time of the day. Additional filter criteria for **time-of-day** is as follows:

- **day-of-month** day: Filters session based on the day of the month. day must be an integer from 1 to 31.

- **day-of-week** day: Filters session based on the day of the week. day must be an integer from 1 to 7 with 1 signifying Sunday and 7 signifying Saturday.

- **start** date/time [ end date/time ]: Filters sessions based on a start time to, optionally, an end time during the day. date/time must be integers in either of the following formats: YYYY:MM:DD:HH:mm or YYYY:MM:DD:mm:ss. YYYY: year range 2005 to 2099 MM: months (integer range 1 to 12) DD: days (integer range 1 to 31) HH: hours (integer range 0 to 23) mm: minutes (integer range 0 to 59) ss: seconds (integer range 0 to 59)

- **week-of-month** week: Filters sessions based on the week of the month. week must be an integer from 1 to 5.

**Important**: AoR regular expressions are supported. Refer to the SCM Engineering Rules Appendix in the Session Control Manager Administration Guide for more information about regular expressions.

**filter-criteria** criteria

Specifies the filter criteria that packets that have passed the base criteria will be compared against. The following criteria is supported:

**access-type** type: Filters sessions based on a specific access-type used by the subscriber. Possible access types are:

- **3gpp-geran**: 3GPP Access Type
- **3gpp-utran-fdd**: 3GPP Access Type
- **3gpp-utran-tdd**: 3GPP Access type
- **3gpp2-1x**: 3GPP2 Access Type
- **3gpp2-1x-hrp**: 3GPP2 Access Type
- **3gpp2-cdma-cs**: 3GPP2-CDMA-CS
- **3gpp2-umb**: 3GPP2-UMB
• **adsl**: FixedLine Access Type
• **adsl2**: FixedLine Access Type
• **adsl2p**: FixedLine Access Type ADSL2+
• **docsis**: DOCSIS
• **gshdsl**: Fixed Line Access Type G.SHDSL
• **hds1**: Fixed Line Access Type
• **hds12**: Fixed Line Access Type
• **ids1**: Fixed Line Access Type
• **ieee-80211**: WLAN Access Type
• **ieee-80211a**: WLAN Access Type
• **ieee-80211b**: WLAN Access Type
• **ieee-80211g**: WLAN Access Type
• **ieee-80216e**: Wireless MAN Access Type
• **radsl**: Fixed Line Access Type
• **sdsl**: Fixed Line Access Type
• **vdsl**: Fixed Line Access Type
• **any**: Filters all CSCF sessions.
• **carrier-id name**: Filters sessions based on the carrier’s ID. `name` must be from 1 to 79 alpha and/or numeric characters in length.
• **destination aor aor**: Filters sessions based on the destination AoR. `aor` must be an existing AoR from 1 to 79 characters in length.

**Important**: The destination aor and carrier-id criteria cannot occur in the same route rule.

• **nexthop-uri name**: Filters sessions based on Address of Record. `name` must be from 1 to 79 alpha and/or numeric characters in length.
• **plmn-id mcc mcc_code mnc mnc_code**: Filters sessions based on the mobile country and network codes. `mcc_code` must be a three-digit integer from 200 to 999. `mnc_code` must be a two or three-digit integer from 00 to 999.
• **source address ip_address**: Filters sessions based on source IP address. `ip_address` must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6.
• **source aor aor**: Filters sessions based on the source AoR. `aor` must be an existing AoR from 1 to 79 characters in length.
• **subscriber-capability capability_type**: Filters sessions based on capability of the subscriber. Possible capability types are:
  • **at** - Custom AT Type
  • **audio** - Audio Capability Type
  • **chat** - Custom CHAT Type
  • **cs** - Custom CS Type
• ft - Custom FT Type
• im - Custom IM Type
• lte-voip - Custom LTE-VOIP Type
• lte-vt - Custom LTE-VT Type
• mms - Custom MMS Type
• msg - Custom MSG Type
• oma-sip-im - Custom OMA SIP-IM Type
• rcs-dp - Custom RCS-DP Type
• rcs-e - Custom RCS-E Type
• rcs-ft - Custom RCS-FT Type
• rcs-im - Custom RCS-IM Type
• rcs-is - Custom RCS-IS Type
• rcs-sp - Custom RCS-SP Type
• rcs-vs - Custom RCS-VS Type
• smart-edu - Custom SMART-EDU Type
• text - Text Capability Type
• video - Video Capability Type
• vt - Custom VT Type
• vt-ft - Custom VT-FT Type
• vt-is - Custom VT-IS Type
• vt-loc - Custom VT-LOC Type
• vt-memo - Custom VT-MEMO Type

• subscriber-ip-type { v4 | v6 }: Filters sessions based on IP type of the subscriber. Possible IP types are:
  • v4 - IPV4 Type
  • v6 - IPV6 Type

• time-of-day: Filters sessions based on the time of the day. Additional filter criteria for time-of-day is as follows:
  • day-of-month day: Filters session based on the day of the month. day must be an integer from 1 to 31.
  • day-of-week day: Filters session based on the day of the week. day must be an integer from 1 to 7 with 1 signifying Sunday and 7 signifying Saturday.
  • start date/time [ end date/time ]: Filters sessions based on a start time to, optionally, an end time during the day. date/time must be integers in either of the following formats: YYYY:MM:DD:HH:mm or YYYY:MM:DD:mm:ss. YYYY: year range 2005 to 2099 MM: months (integer range 1 to 12) DD: days (integer range 1 to 31) HH: hours (integer range 0 to 23) mm: minutes (integer range 0 to 59) ss: seconds (integer range 0 to 59)
  • week-of-month week: Filters sessions based on the week of the month. week must be an integer from 1 to 5.
Important: AoR regular expressions are supported. Refer to the SCM Engineering Rules Appendix in the Session Control Manager Administration Guide for more information about regular expressions.

```plaintext
filter-criteria2 criteria
```

Specifies the filter criteria that packets that have passed the base criteria and filter-criteria1 will be compared against. The following criteria is supported:

- **access-type type**: Filters sessions based on a specific access-type used by the subscriber. Possible access types are:
  - `3gpp-geran`: 3GPP Access Type
  - `3gpp-utran-fdd`: 3GPP Access Type
  - `3gpp-utran-tdd`: 3GPP Access type
  - `3gpp2-1x`: 3GPP2 Access Type
  - `3gpp2-1x-hrpd`: 3GPP2 Access Type
  - `3gpp2-cdma-cs`: 3GPP2-CDMA-CS
  - `3gpp2-umb`: 3GPP2-UMB
  - `ads1`: FixedLine Access Type
  - `ads12`: FixedLine Access Type
  - `ads12p`: FixedLine Access Type ADSL2+
  - `docsis`: DOCSIS
  - `gshdsl`: Fixed Line Access Type G.SHDSL
  - `hds1`: Fixed Line Access Type
  - `hds12`: Fixed Line Access Type
  - `ids1`: Fixed Line Access Type
  - `ieee-80211`: WLAN Access Type
  - `ieee-80211a`: WLAN Access Type
  - `ieee-80211b`: WLAN Access Type
  - `ieee-80211g`: WLAN Access Type
  - `ieee-80216e`: Wireless MAN Access Type
  - `rads1`: Fixed Line Access Type
  - `sds1`: Fixed Line Access Type
  - `vds1`: Fixed Line Access Type
- **any**: Filters all CSCF sessions.
- **carrier-id name**: Filters sessions based on the carrier’s ID. `name` must be from 1 to 79 alpha and/or numeric characters in length.
- **destination aor aor**: Filters sessions based on the destination AoR. `aor` must be an existing AoR from 1 to 79 characters in length.
**Important:** The destination aor and carried-id criteria cannot occur in the same route rule.

- **nexthop-uri** name: Filters sessions based on Address of Record. name must be from 1 to 79 alpha and/or numeric characters in length.
- **plmn-id mcc mcc_code mnc mnc_code**: Filters sessions based on the mobile country and network codes. mcc_code must be a three-digit integer from 200 to 999. mnc_code must be a two or three-digit integer from 00 to 999.
- **source address ip_address**: Filters sessions based on source IP address. ip_address must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6.
- **source aor** aor: Filters sessions based on the source AoR. aor must be an existing AoR from 1 to 79 characters in length.
- **subscriber-capability capability_type**: Filters sessions based on capability of the subscriber. Possible capability types are:
  - **at**: Custom AT Type
  - **audio**: Audio Capability Type
  - **chat**: Custom CHAT Type
  - **cs**: Custom CS Type
  - **ft**: Custom FT Type
  - **im**: Custom IM Type
  - **lte-voip**: Custom LTE-VOIP Type
  - **lte-vt**: Custom LTE-VT Type
  - **mms**: Custom MMS Type
  - **msg**: Custom MSG Type
  - **oma-sip-im**: Custom OMA SIP-IM Type
  - **rcs-dp**: Custom RCS-DP Type
  - **rcs-e**: Custom RCS-E Type
  - **rcs-ft**: Custom RCS-FT Type
  - **rcs-im**: Custom RCS-IM Type
  - **rcs-is**: Custom RCS-IS Type
  - **rcs-sp**: Custom RCS-SP Type
  - **smart-edu**: Custom SMART-EDU Type
  - **rcs-vs**: Custom RCS-VS Type
  - **text**: Text Capability Type
  - **video**: Video Capability Type
  - **vt**: Custom VT Type
  - **vt-ft**: Custom VT-FT Type
  - **vt-is**: Custom VT-IS Type
  - **vt-loc**: Custom VT-LOC Type
**route**

• *vt-memo* - Custom VT-MEMO Type

• *subscriber-ip-type* { v4 | v6 } - Filters sessions based on IP type of the subscriber. Possible IP types are:
  • v4 - IPV4 Type
  • v6 - IPV6 Type

• *time-of-day* - Filters sessions based on the time of the day. Additional filter criteria for time-of-day is as follows:
  • *day-of-month* day - Filters session based on the day of the month. day must be an integer from 1 to 31.
  • *day-of-week* day - Filters session based on the day of the week. day must be an integer from 1 to 7 with 1 signifying Sunday and 7 signifying Saturday.
  • *start* date/time [ end date/time ] - Filters sessions based on a start time to, optionally, an end time during the day. date/time must be integers in either of the following formats: YYYY:MM:DD:HH:mm or YYYY:MM:DD:mm:ss. YYYY: year range 2005 to 2099 MM: months (integer range 1 to 12) DD: days (integer range 1 to 31) HH: hours (integer range 0 to 23) mm: minutes (integer range 0 to 59) ss: seconds (integer range 0 to 59)
  • *week-of-month* week - Filters sessions based on the week of the month. week must be an integer from 1 to 5.

**Important:** AoR regular expressions are supported. Refer to the SCM Engineering Rules Appendix in the Session Control Manager Administration Guide for more information about regular expressions.

**log**

Enables logging for CSCF sessions meeting the criteria specified in the ACL. The logs can be viewed by executing the `logging filter active facility cscf-acl-log` command in the Exec mode.

**Usage**

Use this command to configure routing parameters for the service.

**Important:** Use the `before` or `after` command to place the route entry in the route list.

**Example**

The following command is placed at the end of the route list and routes sessions to a peer server group named `icscf_peer5`, filters sessions with a base criteria of the source address (1.2.3.4) and a filter criteria of the destination AoR ($.@test.com):

```
after route peer-servers icscf_peer5 base-criteria source address 1.2.3.4 filter-criterion destination aor $.@test.com
```
Chapter 93
CSCF Security Configuration Mode Commands

The CSCF Security Configuration Mode is used to configure Denial of Service (DOS) prevention commands.

Mode

Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration > CSCF Security Configuration

configure > context context_name > cscf service service_name > proxy-cscf > security-parameters

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-security-parameters)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
auth-failure-weight

Sets a severity number for authorization failures used in calculating a value for determining when to suspend registration attempts.

**Important**: The system will ignore the configuration of this command unless the `dos-prevention` command has been enabled.

**Product**

SCM (P-CSCF, A-BG)

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration > CSCF Security Configuration

```
configure > context context_name > cscf service service_name > proxy-cscf > security-parameters
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-security-parameters)#
```

**Syntax**

```
auth-failure-weight weight

default auth-failure-weight
```

**default auth-failure-weight**

```
default

Sets/Restores the default value assigned to the specified command.
```

```
weight

Default: 1
Assigns a weight to an authorization failure. Defines the severity of a single authorization failure.

weight must be an integer from 1 to 5.
```

**Usage**

Use this command to define the severity of an authorization failure. This parameter is used in calculating the current number of authorization failures to compare to the `per-aor-failure-limit` and the `per-ip-failure-limit`. Configuring this command with a lower number causes the system to suspend registration attempts with repeated authorization failures much sooner than when configured with a higher number.

**Example**

The following command assigns a weight of 3 to an authorization failure:

```
auth-failure-weight 3
```
bad-request-weight

Sets a severity number for bad registration requests used in calculating a value for determining when to suspend registration attempts.

**Important:** The system will ignore the configuration of this command unless the `dos-prevention` command has been enabled.

**Product**
SCM (P-CSCF, A-BG)

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration > CSCF Security Configuration

```
cfg > context context_name > cscf service service_name > proxy-cscf > security-parameters
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-security-parameters)#
```

**Syntax**

```
bad-request-weight weight

default bad-request-weight
```

**default bad-request-weight**

- `default`
  
  Sets/restores the default value assigned to the specified command.

- `weight`
  
  Default: 2
  
  Assigns a weight to a bad registration request. Defines the severity of a single bad request.
  
  `weight` must be an integer from 1 to 5.

**Usage**

Use this command to define the severity of bad registration request. This parameter is used in calculating the current number of request failures to compare to the `per-aor-failure-limit` and the `per-ip-failure-limit`. Configuring this command with a lower number causes the system to suspend registration attempts with repeated request failures much sooner than when configured with a higher number.

**Example**

The following command assigns a weight of 3 to a bad registration request:

```
bad-request-weight 3
```
dos-prevention

Enables the denial of service (DoS) attack prevention feature.

Product

SCM (P-CSCF, A-BG)

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration > CSCF Security Configuration

configure > context context_name > cscf service service_name > proxy-cscf > security-parameters

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-security-parameters)#

Syntax

[ default | no ] dos-prevention

[ default | no ]

Disables the DoS attack prevention feature.

Usage

Use this command to enable the DoS attack prevention feature. The default value for this command is disabled. When this command is enabled, the commands in this mode are enabled with default values configured.

Important: This command must be enabled before configuring other commands in this mode.
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
**exit**

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
```
exit
```

**Usage**
Use this command to return to the parent configuration mode.
forking-contact-limit

Sets a limit on the number of contacts a user ID can register with the system.

**Important:** The system will ignore the configuration of this command unless the `dos-prevention` command has been enabled.

**Product**

SCM (P-CSCF, A-BG)

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration > CSCF Security Configuration

```
configure > context context_name > csf service service_name > proxy-csf > security-parameters
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-security-parameters)#
```

**Syntax**

```
forking-contact-limit limit

default forking-contact-limit
```

**default forking-contact-limit**

```
default
```

Sets/restores the default value assigned to the specified command.

```
limit
```

Default: 0

Sets the maximum number of contacts a user ID can register with the system. 0 specifies that unlimited contacts can be registered per user ID. `limit` must be an integer from 0 to 10.

**Usage**

Use this command to limit the number of contacts a user ID can register with the system.

**Example**

The following command limits all users to 2 registered contacts on the system:

```
forking-contact-limit 2
```
greylist-duration

Configures the amount of time an AoR or IP address remains on a “grey list” after having crossed the registration authorization limit or the bad registration request limit.

**Important**: The system will ignore the configuration of this command unless the `dos-prevention` command has been enabled.

**Product**
SCM (P-CSCF, A-BG)

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration > CSCF Security Configuration

```
configure > context context_name > cscf service service_name > proxy-cscf > security-parameters
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-security-parameters)#
```

**Syntax**

```
greylist-duration time

default greylist-duration
```

**default**
Sets/restores the default value assigned to the specified command.

**time**
Default: 10
Defines the time, in minutes, that an AoR or IP address remains on a “grey list”. `time` must be an integer from 5 to 1,440.

**Usage**
Use this command to specify the amount of time AoRs or IP addresses remain on a “grey list” after having crossed the registration authorization limit or the bad registration request limit. Limits are described in the `per-aor-failure-limit` command and the `per-ip-failure-limit` command.

**Example**
The following command sets the duration AoRs or IP addresses remain on a “grey list” to 30 minutes:

```
greylist-duration 30
```
per-aor-failure-limit

Sets a failure limit that, when exceeded, causes the suspension of registration attempts for the offending AoR.

Important: The system will ignore the configuration of this command unless the dos-prevention command has been enabled.

Product
SCM (P-CSCF, A-BG)

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration > CSCF Security Configuration

configure > context context_name > cscf service service_name > proxy-cscf > security-parameters

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-security-parameters)#

Syntax

per-aor-failure-limit limit

default per-aor-failure-limit

default
Sets/restores the default value assigned to the specified command.

limit
Default: 200
Defines the threshold for registration failures based on a calculation using weighted multipliers defined in auth-failure-weight and bad-request-weight. limit must be an integer from 5 to 10,000.

Usage
Use this command to set a failure limit for registration attempts from an identified AoR. The following calculation determines when this threshold is reached for a specific AoR:

Current authorization failures ÷ auth-failure-weight = current failures per AoR
or
Total bad registration requests ÷ bad-request-weight = current failures per AoR

If auth-failure-weight = 2 and bad-request-weight = 1, and the per-aor-failure-limit = 100, then the tolerance for registration authentication failures = 50 per AoR and the tolerance for bad registration requests = 100 per AoR.

When an AoR reaches the failure limit, it is added to a “grey list” for a period of time as defined by the greylist-duration command.
Example

The following command sets the AoR failure limit to 300:

```
per-aor-failure-limit 300
```
per-ip-failure-limit

Sets a failure limit that, when exceeded, causes the suspension of registration attempts for the offending IP address.

**Important:** The system will ignore the configuration of this command unless the `dos-prevention` command has been enabled.

**Product**

SCM (P-CSCF, A-BG)

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration > CSCF Security Configuration

configure > context context_name > csfv service service_name > proxy-cscf > security-parameters

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-security-parameters)#
```

**Syntax**

```
per-ip-failure-limit limit

default per-ip-failure-limit
```

**default**

Sets/restores the default value assigned to the specified command.

**limit**

Default: 100

Defines the threshold for registration failures based on a calculation using weighted multipliers defined in `auth-failure-weight` and `bad-request-weight`.

*limit* must be an integer from 5 to 10,000.

**Usage**

Use this command to set a failure limit for registration attempts from an identified IP address. The following calculation determines when this threshold is reached for any IP address:

Current authorization failures ÷ `auth-failure-weight` = current failures per AoR

or

Total bad registration requests ÷ `bad-request-weight` = current failures per AoR

If `auth-failure-weight` = 2 and `bad-request-weight` = 1, and the `per-ip-failure-limit` = 200, then the tolerance for registration authentication failures = 100 per each IP address and the tolerance for bad registration requests = 200 per each IP address.

When an IP address reaches the failure limit, it is added to a “grey list” for a period of time as defined by the `greylist-duration` command.
Example

The following command sets the IP address registration failure limit to 200:

```
per-ip-failure-limit 200
```
**threshold-rate**

Configures the rate per second at which the system must receive authorization failures or bad registration requests before it considers the failures/requests a DoS attack.

**Important:** The system will ignore the configuration of this command unless the **dos-prevention** command has been enabled.

<table>
<thead>
<tr>
<th>Product</th>
<th>SCM (P-CSCF, A-BG)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privilege</td>
<td>Security Administrator, Administrator</td>
</tr>
<tr>
<td>Mode</td>
<td>Exec &gt; Global Configuration &gt; Context Configuration &gt; CSCF Service Configuration &gt; Proxy-CSCF Configuration &gt; CSCF Security Configuration</td>
</tr>
<tr>
<td></td>
<td>configure &gt; context context_name &gt; cscf service service_name &gt; proxy-cscf &gt; security-parameters</td>
</tr>
</tbody>
</table>

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-security-parameters)#
```

**Syntax**

```
threshold-rate rate

default threshold-rate
```

**default**

Sets/restores the default value assigned to the specified command.

**rate**

Default: 1

Specifies the rate per second that the system must receive authorization failures or bad registration requests to determine that it is under a DoS attack.

*rate* must be an integer from 1 to 1,000.

**Usage**

Use this command to specify the threshold rate for authorization failures or bad registration requests. For example, if a malicious user sends bad registration requests at a rate of 5 per second and this parameter is set to 10, the system will not consider itself under a DoS attack.

**Example**

The following command sets the threshold rate to 5 authorization failures or bad registration requests per second:

```
threshold-rate 5
```
threshold-rate
Chapter 94
CSCF Service Configuration Mode Commands

The CSCF Service Configuration Mode is used to create and manage CSCF services within the current context.

Mode

Exec > Global Configuration > Context Configuration > CSCF Service Configuration

configure > context context_name > cscf service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-cscf-service)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
RetryAfter-header-value

Sets the minimum and maximum value in seconds for Retry-After Header.

**Product**
SCM (S-CSCF)

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration
configure > context context_name > cscf service service_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-service)#
```

**Syntax**

```
RetryAfter-header-value min-value sec max-value sec
default RetryAfter-header-value
```

- **default**
  Returns the command to the default settings.

- **min-value** sec: Specifies the minimum amount of time for Retry-After Header. `sec` must be an integer from 2 to 3600. Default is 2 seconds.

- **max-value** sec: Specifies the maximum amount of time for Retry-After Header. `sec` must be an integer from 3 to 3601. Default is 10 seconds.

**Important:** Maximum value should be greater than minimum value.

**Usage**

Use this command to set the minimum and maximum value in seconds for Retry-After Header. If Transactions Per Second (TPS) rate towards the peer-server application server (AS) is exceeded, the incoming requests will be rejected with 500 error response; Retry-After Header specifies the number of seconds before UE should retry.

**Example**

The following command configures the minimum value to 3 and maximum value to 12 for Retry-After Header:

```
RetryAfter-header-value min-value 3 max-value 12
```
access-service

Configures the name of the P-CSCF/A-BG access service from which the system receives requests and sends responses. The access service lets the core service know where a packet needs to be routed.

**Product**
SCM (P-CSCF, A-BG)

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration

```
configure > context context_name > cscf service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-service)#
```

**Syntax**

```
access-service name name

no access-service [ name name ]
```

- `no`
  Removes the access service.

- `name name`
  Specifies the name of the P-CSCF/A-BG access service from which the system receives requests and sends responses.
  *name* must be from 1 to 63 alpha and/or numeric characters.

**Important**: This command should only be issued in the core service configuration, however, multiple access services may be configured per core service.

**Usage**

Use this command to identify the name of the P-CSCF/A-BG access service from which the system receives requests and sends responses from/to the UEs. This command is used in systems that deploy two P-CSCF/A-BG services in bridging (Back-to-Back User Agent) mode configurations where an access service P-CSCF/A-BG faces the UE network and a core P-CSCF/A-BG faces the public network.

**Example**

The following command identifies the P-CSCF/A-BG access service named to the CSCF/A-BG core service:

```
access-service name HA3
```
access-type

Specifies the access types for IMS core.

Product
SCM (P-CSCF, A-BG)

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > CSCF Service Configuration

configure > context context_name > cscf service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-cscf-service)#

Syntax

access-type { type } access-profile { default | name access_profile_name } | ue-ip-address-range name ue_ip_name { address ip_address_mask | range start_ip_address end_ip_address }

no access-type { type } [ access-profile | ue-ip-address-range { name ue_ip_name } ]

no

Removes the specified access type from a CSCF access profile or UE IP address/range.

access-type { type }

3gpp-e-utran-fdd: 3GPP Access Type
3gpp-e-utran-tdd: 3GPP Access Type
3gpp-geran: 3GPP Access Type
3gpp-utran-fdd: 3GPP Access Type
3gpp-utran-tdd: 3GPP Access Type
3gpp2-1x: 3GPP2 Access Type
3gpp2-1x-hrpdp: 3GPP2 Access Type
3gpp2-cdma-cs: 3GPP2-CDMA-CS
3gpp2-umb: 3GPP2-UMB
adsl: FixedLine Access Type
adsl2: FixedLine Access Type
adsl2p: FixedLine Access Type ADSL2+
docsis: DOCSIS
gshdsl: FixedLine Access Type G.SHDSL
hds1: FixedLine Access Type
hds12: FixedLine Access Type
ids1: FixedLine Access Type
ieee-80211: WLAN Access Type
ieee-80211a: WLAN Access Type
ieee-80211b: WLAN Access Type
ieee-80211g: WLAN Access Type
ieee-80211n: WLAN Access Type
**CSCF Service Configuration Mode Commands**

**access-type**

*IEEE-80216e:* Wireless MAN Access Type  
*IEEE-8023:* Ethernet Access Type  
*IEEE-8023a:* Ethernet Access Type  
*IEEE-8023ab:* Ethernet Access Type  
*IEEE-8023ae:* Ethernet Access Type  
*IEEE-8023ak:* Ethernet Access Type  
*IEEE-8023an:* Ethernet Access Type  
*IEEE-8023aq:* Ethernet Access Type  
*IEEE-8023e:* Ethernet Access Type  
*IEEE-8023i:* Ethernet Access Type  
*IEEE-8023j:* Ethernet Access Type  
*IEEE-8023u:* Ethernet Access Type  
*IEEE-8023y:* Ethernet Access Type  
*IEEE-8023z:* Ethernet Access Type  
*RADSL:* FixedLine Access Type  
*SDSL:* FixedLine Access Type  
*VDSL:* FixedLine Access Type

**access-profile { default | name access_profile_name }**

Associates an access type with a CSCF access profile. Different access types can refer to the same access profile.

**ue-ip-address-range name ue_ip_name { address ip_address_mask | range start_ip_address end_ip_address }**

Configures UE IP address/range for a specific access type.

- *ue_ip_name* must be from 1 to 79 alpha and/or numeric characters.
- *address ip_address_mask:* Specifies a combined IP address subnet mask bits to indicate what IP addresses the specific access-type applies to. *ip_address_mask* must be specified using the form “IP Address/Mask Bits” where the IP address must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6, and the mask bits are a numeric value, which is the number of bits in the subnet mask.
- *range start_ip_address end_ip_address:* Configure UE IP range for specific access-type.
  - *start_ip_address* specifies the beginning of the range of addresses.
  - *end_ip_address* specifies the end of the range of addresses.
  - *ip_address* must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6.

**Usage**

Use this command to associate the access types for a specified CSCF access profile or UE IP address/range name.

**Important:** Use the **sip-header** command to enable SIP P-Access-Network-Info (PANI) header insertion. CSCF Proxy-CSCF Configuration Mode commands are defined in the *CSCF Proxy-CSCF Configuration Mode Commands* chapter in this guide.

**Example**

The following command identifies the access type adsl and assigns it to access profile *api*:

```
access-type adsl access-profile name api
```
allow-dereg

Allows the CSCF to send de-registration requests. Feature is disabled by default.

**Product**
SCM

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration

```bash
configure > context context_name > cscf service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-service)#
```

**Syntax**

```
[ no ] allow-dereg
```

- **no**
  Disables the feature.

**Usage**

Use this command to allow the CSCF service to send de-registration requests.
If the UE stops sending keepalive packets, which ends the connection between the UE and the proxy, UE information is cleared from the Proxy-CSCF (P-CSCF) or Access Border Gateway (A-BG). If de-registration requests are enabled, any UE-related information that is shared with the Serving-CSCF (S-CSCF) will also be cleared.
bind

Binds the CSCF service to a logical IP interface and specifies the maximum number of sessions that can access this service over the specified interface.

**Product**
SCM (P-CSCF, A-BG)

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration

`configure > context context_name > cscf service service_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-service)#
```

**Syntax**

```
bind address ip_address [ cscf-hostname host_name ] [ ipsec-crypto-template template ] [ max-sessions max# ] [ port number ] [ reserved-call-capacity percentage ] [ tls-crypto-template template ] [ tls-port number ] [ transport tcp ] [ use-serviceport-towards-network ]
```

`no bind address`

Removes the binding of the service to a specified interface.

```
address ip_address
```

Specifies the IP address of the interface to which the service is being bound.

`ip_address` must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6.

```
cscf-hostname host_name
```

Specifies the local host name of the CSCF service.

`host_name` must be an existing CSCF service name and be from 1 to 127 alpha and/or numeric characters.

Configuring this keyword associates the CSCF service with the AOR domain configured in the `default-aor-domain` command and uses the domain name in SIP headers.

**Important:** If this keyword is not configured, SIP headers will contain the IP address of the CSCF service instead of the domain name.

```
ipsec-crypto-template template
```

Specifies the name of an existing IPSec CSCF crypto template to be used for accessing CSCF service by user equipment. Valid only for P-CSCF or A-BG.

`template` must be an existing IPSec CSCF crypto template and be from 1 to 127 alpha and/or numeric characters.
**Important:** The IPSec CSCF crypto template should be configured in the same context in which the P-CSCF is configured.

```
max-sessions max#
```

Default: 500,000
Specifies the maximum number of sessions managed by this service on this interface.
`max#` must be configured to any integer value from 0 to 500,000.

**Important:** The total session capacity of the system is 500,000. `max-sessions` is also limited by the capacity in the license generated for the service. If licenses for PDSN/GGSN/HA are generated for `x` number of sessions, then the license for the CSCF service will be generated at `500,000-x`. Hardware configuration and installed features can also affect the maximum number of sessions that can be supported.

```
port number
```

Default: 5060
Specifies the UDP port number.
`number` must be an integer value from 1 to 65534.

```
reserved-call-capacity percentage
```

Default: 10
Specifies the call capacity percentage per session manager (sessmgr).
`percentage` must be an integer value from 1 to 50.

```
tls-crypto-template template [ tls-port number ]
```

Specifies the name of an existing Transport Layer Security (TLS) crypto template to enable TLS functionality. Valid only for P-CSCF or A-BG.
`template` must be an existing TLS crypto template and be from 1 to 127 alpha and/or numeric characters.
Default: 5061
Specifies the TLS port number.
`number` must be an integer value from 1 to 65534.

**Important:** When the `tls-crypto-template` is configured, TCP transport must be enabled, otherwise this command will throw an error. The configured `tls-crypto-template` should be configured in the same context in which the P-CSCF service is configured and must be complete with all certificate and cipher suite configuration. If the `tls-crypto-template` is not present or not completely configured, the P-CSCF service will not be started.

```
transport tcp
```

Enables TCP transport for the address.

```
use-serviceport-towards-network
```

Enables use of service port for sending and receiving UDP messages from network elements.
Usage

Use this command to associate the service with a specific logical IP address. This command also configures the identity of the CSCF in SIP headers as either the domain name of the CSCF service or the IP address.

Important: Multiple keywords can be used per bind command.

Example

The following command binds the CSCF service to a logical interface with an IP address of 1.2.3.4 and sets the maximum number of supported sessions for this interface at 250000:

```
bind address 1.2.3.4 max-sessions 250000
```
**caller-preference**

Enables custom SIP caller preferences; standards-based caller preference will not be applied.

**Product**
SCM

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration

```plaintext
configure > context context_name > cscf service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-service)#
```

**Syntax**

`caller-preference custom`

```
[ default | no ] caller-preference
```

**Usage**

Use this command to enable or disable custom SIP caller preferences.
charging

Enables Rf charging in this CSCF service for SIP messages.

Product
SCM

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > CSCF Service Configuration

configure > context context_name > cscf service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-cscf-service)#

Syntax

[ default | no ] charging

  default | no

  Disables Rf charging in this CSCF service for SIP messages.

Usage

Use this command to enable the RF charging feature in this service and enter the CSCF Charging Configuration Mode.

Entering this command results in the following prompt:

[context_name]host_name(config-cscf-charging)#

CSCF Charging Configuration Mode commands are defined in the CSCF Charging Configuration Mode Commands chapter in this guide.
**cnsa-media-profile**

Configures the media profile id to be set for a previously created service policy.

**Product**

SCM (S-CSCF)

**Privilege**

Administrator

**Mode**

Exec > Global Configuration > Context Configuration > CSCF Service Configuration

```
configure > context context_name > cscf service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-service)#
```

**Syntax**

```
[ no ] cnsa-media-profile profile_id cscf-service-policy policy_name content-type {
  application-3gpp-ims-xml | application-pidf-diff-xml | application-pidf-partial-xml |
  application-pidf-xml | application-reginfo-xml | application-sdp | application-xml |
  message-sipfrag | multipart-mixed | multipart-related | text-plain }
```

- **no**
  
  Removes the media profile from the service policy.

```
cnsa-media-profile profile_id
```

Specifies the media profile id.

*profile_id* must be an integer from 0 to 10 and be an existing media profile id in the system. CNSA media profile ids are created and maintained in the CSCF ISC Template Configuration Mode.

```
cscf-service-policy policy_name
```

Assigns the media profile id to a service policy.

*policy_name* must be from 1 to 63 alpha and/or numeric characters and be an existing policy name in the system. Service policies are created and maintained in the CSCF Policy Configuration Mode.

```
cnsa-media-profile profile_id
cscf-service-policy policy_name
```

```
content-type {
  application-3gpp-ims-xml | application-pidf-diff-xml |
  application-pidf-partial-xml | application-pidf-xml | application-reginfo-xml |
  application-sdp | application-xml | message-sipfrag | multipart-mixed |
  multipart-related | text-plain }
```

Specifies the content type(s).

- **application-3gpp-ims-xml** - format for exchanging information in SIP Requests and Responses as used within the 3GPP IM CN Subsystem
- **application-pidf-diff-xml** - contains changed presence elements. Contains full presence document when there are many changes
- **application-pidf-partial-xml** - contains only changed parts of PIDF-based presence information
- **application-pidf-xml** - XML MIME entity that contains presence information
- **application-reginfo-xml** - used in Notifications to SIP user agents about registration expiry
**application-sdp** - SDP session description
**application-xml** - content type for generic xml documents
**message-sipfrag** - contains subsets of well formed SIP messages
**multipart-mixed** - intended for use when the body parts are independent and need to be bundled in a particular order
**multipart-related** - intended for compound objects consisting of several inter-related body parts
**text-plain** - plain text

**Important:** You may specify multiple types of content.

Usage

Use this command to assign a media profile id to a service policy. The policies defined in the service policy apply to all subscribers using this service.

CNSA media profile ids are created and maintained in the CSCF ISC Template Configuration Mode. Service policies are created and maintained in the CSCF Policy Configuration Mode.

Example

The following command defines the media profile id as 2 and assigns it to `serv_policy3` with plain text content type.

```plaintext
cnsa-media-profile 2 cscf-service-policy serv_policy3 content-type text-plain
```
core-service

Configures a core service if:

- CSCF services are run in bridging (Back-to-Back User Agent) mode
- A-BG is an Application-level Gateway (ALG) for Network Address Translation (NAT)

By default, no core-service name will be present.

**Product**

SCM (CSCF, A-BG)

**Privilege**

Administrator

**Mode**

Exec > Global Configuration > Context Configuration > CSCF Service Configuration

```
configure > context context_name > cscf service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-service)#
```

**Syntax**

```
[ no ] core-service name service_name
```

- **no**
  - Removes the core service.

- **name service_name**
  - Specifies the name of the core service.
  - `service_name` must be from 1 to 80 alpha and/or numeric characters.

**Usage**

Use this command to assign a core service to the CSCF/A-BG service.

**Example**

The following command identifies the core service:

```
core-service name service1
```
custom cdf-selection

Enables using the CDF selected during registration for “VT” calls. For other calls, the CDF in default AAA-Group is used. Default is disabled.

Product
SCM (S-CSCF)

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > CSCF Service Configuration
configure > context context_name > cscf service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-cscf-service)#

Syntax

[ no ] custom cdf-selection

no
When disabled, the CDF selected during registration shall be used for all calls.

Usage
Use this command to apply prefix-based CDF selection logic for VT calls only. For non-VT calls, CDF in default AAA Group is used.
When disabled, prefix-based CDF selection logic is applied for all calls.
custom reason-header-cause

This command configures SIP Reason header cause value.

Product
SCM (S-CSCF)

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > CSCF Service Configuration
configure > context context_name > cscf service service_name

Entering the above command sequence results in the following prompt:
[context_name]host_name(config-cscf-service)#

Syntax

custom reason-header-cause node-type node_type node-number node_num base-cause-code cause_code

no custom reason-header-cause node-type

no
Disables SIP reason header cause configuration.

(node-type node_type
Specifies the node type and indicates P-CSCF or S-CSCF.
node_type must be an integer from 1 to 9.

(node-number node_num
Specifies the node number assigned to the node.
node_num must be an integer from 1 to 99.

(base-cause-code cause_code
Specifies the base number to be added to internal cause code.
cause_code must be an integer from 1 to 65536.
Default: 999

Usage
Use this command to configure parameters which will be used for building the SIP Reason header's cause value.

Example
The following command sets the node type to 1, node number to 5 and base cause code value to 7000:
custom reason-header-cause node-type 1 node-number 5 base-cause-code 7000
custom reg-binding

Enables the S-CSCF to return only one binding (latest contact) for each registration without including other bindings, if any. Default is disabled.

**Product**
SCM (S-CSCF)

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration

```
configure > context context_name > cscf service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-service)#
```

**Syntax**

```
[ no ] custom reg-binding
```

```
no
```

S-CSCF returns all the bindings for AOR in 200 OK REGISTER response.

**Usage**

Use this command to control whether the S-CSCF returns only one or all bindings for AOR in 200 OK REGISTER response.
custom response

Configures reject with specific response code for UE capability failure or UE status. Feature is disabled by default.

Product
SCM (S-CSCF)

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > CSCF Service Configuration

configure > context context_name > cscf service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-cscf-service)#

Syntax

custom response { ue-capability-failure capability_type | ue-status status } reject response-code response_code

no custom response { ue-capability-failure capability_type | ue-status status }

no

Removes customer-specific UE capability failure or UE status configuration, if present, and uses default RFC/3GPP specification behavior.

ue-capability-failure capability_type

Specifies UE capability failure type:

- all - UE capability all
- at - UE capability AT
- audio - UE capability audio
- chat - UE capability CHAT
- cs - UE capability CS
- ft - UE capability FT
- im - UE capability IM
- lte-voip - UE capability LTE-VOIP
- lte-vt - UE capability LTE-VT
- mms - UE capability MMS
- msg - UE capability MSG
- oma-sip-im - UE capability OMA SIP-IM
- rcs-dp - UE capability RCS-e DP
- rcs-e - UE capability RCS-E
CSCF Service Configuration Mode Commands

- `rcs-ft` - UE capability RCS-e FT
- `rcs-im` - UE capability RCS-e IM
- `rcs-is` - UE capability RCS-e IS
- `rcs-sp` - UE capability RCS-e SP
- `rcs-vs` - UE capability RCS-e VS
- `smart-edu` - UE capability SMART-EDU
- `text` - UE capability text
- `video` - UE capability video
- `vt` - UE capability VT
- `vt-ft` - UE capability VT-FT
- `vt-is` - UE capability VT-IS
- `vt-loc` - UE capability VT-LOC
- `vt-memo` - UE capability VT-MEMO

```
ue-status status
```

Specifies UE status:
- `1x-busy` - UE status 1x-busy
- `all` - UE status all
- `idle` - UE status idle
- `power-off` - UE status power-off
- `unreg` - UE status unreg
- `vt-busy` - UE status vt-busy

```
reject response-code response_code
```

Specifies reject for UE capability failure with specific response code.
`response_code` must be an integer from 400 to 699.

**Usage**
As per RFC/3GPP specifications, S-CSCF rejects with 480 response code for UE capability failure (caller preference) or UE status. Use this command to configure the S-CSCF to reject with specific response code based on UE capability failure or UE status.

**Example**
The following command configures S-CSCF reject with response code 455 for a UE capability audio failure.

```
custom-response ue-capability-failure audio reject response-code 455
```
**custom volte**

Enables custom Voice over LTE (VoLTE) features.

**Product**
SCM

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration

```bash
configure > context context_name > cscf service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-service)#
```

**Syntax**

```
[ default | no ] custom volte
```

- **default** | **no**

  Disables custom features.

**Usage**

Use this command to enable or disable custom VoLTE features.
default-aor-domain

Configures the domain name of the service.

Product
SCM

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > CSCF Service Configuration

configure > context context_name > cscf service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-cscf-service)#

Syntax

[ no ] default-aor-domain alias

no

Removes the domain name from the service.

alias

Specifies the domain name for the service.

alias is the name of the domain for this service and must be from 1 to 79 alpha and/or numeric characters in length.

Usage

Use this command to define the domain name of the service.

Example

The following command defines the domain name of the CSCF service as business.com:

default-aor-domain business.com
emergency-cscf

Enables the Emergency-CSCF for the service and enters the Emergency-CSCF Configuration Mode. Default is disabled.

Product
SCM

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > CSCF Service Configuration

configure > context context_name > cscf service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-cscf-service)#

Syntax

[ no ] emergency-cscf

no

Disables the E-CSCF for the service.

Usage

Use this command to enable the Emergency-CSCF feature and enter the Emergency-CSCF Configuration Mode.

Entering this command results in the following prompt:

[context_name]host_name(config-cscf-service-emergency-cscf)#

Emergency-CSCF Configuration Mode commands are defined in the CSCF Emergency-CSCF Configuration Mode Commands chapter in this guide.

ℹ️ **Important:** Only one function (P-CSCF, S-CSCF, E-CSCF, SIP Proxy, or A-BG) can be enabled per service.
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**

Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

```bash
exit
```

**Usage**

Use this command to return to the parent configuration mode.
**history-info**

Enables the addition of the history-info header to SIP requests in order to capture request URI information. By default, this command is disabled.

**Product**
SCM

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration

```plaintext
configure > context context_name > cscf service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-service)#
```

**Syntax**

```
[ default | no ] history-info
```

---

<table>
<thead>
<tr>
<th><code>default</code></th>
<th><code>no</code></th>
</tr>
</thead>
<tbody>
<tr>
<td>Disables the inclusion of the history-info header.</td>
<td></td>
</tr>
</tbody>
</table>

**Usage**

Use this command to include the history-info header in SIP requests to capture the request URI information for routing or translation.
interface statistics sip

Enables interface SIP statistic collection in this CSCF service.

**Product**
SCM

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration
configure > context context_name > cscf service service_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-service)#
```

**Syntax**

```
[ default | no ] interface statistics sip
```

- **default | no**

  Disables interface SIP statistic collection for this service.

**Usage**

Use this command to enable or disable the collection of interface SIP statistics in this service.
interrogating-cscf

This command is not supported in this release.
**ipv4-ipv6-interworking**

Allows the P-CSCF to provide IPv4-IPv6 interworking when UEs are IPv6-only and the IMS core network is IPv4-only. Feature is disabled by default.

**Product**
SCM (P-CSCF)

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration
configure > context context_name > cscf service service_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-service)#
```

**Syntax**

```
[ no ] ipv4-ipv6-interworking
```

- **no**
  Disables the feature.

**Usage**

Use this command to allow IPv4-IPv6 interworking functionality.
keepalive

Configures the CSCF to receive and respond to different types of keep-alive requests.

**Product**
SCM

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration

```
configure > context context_name > cscf service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-service)#
```

**Syntax**

```


no keepalive [ method { crlf | stun } ]
```

---

**default**

Returns the command to the default settings. All methods are enabled by default. See keywords above for specific defaults.

---

**no**

Disables the specified method of keepalive messages.

---

**expire-timer sec**

Default: 29

This value is used according to timed-keepalives parameter present in Path header. UEs are expected to send keepalive messages according to this time interval.

`sec` must be an integer from 24 to 150.

---

**max-retry num**

Default: 3

Specifies the maximum number of times the CSCF waits for the UE to send a keepalive request before it deletes the user information.

`num` must be an integer from 1 to 10.

---

**method { crlf | stun }**

Default: both methods enabled.
Specifies the method of keepalive messages supported by the CSCF.

**cr1f**: "\r\n" string (CRLF packets) sent by UE

**stun**: STUN protocol messages (rfc3489-bis)

### Usage

Use this command to configure how the CSCF manages keepalive requests.

### Example

The following example sets the expire timer to 40 and the maximum retry parameter to 5:

```
keepalive expire-timer 40 max-retry 5
```
lawful-intercept

Enables Lawful Intercept (LI) in this CSCF service. Feature is disabled by default.

Product
SCM

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > CSCF Service Configuration

configure > context context_name > cscf service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-cscf-service)#

Syntax

[ no ] lawful-intercept

no

Disables the feature.

Usage

Refer to the Lawful Intercept Configuration Guide for more information on LI.
li-packet-cable

Refer to the *Lawful Intercept Configuration Guide* for a description of this command.
**max-reqmsg-size**

Configures the maximum SIP Request processing size.

**Product**
SCM

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration
`configure > context context_name > cscf service service_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-service)#
```

**Syntax**

```
[ no ] max-reqmsg-size sipreq_size
```

- **no**
  Disables the SIP processing configuration.
  If disabled, then P-CSCF will not reject the message with 513 and the old functionality of message drop based on `max-sipmsg-size` will only apply.

- **sipreq_size**
  Configures the SIP request processing size limit in bytes.
  `sipreq_size` must be an integer from 1024 to 65535.

**Usage**
Use this command to configure the maximum SIP Request processing size.
The configured value for `max-reqmsg-size` must always be lesser than the configured value for `max-sipmsg-size` in the same CSCF service for the new implementation to take effect.

**Example**
The following command limits the SIP request processing size to 1024 bytes:

```
max-reqmsg-size 1024
```
max-sipmsg-size

Configures the maximum SIP message size.

Product
SCM

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > CSCF Service Configuration
configure > context context_name > cscf service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-cscf-service)#

Syntax

max-sipmsg-size limit

[ default | no ] max-sipmsg-size

default | no
Returns/sets the maximum SIP message size to 4096 bytes.

limit
Default: 4096
Configures the SIP message size limit in bytes.
limit must be an integer from 1024 to 65535.

Important: Maximum SIP message size should be more than the message-max-size set in the CSCF Proxy-CSCF Configuration Mode.

Usage

Use this command to configure the maximum SIP message size.

Example

The following command limits the SIP message size to 4500 bytes:

max-sipmsg-size 4500
**media-bridging**

Enables SDP modification that terminate media on CSCF. Feature is disabled by default.

**Product**
SCM (P-CSCF)

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration

```
configure > context context_name > cscf service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-service)#
```

**Syntax**

```
media-bridging [ v6port-range start_port end_port ]

no media-bridging
```

**no**

Disables the feature.

**v6port-range start_port end_port**

Specifies port ranges to be used with IPv6 addresses. Only selected ports from the range specified should be used for media bridging.

- **start_port**: Start of port range; must be an integer from 1024 to 65535.
- **end_port**: End of port range; must be an integer from 1025 to 65535.

**Usage**

Use this command to allow termination of media on CSCF.

**Example**

The following command allows media bridging on ports 2000 to 4000 for IPv6 addresses:

```
media-bridging v6port-range 2000 4000
```
monitoring

Enables thresholds alerting for this CSCF service.

Product
SCM

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > CSCF Service Configuration

configure > context context_name > cscf service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-cscf-service)#

Syntax

monitoring

Usage

Use this command to enable thresholds alerting for this CSCF service.
multiple-reg same-private-id

This command allows multiple registrations for the same private user-id from different devices.

Product
SCM (P-CSCF, A-BG, S-CSCF)

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > CSCF Service Configuration

configure > context context_name > cscf service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-cscf-service)#

Syntax

[ default | no ] multiple-reg same-private-id

default | no
Multiple registrations are not allowed for the same private user-id.

Usage
Use this command to allow or disallow multiple registrations for the same private user-id from different devices.

Example
The following command allows multiple registrations for the same private user-id from different devices:

multiple-reg same-private-id
nat-policy

Configures a NAT (Network Address Translation) policy for the service if the CSCF service is performing one of the following functions:

- CSCF services are run in bridging (Back-to-Back User Agent) mode
- A-BG is an Application-level Gateway (ALG) for NAT

Product
SCM (CSCF A-BG)

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > CSCF Service Configuration

configure > context context_name > cscf service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-cscf-service)#

Syntax

nat-policy policy_name { private-address (address ip_address_mask | default | range
start_ip_address end_ip_address ) } | bridge-network { address ip_address_mask | range
start_ip_address end_ip_address }

no nat-policy policy_name

no
Removes the specified NAT policy from the service.

policy_name
Specifies a name for the NAT policy.
policy_name must be from 1 to 79 alpha and/or numeric characters.

private-address { address ip_address_mask | default | range start_ip_address
end_ip_address }

Specifies the private-address policy type for nat-pool.
address ip_address_mask: Address for nat-policy policy type for nat-pool. Specifies a combined IP address subnet mask bits to indicate what IP addresses the specific policy type applies to. ip_address_mask must be specified using the form “IP Address/Mask Bits” where the IP address must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6, and the mask bits are a numeric value, which is the number of bits in the subnet mask.

default: Default for nat-policy policy type for nat-pool. Default is defined as the address range specified by rfc1918.

- 10.0.0.0 - 10.255.255.255 (10/8 prefix)
- 172.16.0.0 - 172.31.255.255 (172.16/12 prefix)
- 192.168.0.0 - 192.168.255.255 (192.168/16 prefix)
range start_ip_address end_ip_address: Range for nat-policy policy type for nat-pool.
  • start_ip_address specifies the beginning of the range of addresses.
  • end_ip_address specifies the end of the range of addresses.
  • ip_address must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6.

bridge-network { address ip_address_mask | range start_ip_address end_ip_address }

Specifies the bridge-network policy type for S-CSCF bridging.
address ip_address_mask: Address for bridge-network policy type for S-CSCF bridging. Specifies a combined IP address subnet mask bits to indicate what IP addresses the specific policy type applies to. ip_address_mask must be specified using the form “IP Address/Mask Bits” here the IP address must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6, and the mask bits are a numeric value, which is the number of bits in the subnet mask.
range start_ip_address end_ip_address: Range for bridge-network policy type for S-CSCF bridging.
  • start_ip_address specifies the beginning of the range of addresses.
  • end_ip_address specifies the end of the range of addresses.
  • ip_address must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6.

Usage

Generally, if a SIP packet has a VIA address (physical address that identifies where the service is located) different from the Source address, ALG functionality is invoked. Even if the VIA and Source addresses are the same, however, this command allows the ALG functionality to be started. For ALG to start, the VIA address should belong to one of the nat-policy address ranges.

Example

The following command identifies the NAT policy named policy1 with a private-address policy type of 10.10.10.10 255.255.255.0:

```
nat-policy policy1 private-address address 10.10.10.10 255.255.255.0
```

The following command identifies the NAT policy named policy2 with a private-address range policy type of 172.162.23.23 172.162.23.230:

```
nat-policy policy2 private-address address 172.162.23.23 172.162.23.230
```

The following command identifies the NAT policy named policy3 with a default policy type:

```
nat-policy policy3 private-address default
```
nat-pool

Configures a NAT (Network Address Translation) pool for the service if the CSCF service is performing one of the following functions:

- P-CSCF services are run in bridging (Back-to-Back User Agent) mode
- A-BG is an Application-level Gateway (ALG) for NAT

By default, no nat-pool name will be present.

**Product**
SCM (P-CSCF A-BG)

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration

```
cscf service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-service)#
```

**Syntax**

```
nat-pool name pool_name [ signalling-pool signalling_pool_name ]
no nat-pool name pool_name
```

**no**

Removes the NAT pool from the service.

**name pool_name**

Specifies the name of an existing NAT pool.

`pool_name` must be from 1 to 32 alpha and/or numeric characters.

**Important:** NAT pools are created in Context Configuration Mode with the `ip pool` command.

```
signalling-pool signalling_pool_name
```

Specifies the name of an existing IP pool from where IP addresses will be used to fill in signalling headers only.

`signalling_pool_name` must be from 1 to 32 alpha and/or numeric characters.

**Important:** If `signalling-pool` is not specified, service IP:port will be filled in signalling headers.

**Usage**

Use this command to assign a NAT pool to the P-CSCF/A-BG service.
The following command identifies the NAT pool:

```
nat-pool name pool2
```
policy

Enables or disables early media support and IBCF capability in P-CSCF/A-BG. In addition, configures Interim-Interval value for CSCF accounting sessions, overload response, and the congestion control threshold and tolerance values that are to be monitored on this CSCF service.

Product
SCM (P-CSCF, A-BG)

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > CSCF Service Configuration

configure > context context_name > cscf service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-cscf-service)#

Syntax

```
policy { accounting interim-interval value | allow-early-media | ibcf-capability domain domain/name | overload [ drop | redirect IPv4_address1 [ weight weight1 ] [ IPv4_address2 [ weight weight2 ] ] ... | reject ] | threshold congestion-control { system-cpu-utilization percent | tolerance percent } }

default policy { allow-early-media | overload | threshold congestion-control { system-cpu-utilization | tolerance } }

no policy { accounting interim-interval | allow-early-media | ibcf-capability domain domain/name | overload [ redirect IPv4_address1 ] [ IPv4_address2 ] ... | threshold congestion-control { system-cpu-utilization | tolerance } }

default

Returns the command to the default settings. See keywords above for specific defaults.

no

Disables the specified functionality.

accounting interim-interval value

Default: Disabled
Used to configure Interim-Interval value for CSCF accounting sessions.
value can be configured to any integer value from 50 to 7200. This value is sent in the “Acct-Interim-Interval” AVP of the accounting message. Based on the response message from accounting server, Interim-Interval timer is started.

allow-early-media

Default: Enabled
Allows early media by doing QoS commit during QoS Authorization (with PCRF) in P-CSCF.
ibcf-capability domain domain/name

Enables IBCF capability to support Mx reference point in CSCF.
IBCF capability domain name must be entered using from 1 to 80 alpha and/or numeric characters.

Important: This CLI can be repeated to add/delete multiple entities to/from the ibcf-capability domain table. An ibcf-capability domain can be removed by using the no keyword; using the no keyword without giving any domain name will delete all entries from the list.

overload [ drop | redirect IPv4_address1 [ weight weight1 ] [ IPv4_address2 [ weight weight2 ] ] ... | reject ]

Configures the overload response for this policy. When the P-CSCF/A-BG becomes congested, this overload policy is used to drop/reject subsequent sessions or redirect them to another server.

drop: Specifies that upon policy overload, the system will drop the session.
redirect: Specifies that upon policy overload, the system will redirect the session to another CSCF.

• IPv4_address1 must be expressed in dotted decimal notation.
• weight weight1: Defines the priority of the redirect address.
  weight1 must be an integer from 1 to 10. Default is 1.
reject: Specifies that upon policy overload, the system will reject the session with 503 (Service Unavailable) SIP error response. This is the default setting.

threshold congestion-control { system-cpu-utilization percent | tolerance percent}

Enables congestion control. CSCF performs congestion control based on the memory usage inside every sessmgr at two levels.

• Level 1: For every new call/event received, the system checks if sessmgr memory-usage is above a threshold value (such as 95 percent). If it is, memory-congestion is triggered and new call messages are rejected with 500 SIP response. Memory congestion is disabled when memory usage drops by a tolerance value (default is 10 percent).

• Level 2: If the sessmgr usage reaches 100 percent, all newly received SIP messages are dropped at the socket layer in that sessmgr except for the BYE message. The new SIP messages are not processed until the memory reaches the threshold value (95 percent).

A trap is also generated whenever sessmgr is in congestion state

system-cpu-utilization percent: The average percent utilization of a CPU in a PSC/PSC2/PSC3 running the CSCF service as measured in 10 second intervals.
percent can be configured to any integer value from 0 to 100. This value becomes the upper threshold for triggering the CPU-based congestion for CSCF services. Default is 80
tolerance percent: The percentage under a configured threshold that dictates the point at which the condition is cleared.
percent is an integer value from 1 to 25. Default is 5

Usage

Use this command to set the following policy for this CSCF service:
• Configure Interim-Interval value for CSCF accounting sessions.

• Set QoS support during either the initial SDP response or the 200OK response to the INVITE. When allow-early-media is enabled, QoS commit is done during initial SDP answer. When disabled, QoS commit is done during 200OK INVITE. By default, this command is enabled.
• Enable or disable IBCF capability.
• Define the response to an overload condition.
• Set thresholds to dictate the conditions for which congestion control is to be enabled and establish limits for defining the state of the CSCF service (congested or clear). The tolerance parameter establishes the threshold at which the condition is cleared.

**Important:** When congestion is triggered, new CSCF calls are not rejected.

**Example**

The following command sets the upper threshold for CPU utilization for triggering congestion control at 90%.

```
policy threshold congestion-control system-cpu-utilization 90
```

The following command sets the tolerance to its default value of 5.

```
default policy threshold congestion-control tolerance
```
**policy-name**

Assigns a previously created service policy to this service.

**Product**
SCM

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration

```bash
configure > context context_name > cscf service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-service)#
```

**Syntax**

```bash
policy-name name

no policy-name
```

- **name**
  Remove the assigned service policy from this service.

- **name**
  Specifies the name of the service policy being assigned to this service.
  
  *name* must be from 1 to 79 alpha and/or numeric characters and be an existing policy name in the system.
  
  Service policies are created and maintained in the CSCF Policy Configuration Mode.

**Usage**

Use this command to assign a service policy to this service. The policies defined in the service policy apply to all subscribers using this service. Service policies are created and maintained in the CSCF Policy Configuration Mode.

**Example**

The following command assigns a service policy named *serv_policy3* to this service:

```bash
policy-name serv_policy3
```
proxy-cscf

Enables the Proxy-CSCF for the service and enters the Proxy-CSCF Configuration Mode. Default is disabled.

**Product**
SCM (P-CSCF)

**Privilege**
Administrator

**Mode**
 Exec > Global Configuration > Context Configuration > CSCF Service Configuration
`configure > context context_name > cscf service service_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-service)#
```

**Syntax**

```
[ no ] proxy-cscf
```

```
no
```

Disables the P-CSCF for the service.

**Usage**
Use this command to enable the Proxy-CSCF feature and enter the Proxy-CSCF Configuration Mode. Entering this command results in the following prompt:

```
[context_name]host_name(config-cscf-service-proxy-cscf)#
```

Proxy-CSCF Configuration Mode commands are defined in the *CSCF Proxy-CSCF Configuration Mode Commands* chapter in this guide.

**Important:** The Proxy-CSCF is a license-enabled function of the Session Control Manager. Only one function (P-CSCF, S-CSCF, E-CSCF, SIP Proxy, or A-BG) can be enabled per service.
proxy-serving-cscf

This command is not supported in this release.
**recurse-on-redirect-resp**

Enables the 3xx recursion feature. If enabled, the service will send further invites to the contacts specified upon receiving a 3xx redirect response. Default is disabled.

**Product**
SCM

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration

```bash
configure > context context_name > cscf service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-service)>
```

**Syntax**

```
[ no ] recurse-on-redirect-resp
```

<table>
<thead>
<tr>
<th>no</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disables the 3xx recursion feature.</td>
</tr>
</tbody>
</table>

**Usage**

When enabled and on receipt of a 3xx response, the service will collect the SIP URIs present in the Contact header(s) of 3xx and recursively contact each one of them until the call succeeds. The contacts are tried serially. There is a maximum implementation limit of 50 URIs. Each contact, in turn, can send a 3xx response. The service will honor them and append the new contacts. When disabled, the service treats a 3xx response as the final failure response and declares the call attempt “failed”. By default, this feature is disabled.

**Example**

Enable recursion on 3xx:

```
recurse-on-redirect-resp
```

Disable recursion on 3xx:

```
no recurse-on-redirect-resp
```
reject-on-cnsa-failure

Enables rejection of messages on Core Network Service Authorization failure. Default is disabled.

**Product**
SCM

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration

`configure > context context_name > cscf service service_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-service)#
```

**Syntax**

```
[ no ] reject-on-cnsa-failure
```

- **no**
  Disables the rejection of messages on Core Network Service Authorization failure.

**Usage**

Enables rejection of messages on Core Network Service Authorization failure. By default, this feature is disabled.

In a mobile originating case, S-CSCF checks for the presence of P-Preferred-Service (PPS) header. If the header is present, media profile authentication is successful and if the incoming ICSI (IMS Communication Service Identifier) value also matches with one of the values in the service_id list, then the request will be forwarded after replacing the PPS header with PAS (P-Asserted-Service). If media profile authentication fails, S-CSCF will check `reject-on-cnsa-failure`. If enabled, then call is rejected with 403 message. If disabled, a default ICSI is selected from the service_id list and will be put into PAS while forwarding the request by the S-CSCF on service authentication failure.

In PPS is not received by the S-CSCF and media profile authentication is successful, an ICSI from the service_id list, if present, is selected and will be added in PAS header. If media profile authentication fails, `reject-on-cnsa-failure` is checked. If enabled, call is rejected with 403 message. If disabled, PAS header is added if service_id list is present with an ICSI value.

**Example**

Enable rejection of messages on Core Network Service Authorization failure:

```
reject-on-cnsa-failure
```

Disable rejection of messages on Core Network Service Authorization failure:

```
no reject-on-cnsa-failure
```
release-call-on-media-loss

Release call on detection of media loss.

Product
SCM (P-CSCF, A-BG)

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > CSCF Service Configuration

configure > context context_name > cscf service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-cscf-service)#

Syntax

release-call-on-media-loss media-type audio [ timeout seconds ]

no release-call-on-media-loss

no
Disables the release of SIP calls upon the detection of media loss.

media-type audio
Enables the release of SIP calls upon the detection of media loss on media-type audio.

timeout seconds
Specifies the media loss timeout value; media loss after timeout value results in call release.
seconds must be an integer from 5 to 3600.
If timeout value is not configured, media loss after 5 seconds results in call release.

Usage
Use this command to enable the release of SIP calls upon the detection of media loss.

Example
Enables the release of SIP calls upon the detection of media loss:

release-call-on-media-loss media-type audio

Enables the release of SIP calls upon the detection of media loss:

no release-call-on-media-loss
rfc3261-proxy

Enables RFC3261 proxy (SIP Proxy) for this service and enters the SIP Proxy Configuration Mode. Default is disabled.

**Product**  
SCM (SIP Proxy)

**Privilege**  
Administrator

**Mode**  
Exec > Global Configuration > Context Configuration > CSCF Service Configuration  
`configure > context context_name > cscf service service_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-service)#
```

**Syntax**

```
[ default | no ] rfc3261-proxy
```

- `default | no`
  - Disables RFC3261 proxy in this service.

**Usage**

Use this command to enable the Sip Proxy feature and enter the SIP Proxy Configuration Mode. Entering this command results in the following prompt:

```
[context_name]hostname(config-cscf-service-rfc3261-proxy)#
```

SIP Proxy Configuration Mode commands are defined in the *CSCF SIP Proxy Configuration Mode Commands* chapter in this guide.

**Important:** The SIP Proxy is a license-enabled function of the Session Control Manager. Only one function (P-CSCF, S-CSCF, E-CSCF, SIP Proxy, or A-BG) can be enabled per service.
server-header

This command determines the handling of the server header. This is applicable for B2BUA mode only; Proxy mode will forward the message as it is.

Product
SCM (P-CSCF, A-BG, S-CSCF, SIP Proxy)

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > CSCF Service Configuration

`configure > context context_name > cscf service service_name`

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-cscf-service)#`

Syntax

```
server-header { name header_name | pass-through }

[ default | no ] server-header
```

<table>
<thead>
<tr>
<th>default</th>
</tr>
</thead>
</table>
| Sets the server header to the default server header. The default server name is “Cisco”.

<table>
<thead>
<tr>
<th>no</th>
</tr>
</thead>
</table>
| Suppresses server header; no server header is forwarded or added.

<table>
<thead>
<tr>
<th>name header_name</th>
</tr>
</thead>
</table>
| Sets the server header to the value specified by `header_name`. `header_name` must be from 1 to 63 alpha and/or numeric characters.

<table>
<thead>
<tr>
<th>pass-through</th>
</tr>
</thead>
</table>
| S-CSCF forwards the server header received without any modification. If no server header is received, no server header is added.

Usage
Use this command to determine the handling of the server header, including forwarding, modifying, adding, or suppressing.

Example
The following command forwards the server header received without any modification:

```
server-header pass-through
```
server-name

Enables/disables filling the server name AVP in MAR and SAR for Cx interface, and the From header in third party register request, with configured server name. In addition, it can be used by other CSCF service to fill From header while performing peer server monitoring using OPTIONS request. This command is disabled by default.

**Product**
SCM (S-CSCF)

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration

```
configure > context context_name > cscf service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-service)#
```

**Syntax**

```
server-name server_name

no server-name
```

**no**

S-CSCF uses configured cscf-hostname or bind IP address to fill the server name AVP in MAR and SAR for Cx interface. This is the default CSCF behavior.

**server_name**

Configures the name that will be used to fill the server name AVP in MAR and SAR for Cx interface, and the From header in third party register request. In addition, it can be used by other CSCF service to fill From header while performing peer server monitoring using OPTIONS request.

*name* must be from 1 to 63 alpha and/or numeric characters.

**Usage**

Use this command to enable/disable filling the server name AVP in MAR and SAR for Cx interface, and the From header in third party register request, with configured server name. In addition, it can be used by other CSCF service to fill From header while performing peer server monitoring using OPTIONS request.

**Example**

The following command configures the CSCF server name as `stp-c-scscfl.cisco.co.kr`:

```
server-name stp-c-scscfl.cisco.co.kr
```
serving-cscf

Enables Serving-CSCF for the service and enters the Serving-CSCF Command Mode. Default is disabled.

**Product**
SCM (S-CSCF)

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration
configure > context context_name > cscf service service_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-service)#
```

**Syntax**

```
[ no ] serving-cscf
```

- **no**
  Disables S-CSCF for the service.

**Usage**

Use this command to enable the Serving-CSCF feature and enter the Serving-CSCF Configuration Mode. Entering this command results in the following prompt:

```
[context_name]host_name(config-cscf-service-serving-cscf)#
```

Serving-CSCF Configuration Mode commands are defined in the *CSCF Serving-CSCF Configuration Mode Commands* chapter in this guide.

**Important:** The Serving-CSCF is a license-enabled function of the Session Control Manager. Only one function (P-CSCF, S-CSCF, E-CSCF, SIP Proxy, or A-BG) can be enabled per service.
serving-cscf-list

Configure a list of Serving CSCFs and their capabilities.

Product
SCM

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > CSCF Service Configuration
cfg-context context_name > cscf service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-cscf-service)#

Syntax

[ no ] serving-cscf-list server { address address | domain domain } { capability value | port num } { capability value } }

| no |
| Removes an entry from this list. |

| server { address address | domain domain } |
| Specifies the S-CSCF server. |

| address address |
| IP addresses must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6. |

| domain domain |
| Domain names must be entered using from 1 to 80 alpha and/or numeric characters. |

| capability value |
| Specifies the capability of the S-CSCF server. value is assigned by the Service Provider and may be an integer from 1 to 999999. |

| port num |
| Specifies the port at which service is provided by the S-CSCF server. num may be an integer from 1 to 65535. |

Usage

Use this command to configure a list of Serving CSCFs and their capabilities.

Important: This command can be entered multiple times to identify multiple Serving CSCFs.

Example

The following command adds a S-CSCF with an IP address of 1.2.3.4 and a capability value of 75 to this service’s list:

serving-cscf-list server address 1.2.3.4 capability 75
**session-timer**

Configures the session expiry for sessions (Session will expire at the configured value unless refreshed.) and the minimum number of seconds in a session timer (session-expires) value the system will allow.

**Product**
SCM

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration

```
configure > context context_name > cscf service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-service)#
```

**Syntax**

```
session-timer { min-se sec [ session-expires sec ] | session-expires sec [ min-se sec ] }

default session-timer [ min-se ] [ session-expires ]

no session-timer
```

- **default**
  Returns the command to the default settings.

- **no**
  Disables the session timer.

- **min-se sec**
  Default: 90
  Specifies the minimum number of seconds the system will allow a session-expires value in a session request.
  `sec` must be an integer value between 90 and the value of the `session-expires` command.

- **session-expires sec**
  Default: 1800 (30 minutes)
  Specifies the number of seconds a session is allowed exist before it expires.
  `sec` must be an integer value between 90 and 18000.

**Usage**

Use this command to set a session expiry value for all invites generated by the SCM and a minimum value for a session request session timer the system will allow. If a session is requested with a timer of less than this command’s value, the system will reject the request with a “422 Session Interval Too Small” response code.

**Example**

The following command sets the session expiry for all sessions generated by the SCM to 60 minutes:
session-timer session-expires 3600
strict-check configured-aor-domain

Enables strict checking on default-aor-domain so S-CSCF will reject registration and invite if there is a mismatch between AoR in To/From and the configured default-aor-domain.

**Product**
SCM (S-CSCF)

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration

```plaintext
configure > context context_name > cscf service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-service)#
```

**Syntax**

```
[ default | no ] strict-check configured-aor-domain
```

**Usage**

Use this command to enable or disable strict checking on default-aor-domain. This allows support for registration of subscribers from multiple domains.
strict-outbound

When enabled, the CSCF rejects registration without outbound parameters from an already registered AoR (the AoR would have included outbound parameters in a previous registration). When disabled, the CSCF allows registration without outbound parameters from the previously registered AoR.

**Product**

SCM

**Privilege**

Administrator

**Mode**

Exec > Global Configuration > Context Configuration > CSCF Service Configuration

```bash
configure > context context_name > cscf service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-service)#
```

**Syntax**

```
[ no ] strict-outbound
```

<table>
<thead>
<tr>
<th>no</th>
</tr>
</thead>
</table>

Disables the feature. This is the default behavior.

**Usage**

Use this command to reject registration from a previously registered AoR if the AoR fails to register with outbound parameters but included them in the previous registration.
**subscriber-policy-override**

Configures the system to allow the subscriber-based policy to override the service-based policy. Default is disabled.

**Product**
SCM

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration

```
configure > context context_name > cscf service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name] host_name(config-cscf-service)#
```

**Syntax**

```
[ default | no ] subscriber-policy-override
```

- **default**
  - Removes the subscriber policy override from the service.

**Usage**

By default, if a conflict occurs between the subscriber-based policy and the service-based policy, the service policy takes precedence. Use this command to override the default behavior of the system and allow the subscriber-based policy to overrule the service policy.
subscription

Enables the registration event package for the service and configures a system-wide subscription lifetime for all subscribers to the service.

**Product**
SCM

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration
```
configure > context context_name > cscf service service_name
```

Entering the above command sequence results in the following prompt:
```
[context_name]host_name(config-cscf-service)#
```

**Syntax**
```
subscription package reg [ lifetime { default sec | max sec [ default sec ] | min sec [ max sec ] [ default sec ] } ]
[ default | no ] subscription package reg
```

- **default**
  Returns the command to the default settings.

- **no**
  Disables the registration event package for the service.

- **package reg [ lifetime { default sec | max sec ] | min sec }**

  **default sec**: Specifies the default amount of time that a subscription can exist on the system. **sec** must be an integer from 60 to max sec -1.
  Default: 3761

  **Important**: **default sec** must be < or = to max sec and > or = to min sec.

  The following keywords are specific to the S-CSCF functionality:

  **max sec**: Specifies the maximum amount of time that a subscription can exist on the system.
  **sec** must be an integer from 60 to 2147483646.
  Default: 86400

  **Important**: **max sec** must be > or = to min sec.

  **min sec**: Specifies the minimum amount of time that a subscription can exist on the system.
  **sec** must be an integer from 60 to max sec -1.
  Default: 60
**Important:** min sec must be ≤ or = to max sec.

### Usage

Use this command to enable the registration event package for the service and control the amount of time subscriptions are allowed to exist on this service.

The system responds to subscriptions in the following manner:

Using default values:

- If a subscription with an expiration value lower than the service’s minimum (60) is received, the service will respond with a 423 Interval Too Small message.

- If a subscription with an expiration value higher than the service’s maximum (2147483646) is received, the service will automatically reduce the expiration value to the default value.

If a subscription is received missing the “Expires” value, or the value is malformed, the service will automatically respond with 3761 in the 200OK message.

### Example

The following command configures the maximum subscription lifetime to 43200 (12 hours):

```
subscription package reg lifetime max 43200
```
support-content-type any

Validates Content-Type in this CSCF service.

**Product**
SCM

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration

```
configure > context context_name > cscf service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-service)#
```

**Syntax**

```
[ no ] support-content-type any
```

<table>
<thead>
<tr>
<th>no</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disables the feature. If disabled, CSCF service rejects unsupported Content-Type with “415 Unsupported Media Type”.</td>
</tr>
</tbody>
</table>

**Usage**

Use this command to either allow any type of Content-Type or reject unsupported Content-Type.

**Example**

Allows any type of Content-Type for the CSCF service:

```
support-content-type any
```

Rejects unsupported Content-Type for the CSCF service:

```
no support-content-type any
```
**tcp-proxy**

Enables SIP TCP proxy for the CSCF service.

**Product**

SCM

**Privilege**

Administrator

**Mode**

Exec > Global Configuration > Context Configuration > CSCF Service Configuration

```config > context context_name > cscf service service_name```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-service)#
```

**Syntax**

```
tcp-proxy [ port port_number ]

no tcp-proxy
```

- **no**
  
  Disables SIP TCP proxy for the CSCF service

- **port port_number**
  
  Default: 5062
  
  Specifies the port used for SIP TCP proxy connections.
  
  *port_number* must be an integer from 1 to 65534.

**Usage**

Use this command to enable SIP TCP proxy for the CSCF service.

**Example**

Enables SIP TCP proxy for the CSCF service on port 5062:

```
tcp-proxy port5062
```

Disables SIP TCP proxy for the CSCF service:

```
no tcp-proxy
```
threshold

Enables thresholds alerting and configuration of thresholds for CSCF Service.

**Product**
SCM

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration

```
configure > context context_name > csf service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-service)#
```

**Syntax**

```

[ default | no ] threshold monitoring
```

<table>
<thead>
<tr>
<th><strong>default</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Returns the command to the default settings.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>no</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Disables thresholds alerting for CSCF Service.</td>
</tr>
</tbody>
</table>

```
{ call-setup-failures | call-total-active | error-no-resource | error-presence | error-reg-auth | error-tcp | invite-rcvd-rate | reg-rcvd-rate | reg-total-active | route-failures } high_thresh clear low_thresh
```

- **call-setup-failures**: Number of CSCF call setup failures.
  - Default: 0
- **call-total-active**: Number of total active CSCF calls.
  - Default: 0
- **error-no-resource**: Number of CSCF call setup failures due to no-resource.
  - Default: 0
- **error-presence**: Number of CSCF Presence errors.
  - Default: 0
- **error-reg-auth**: Number of CSCF Registration Authentication failures.
  - Default: 0
- **error-tcp**: Number of CSCF call setup failures due to TCP error.
  - Default: 0
- **invite-rcvd-rate**: Number of CSCF calls per polling interval.
  - Default: 0
- **reg-rcvd-rate**: Number of CSCF registrations per polling interval.
  - Default: 0
threshold

reg-total-active: Number of total CSCF active registrations.
Default: 0
route-failures: Maximum number of route-failures, after which the alarm/alert will be raised. Default: 5
high_thresh: The high threshold number that must be met or exceeded within the polling interval to generate an alert or alarm. Can be configured to any integer value between 0 and 2000000 (0 and 60000 for route-failures).
clear low_thresh: The low threshold number that must be met or exceeded within the polling interval to clear an alert or alarm. Can be configured to any integer value between 0 and 2000000 (0 and 60000 for route-failures).

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

monitoring
Enables thresholds alerting for CSCF Service.

**Usage**
Use this command to:
- enable/disable thresholds alerting for CSCF Service
- set an alert or an alarm when a threshold exceeds the configured level

Alerts or alarms are triggered for the number of registration reply errors on the following rules:
- Enter condition: Actual number > High Threshold
- Clear condition: Actual number < Low Threshold

**Example**
The following command configures a route failures threshold of 1000 and a low threshold of 500 for a system using the Alarm thresholding model:

```
threshold route-failures 1000 clear 500
```
timeout

Sets timeout values for CSCF and SIP transactions.

Product
SCM

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > CSCF Service Configuration

configure > context context_name > cscf service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-cscf-service)#

Syntax

timeout { hss-wait sec | map-slr-response sec | no-answer sec | policy-interface sec | sip { 3gpp-d sec | 3gpp-t1 msec | 3gpp-t2 sec | 3gpp-t4 sec | c sec | d sec | idle-tcp-connection msec | cleanup-timer msec } | invite-expiry sec | t1 msec | t2 sec | t4 sec } |

default timeout { hss-wait | map-slr-response | no-answer | policy-interface | sip { 3gpp-d | 3gpp-t1 | 3gpp-t2 | 3gpp-t4 | c | d | idle-tcp-connection | invite-expiry | t1 | t2 | t4 } }

default

Returns the command to the default settings. See keywords above for specific defaults.

hss-wait sec

Default: 5
This timer is used by S-CSCF with HSS interface for timeout.
sec must be an integer from 0 to 2147483646.

map-slr-response sec

Default: 15
This timer is used by the E-CSCF for MAP SLR response timeout.
sec must be an integer from 15 to 30.

no-answer sec

Default: 100
This timer is specially used for No-Answer Call Feature executed by S-CSCF. The timer will be started as soon as 180 Ringing response is received and No-Answer call feature is enabled. The value of this timer should be always less than INVITE Timeout used by DC-SIP.
sec must be an integer from 0 to 2147483646.
**policy-interface** `sec`

Default: 5
This timer is used by the P-CSCF/A-BG with Policy interface for timeout. `sec` must be an integer from 0 to 2147483646.

**sip** `{ 3gpp-d sec | 3gpp-t1 msec | 3gpp-t2 sec | 3gpp-t4 sec | c sec | d sec | idle-tcp-connection msec | cleanup-timer msec | invite-expiry sec | t1 msec | t2 sec | t4 sec }`

Sets transaction and expiry timers for SIP.

- **3gpp-d sec**: This timer is used to control the retransmission of 200OK messages to INVITEs after an ACK is sent. The ACK transaction is cleared after this period. This timer is applicable only for unreliable transport. `sec` must be an integer from 0 to 2147483646.
  
  Default: 64*T1 (128 seconds, recommended minimum)

- **3gpp-t1 msec**: This timer is used to control the time interval between each retransmission. The interval doubles after each retransmission. This is used by P-CSCF/A-BG only when it sending message toward the UE. Example: T1, 2T1, 4T2, etc. This timer is applicable only for unreliable transport. `msec` must be an integer from 0 to 4294967294.
  
  Default: 2000 ms (2 secs, recommended minimum).

- **3gpp-t2 sec**: This timer is used to control the period for which the request continues to get retransmitted. This is used by P-CSCF/A-BG only when it sending message toward the UE. This timer is applicable both for reliable and unreliable transport. `sec` must be an integer from 0 to 2147483646.
  
  Default: 16 seconds (recommended minimum).

- **3gpp-t4 sec**: This timer is used to control the period for which the final response to non-invite transaction should be buffered. The buffered response for the retransmitted non-invite request should be sent within that interval. This timer is applicable only for unreliable transport. `sec` must be an integer from 0 to 2147483646.
  
  Default: 17 seconds (recommended minimum).

- **c sec**: This timer is used for an INVITE transaction; if the response is a provisional response with status codes 101 to 199 inclusive (anything but 100), the proxy must reset timer C for that client Transaction. The timer may be reset to a different value, but this value must be greater than 3 minutes (180 seconds). When timer C in S-CSCF fires first, S-CSCF will send CANCEL request to Terminating P-CSCF and Terminating P-CSCF will send CANCEL request to UAS. `sec` must be an integer from 180 to 2147483646.
  
  Default: 180 seconds

- **d sec**: This timer is used to control the retransmission of 200OK to INVITE after ACK is sent. The ACK transaction will be cleared after this interval. This timer is applicable only for unreliable transport. `sec` must be an integer from 0 to 2147483646.
  
  Default: 64*T1 (32 seconds, recommended minimum)

- **idle-tcp-connection msec**: This timer is used for closing idle TCP connections. If there is not activity in the TCP connection for the configuration duration, then the connection will be closed. `msec` must be an integer from 1000 (recommended minimum) to 4294967294.
  
  Default: 42000 milliseconds.

- **cleanup-timer msec**: This timer is used to control how often to check for idle TCP connections. `msec` must be an integer from 2000 to 2147483646.
CSCF Service Configuration Mode Commands


• **invite-expiry** *sec:* This timer is used by SIP while acting as UA Role and no final response is received for the INVITE request sent. This timer is applicable for both reliable and unreliable transport. *sec* must be an integer from 0 to 2147483646.
  
  Default: 100 seconds (recommended minimum).

• **t1** *msec:* Specifies the time interval (in microseconds) between each retransmission. The interval doubles after each retransmission, for example: T1, 2T1, 4T2, etc. This timer is applicable only for unreliable transport. *msec* must be an integer from 0 to 2147483646.
  
  Default: 500 milliseconds (recommended minimum).

• **t2** *sec:* This timer is used to control the period for which the request keeps getting retransmitted. This timer is applicable both for reliable and unreliable transport. *sec* must be an integer from 0 to 2147483646. The recommended minimum value for this parameter is 4 seconds.
  
  Default: 64*T1 (32 seconds)

• **t4** *sec:* This timer is used to control the period for which the final response to non-invite transaction should be buffered so as to send the buffered response for the retransmitted non-invite request within that interval. This timer is applicable only for unreliable transport. *sec* must be an integer from 0 to 2147483646.
  
  Default: 5 seconds (recommended minimum).

**Usage**

Use this command to configure SIP Stack timers and CSCF service specific timers.

**Example**

The following command sets the SIP d timer to 64 seconds:

```
timeout sip d 64
```
transport-switching

Sets the message size that triggers a transport protocol switch.

**Product**
SCM

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration

```
configure > context context_name > cscf service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-service)#
```

**Syntax**

```
transport-switching policy protocol tcp trigger msg-size size
```

```
default transport-switching policy protocol tcp trigger msg-size size
```

```
default
```

Returns the size of the SIP message beyond which transport changes to TCP to 1300 bytes.

```
policy protocol tcp trigger msg-size size
```

Default: 1300

Specifies the size of the SIP message beyond which transport changes to TCP.

`size` can be configured to any integer value between 1300 and 65535.

**Usage**

Use this command to configure the size of the SIP message beyond which transport changes to TCP.

**Example**

Switch to TCP transport protocol when the SIP message size is 4000 bytes or more:

```
transport-switching policy protocol tcp trigger msg-size 4000
```
trusted-domain-entity

Adds trusted network nodes (or entities) to a table used by this service to identify those nodes that can be trusted with subscriber information.

**Product**
SCM (S-CSCF)

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration

```
configure > context context_name > cscf service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-service)#
```

**Syntax**

```
trusted-domain-entity address [ foreign-network ] [ private-network ]
```

```
no trusted-domain-entity address
```

no

Removes an entry from this service’s trusted domain table.

```
address
```

Specifies the IP address of the network node identified as a trusted entity by this service. `address` must be either an IP address or a domain name. IP addresses must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6. Domain names must be entered using from 1 to 80 alpha and/or numeric characters.

```
foreign-network
```

Entity belongs to Foreign Network.

```
private-network
```

Entity belongs to Private Network.

**Usage**

Use this command to identify to the service the network entities that can be trusted with subscriber information by this service.

**Important:** This command can be entered multiple times to identify multiple trusted network entities. In StarOS v12.x and earlier, a maximum of 50 entries can be configured per CSCF service. In StarOS v14.0 and later, a maximum of 256 entries can be configured per CSCF service.

**Example**
The following command adds a network node with an IP address of 1.2.3.4 to this service’s trusted domain table:

```
trusted-domain-entity 1.2.3.4
```
Chapter 95
CSCF Serving-CSCF Configuration Mode Commands

The Serving-CSCF Configuration Mode is used to set various commands supporting the role of the CSCF service as a Serving CSCF.

Mode

Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Serving-CSCF Configuration
configure > context context_name > cscf service service_name > serving-cscf

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-cscf-service-serving-cscf)#

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
3gpp

Enables/disables functionality related to 3GPP Release 8 support. This command is disabled by default.

Product
SCM (S-CSCF)

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Serving-CSCF Configuration
configure > context context_name > cscf service service_name > serving-cscf

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-cscf-service-serving-cscf)#

Syntax

3gpp Rel8 Cx { alias-indication | dynamic-password-change | ims-restoration | num-auth-vectors value }

[ default | no ] 3gpp Rel8 Cx { alias-indication | dynamic-password-change | ims-restoration | num-auth-vectors }

default | no
Disables specified 3GPP Release 8 support feature.

Rel8 Cx
Specifies functionality related to 3GPP Release 8 support.

alias-indication
Enables alias indication functionality, a collaborative information exchange between the S-CSCF and HSS. Use this command to display alias information from the HSS. If both the HSS and the S-CSCF support this feature, Alias Group IDs will be displayed in the output of the show subscribers cscf-only full command.

dynamic-password-change
Enables dynamic password change support on the S-CSCF service, as per 3GPP 33.203 release 8 version 8.8.0.

ims-restoration
Enables IMS restoration procedures on the S-CSCF service. Use this command to enable IMS REGISTER and INVITE restoration procedures defined in 3GPP TS 23.820.

num-auth-vectors value
Enables configurable value for SIP-Number-Auth-Items in MAR.
value must be an integer from 1 to 3. Default is 1.
SCSCF can retrieve multiple authentication vectors from HSS by setting SIP-Number-Auth-Items to an appropriate value. Previously, S-CSCF always set this value to “1”. Using higher values helps to reduce MAR-MAA transactions.

Usage
Use this command to configure the S-CSCF to support 3GPP Release 8 functionality.

Example
The following command enables 3GPP Release 8 alias indication functionality on this service:

```bash
3gpp Rel8 Cx alias-indication
```

The following command disables 3GPP Release 8 dynamic password change support on this service:

```bash
no 3gpp Rel8 Cx dynamic-password-change
```
allow rfc3261-ua-interworking

Enables the function to allow IMS interworking with RFC3261 SIP User Agents.

Product
SCM (S-CSCF)

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Serving-CSCF Configuration
configure > context context_name > cscf service service_name > serving-cscf

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-cscf-service-serving-cscf)#

Syntax

[ no ] allow rfc3261-ua-interworking

no

Disables the interworking capability.

Usage

Use this command to enable the S-CSCF to allow IMS interworking with RFC3261 SIP User Agents.
as-call invite-request-uri update

Enabling this command causes request-URIs in INVITE messages to be updated with the result of the translation before being passed to an Application Server (AS). This command is disabled by default.

Product
SCM (S-CSCF, SIP Proxy)

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Serving-CSCF Configuration
configure > context context_name > cscf service service_name > serving-cscf

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-cscf-service-serving-cscf)#

Syntax

[ default | no ] as-call invite-request-uri update

<table>
<thead>
<tr>
<th>default</th>
<th>no</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>The translation result is ignored.</td>
<td></td>
</tr>
</tbody>
</table>

Usage

Use this command to update the request-URI in INVITE messages with the result of the translation before passing it to an AS.
authentication

Configures the authentication method used by the S-CSCF service.

**Product**
SCM (S-CSCF, SIP Proxy)

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Serving-CSCF Configuration

```
configure > context context_name > csf service service_name > serving-cscf
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-service-serving-cscf)#
```

**Syntax**

```
authentication { aka-v1 value | allow-auth-rsp-failure re-register | allow-hss-failure re-register | allow-noauth [ invite | re-register| register ] | allow-noipauth [ invite | re-register| register ] | allow-skip-sar re-register | allow-unsecure | aor-auth | custom-md5 value | md5 value }
```

```
no authentication { aka-v1 | allow-auth-rsp-failure re-register | allow-hss-failure re-register | allow-noauth [ invite | re-register| register ] | allow-noipauth [ invite | re-register| register ] | allow-skip-sar re-register | allow-unsecure | aor-auth | custom-md5 | md5 }
```

```
no
```

Disables the specified authentication method for the S-CSCF service.

- **aka-v1 value**
  Specifies that AKA-v1 algorithm is used as the authentication type when accessing the CSCF service. The value specifies a preference - the lower the value, the higher the preference. The value must be an integer from 1 to 1000.

- **Important:** In order to change a priority level, you must remove the original value and configure a new one.

- **allow-auth-rsp-failure re-register**
  Specifies that S-CSCF will not validate authorization received from UE for challenge re-register. If enabled, S-CSCF will send SAR without validating authentication; after receiving SAA, it will send 200 OK for register.

- **allow-hss-failure re-register**
  Specifies that S-CSCF should send 200 OK for re-register in case of HSS failure. When S-CSCF receives register, it sends MAR/SAR to HSS to authenticate the user when authentication is enabled and to get the subscriber profile. When S-CSCF fails to receive response MAA/SAA from HSS, it
sends 500 error response to UE. When allow-hss-failure is enabled, S-CSCF sends 200 OK for register instead of 500 response.

```plaintext
allow-noauth [ invite | re-register| register ]
```

Specify that access to the S-CSCF service is allowed if authentication fails.

- `invite`: Specifies that access to the S-CSCF service is allowed if authentication fails on INVITE requests only.
- `re-register`: Specifies that access to the S-CSCF service is allowed if authentication fails on RE-REGISTER requests when the request is integrity-protected only.
- `registration`: Specifies that access to the S-CSCF service is allowed if authentication fails on REGISTER requests only.

```plaintext
allow-noipauth [ invite | re-register| register ]
```

Specify that access to the S-CSCF service is allowed if early IMS-based IP authentication fails.

- `invite`: Specifies that access to the S-CSCF service is allowed if early IMS-based IP authentication fails on INVITE requests only.
- `re-register`: Specifies that access to the S-CSCF service is allowed if authentication fails on RE-REGISTER requests when the request is integrity-protected only.
- `registration`: Specifies that access to the S-CSCF service is allowed if early IMS-based IP authentication fails on REGISTER requests only.

```plaintext
allow-skip-sar re-register
```

Specify that S-CSCF should skip SAR to HSS for re-register.

When S-CSCF receives re-register/challenge for re-register, it sends SAR to HSS to get subscriber profile. To avoid overloading HSS, enabling allow-skip-sar allows S-CSCF to skip SAR for re-register.

```plaintext
allow-unsecure
```

Specify that un-secure access is allowed to the S-CSCF service.

```plaintext
aor-auth
```

Specify that authentication is based on the AoR when accessing the S-CSCF service.

```plaintext
custom-md5 value
```

Specify that custom algorithm HTTP-Digest-MD5 is used as the authentication type for accessing the S-CSCF service. `value` specifies a preference - the lower the value, the higher the preference. `value` must be an integer from 1 to 1000.

**Important:** In order to change a priority level, you must remove the original value and configure a new one.

```plaintext
md5 value
```

Specify that the MD5 algorithm is used as the authentication type for accessing the S-CSCF service. `value` specifies a preference - the lower the value, the higher the preference. `value` must be an integer from 1 to 1000.

**Important:** In order to change a priority level, you must remove the original value and configure a new one.
Usage

Use this command to configure the authentication method used by the S-CSCF service.

**Important:** The S-CSCF supports multiple authorization schemes, but this requires disabling all authorization configured in the S-CSCF service so that it will send “Unknown” in the Sip-Authorization-Scheme AVP. This allows the HSS to dictate authorization. The following commands disable all authorization configured in the S-CSCF service to allow HSS to control authorization:

```
authentication allow-noipauth
allow rfc3261-ua-interworking
no authentication aka-v1
no authentication md5
```

Example

The following command configures the authentication method used by the S-CSCF service to MD5 with a preference of 3:

```
authentication md5 3
```
bgcf-proxy

Enables SIP BGCF proxy for the service.

**Product**
SCM (S-CSCF)

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Serving-CSCF Configuration

```
configure > context context_name > cscf service service_name > serving-cscf
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-service-serving-cscf)#
```

**Syntax**

```
bgcf-proxy [ port value | transport { tcp | udp } port value ] ]
[ default | no ] bgcf-proxy
```

- **default | no**
  Disables SIP BGCF proxy for the service.

- **port value**
  Configures port value for SIP BGCF proxy.
  `value` must be an integer from 1 to 65534.

- **transport**
  Enables the specific transport protocol for BGCF proxy.
  - **tcp**: Enables TCP transport protocol for BGCF proxy.
  - **udp**: Enables UDP transport protocol for BGCF proxy.

**Usage**

Use this command to enable or disable SIP BGCF proxy for the service.

**Example**

The following command enables a SIP BGCF proxy on port 561 for this service:

```
bgcf-proxy port 561
```

The following command disables SIP BGCF proxy for this service:

```
no bgcf-proxy
```
diversion-info

Enabling this command prompts the service to add a diversion header (draft-levy-sip-diversion-08) when the call is diverted to a different endpoint due to a call feature. By default, diversion-info is disabled.

**Product**
SCM (S-CSCF, SIP Proxy)

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Serving-CSCF Configuration

`configure > context context_name > cscf service service_name > serving-cscf`

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-cscf-service-serving-cscf)#`

**Syntax**

```
[ default | no ] diversion-info
```

**Usage**

Use this command to enable the service to add a diversion header to call setup packets when calls are diverted due to the application of call features.
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
exit
```

**Usage**

Use this command to return to the parent configuration mode.
forking

Controls the default-request forking-type in S-CSCF.

Product
SCM (S-CSCF)

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Serving-CSCF Configuration

configure > context context_name > cscf service service_name > serving-cscf

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-cscf-service-serving-cscf)#

Syntax

forking { parallel | serial }
[ default | no ] forking

default
Perform parallel forking of request.

no
Do not perform any forking of request.

parallel | serial
Defines the fork type for request forking.

*parallel: Perform parallel forking of request.
*serial: Perform serial forking of request.

Usage
Use this command to control the default-request forking-type in S-CSCF. This configuration will be effective in the absence of “Request-Disposition” header in the message.

Example
The following command enables serial forking of request:

forking serial

The following command disables any forking of request:

no forking
interrogating-cscf-role

Enables the function to also perform as an Interrogating-CSCF.

Product
SCM (S-CSCF)

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Serving-CSCF Configuration

Syntax

[ no ] interrogating-cscf-role

no

Disables the Interrogating-CSCF role in this function.

Usage
Use this command to enable the S-CSCF to also perform as an Interrogating-CSCF.
**lir-failure**

This command allows you to define routes towards the target server for LIR failure case.

**Product**
SCM (S-CSCF)

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Serving-CSCF Configuration

```
configure > context context_name > cscf service service_name > serving-cscf
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-service-serving-cscf)#
```

**Syntax**

```
lir-failure route-list route_list_name
```

```
no lir-failure route-list
```

Disables routing of register messages for this S-CSCF.

**Usage**

Use this command to route register messages based on the route table if LIR-LIA fails during HSS interaction.
local-call-features

Enables/disables local call features. This command is disabled by default.

**Product**  
SCM (S-CSCF)

**Privilege**  
Administrator

**Mode**  
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Serving-CSCF Configuration

configure > context context_name > cscf service service_name > serving-cscf

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-service-serving-cscf)#
```

**Syntax**

```
[ default | no ] local-call-features
```

- **default** | **no**
  Disables local call features for this S-CSCF.

**Usage**

Use this command to enable local call features.
network-id

Configures the Network Identifier.

**Product**
SCM (S-CSCF)

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Serving-CSCF Configuration

`configure > context context_name > cscf service service_name > serving-cscf`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-service-serving-cscf)#
```

**Syntax**

```
network-id id

no network-id
```

- `no`
  Removes the configured Network Identifier of the entity.

- `id`
  The Network Identifier of the entity.
  `id` must be from 1 to 79 alpha and/or numeric characters in length.

**Usage**
The Network Identifier is used to compare with the P-Visited-Network-ID header received from P-CSCF to decide home or roaming subscriber at S-CSCF service.

**Example**
Sets the Network Identifier to `pcscf01.company.com`:

```
network-id pcscf01.company.com
```
npdb-client

Creates an NPDB (Number Portability Data Base) client under CSCF and enters the CSCF NPDB Client Configuration Mode.

Product
SCM (S-CSCF)

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Serving-CSCF Configuration
configure > context context_name > cscf service service_name > serving-cscf

Entering the above command sequence results in the following prompt:
[context_name]host_name(config-cscf-service-serving-cscf)#

Syntax

npdb-client client_name [ -noconfirm ]

no npdb-client

- no

Deletes NPDB client under CSCF.

- client_name

Specifies the name of the NPDB client.
client_name must be from 1 to 79 alpha and/or numeric characters.

- -noconfirm

Indicates that the command is to execute without any additional prompt and confirmation from the user.

Usage

Use this command to enable the NPDB client feature and enter the NPDB Client Configuration Mode. Entering this command results in the following prompt:
[context_name]host_name(config-npdb-client)#

NPDB Client Configuration Mode commands are defined in the CSCF NPDB Client Configuration Mode Commands chapter in this guide.

Example

The following command creates an NPDB client named npdb1 and enters NPDB Client Configuration Mode:

npdb-client npdb1
policy

Configures the policy for Served User Routing in this S-CSCF service.

Product
SCM (S-CSCF)

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Serving-CSCF Configuration
configure > context context_name > cscf service service_name > serving-cscf

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-cscf-service-serving-cscf)#

Syntax

[ default | no ] policy allow p-served-user-routing

<table>
<thead>
<tr>
<th>default</th>
<th>no</th>
</tr>
</thead>
</table>
| Disables Served User Routing functionality for this S-CSCF.

<table>
<thead>
<tr>
<th>allow p-served-user-routing</th>
</tr>
</thead>
</table>
| Enables Served User Routing functionality for this S-CSCF.

Usage

Use this command to enable/disable the policy for Served User Routing.

Example

The following command enables Served User Routing on this service:

```
policy allow p-served-user-routing
```

The following command disables Served User Routing on this service:

```
no policy allow p-served-user-routing
```
registration lifetime

Configures a registration lifetime for all subscribers to the service.

Product
SCM (S-CSCF, SIP Proxy)

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Serving-CSCF Configuration
configure > context context_name > cscf service service_name > serving-cscf

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-cscf-service-serving-cscf)##

Syntax

registration lifetime { default sec | implicit sec | max sec | min sec }

default registration lifetime

default

Returns the command to the default settings.

default sec | implicit sec | max sec | min sec

default sec: Specifies the default amount of time that a registration can exist on the system. sec must be an integer from 60 to max sec -1.
Default: 3600

**Important:** default sec must be < or = to max sec and > or = to min sec.

implicit sec: Specifies the implicit amount of time that a registration can exist on the system. sec must be an integer from 60 to 1209600.
Default: 0

max sec: Specifies the maximum amount of time that a registration can exist on the system. sec must be an integer from 60 to 1209600.
Default: 86400

**Important:** max sec must be > or = to min sec.

min sec: Specifies the minimum amount of time that a registration can exist on the system. sec must be an integer from 60 to max sec -1.
Default: 60

**Important:** min sec must be < or = to max sec.
Usage

Use this command to control the amount of time registrations are allowed to exist on this service. The system responds to registrations in the following manner:
If implicit-timer is configured (>0), and if UE expires time < min expires time, respond with 200 OK with Expires-header set to configured implicit-expires time.
If implicit timer is not configured (=0), the service will respond with a 423 Interval Too Small message.
Using default values:
- If a registration with an expiration value lower than the service’s minimum (60) is received, the service will respond with a 423 Interval Too Small message.
- If a registration with an expiration value higher than the service’s maximum (2147483646) is received, the service will automatically reduce the expiration value to the default value.
- If a registration is received missing the “Expires” value, or the value is malformed, the service will automatically respond with 3761 in the 200 OK message.

Example

The following command configures the maximum registration lifetime to 43200 (12 hours):

```
registration lifetime max 43200
```
reliable-prov-resp

Enables/disables the reliability of provisional responses feature.

**Product**
SCM (S-CSCF, SIP Proxy)

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Serving-CSCF Configuration

```
configure > context context_name > cscf service service_name > serving-cscf
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-service-serving-cscf)#
```

**Syntax**

```
reliable-prov-resp { mandatory | optional }
```

**no reliable-prov-resp**

```
no
```

Disables the reliability of provisional responses feature.

```
mandatory | optional
```

**mandatory**: Both inbound and outbound will request reliability.

**optional** (default): Reliability is imposed by inbound side. Only if inbound call requests reliability will outbound also request reliability.

**Usage**

Use this command to enable/disable the reliability of provisional responses feature.

**Example**

The following command sets the reliability of provisional responses feature to mandatory:

```
reliable-prov-resp mandatory
```
server-name

Enables/disables filling the server name AVP in MAR and SAR for Cx interface with configured server name. This command is disabled by default.

**Important:** The `server-name` command has been moved to **CSCF Service Configuration Mode** in StarOS release 14.0 and later.

**Product**
SCM (S-CSCF)

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Serving-CSCF Configuration

`configure > context context_name > csf service service_name > serving-cscf`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-service-serving-cscf)#
```

**Syntax**

```
server-name server_name

no server-name
```

**Usage**

S-CSCF uses configured cscf-hostname or bind IP address to fill the server name AVP in MAR and SAR for Cx interface. This is the default CSCF behavior.

```
server_name
```

Configures the name that will be used to fill the server name AVP in MAR and SAR for Cx interface. `name` must be from 1 to 63 alpha and/or numeric characters.

**Example**

Use this command to enable/disable filling the server name AVP in MAR and SAR for Cx interface with configured server name.

The following command configures the CSCF server name as `stp-c-scscfl.cisco.co.kr`:

```
server-name stp-c-scscfl.cisco.co.kr
```
**sifc**

Enables Shared Initial Filter Criteria (SiFC) functionality. This command is disabled by default.

**Product**
SCM (S-CSCF, SIP Proxy)

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Serving-CSCF Configuration

`configure > context context_name > cscf service service_name > serving-cscf`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-service-serving-cscf)#
```

**Syntax**

```
[ default | no ] sifc
```

- **default**
  - Disables shared iFC functionality for this S-CSCF.

**Usage**

Use this command to configure the S-CSCF to share iFC functionality.

> **Important:** 48 SiFC IDs are supported per subscriber.

If both the HSS and the S-CSCF support this feature, subsets of iFC may be shared by several service profiles. The HSS downloads the unique identifiers of the shared iFC sets to the S-CSCF. The S-CSCF uses a locally administered database to map the downloaded identifiers onto the shared iFC sets. If the S-CSCF does not support this feature, the HSS will not download identifiers of shared iFC sets.

> **Important:** When using this feature option, the network operator is responsible for keeping the local databases in the S-CSCFs and HSSs consistent.
**sip-header insert**

Enable SIP header insertion for the S-CSCF service. SIP header insertion is disabled by default.

**Product**
SCM (S-CSCF)

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Serving-CSCF Configuration

`configure > context context_name > cscf service service_name > serving-cscf`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-service-serving-cscf)#
```

**Syntax**

```
[ no ] sip-header insert { p-cust1-prid-info | p-user-database }
```

- **no**
  Disables specific SIP header insertion for the S-CSCF service.

- **p-cust1-prid-info**
  Inserts a custom header, P-LGUPlus-PRID-Info, which contains the private user id of the user sending the REGISTER request, to be added in the REGISTER message toward AS during third party registration.

- **p-user-database**
  Inserts PUD header in SIP (REGISTER) message and Invite from I-CSCF to S-CSCF.

**Usage**

Enabling this command allows header insertion in SIP (REGISTER) message.

**Example**

The following command disables insertion of custom header, P-LGUPlus-PRID-Info, in SIP (REGISTER) message:

```
no sip-header insert p-cust1-prid-info 5
```

The following command enables insertion of PUD header in SIP (REGISTER) message and Invite from I-CSCF to S-CSCF:

```
sip-header insert p-user-database 5
```
**sirp-request**

Configures SIP Request-related configuration in this S-CSCF service.

**Product**
SCM (S-CSCF, SIP Proxy)

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Serving-CSCF Configuration

```
configure > context context_name > csf service service_name > serving-cscf
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-service-serving-cscf)#
```

**Syntax**

```
sip-request re-route { max-attempts attempts | response-code code }  
default sip-request re-route max-attempts  
no sip-request re-route response-code code
```

---

**Important:** You may configure a maximum of five response code values per S-CSCF service.
Usage

Use this command to configure:
- list of Response codes that will be considered as re-routable responses to a call attempt.
- the maximum number of re-route attempts that a S-CSCF should allow for a given call before passing the negative response upstream.

Example

The following command configures the maximum number of re-route attempts to 5:

```bash
sip-request re-route max-attempts 5
```
tas

Configures the S-CSCF to perform Telephony Application Server (TAS) functions.

Product
SCM (S-CSCF, SIP Proxy)

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Serving-CSCF Configuration
configure > context context_name > cscf service service_name > serving-cscf

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-cscf-service-serving-cscf)#

Syntax

[ default | no ] tas

default | no

Disables the TAS feature for this S-CSCF.

Usage

Use this command to configure the S-CSCF to perform TAS functions.
tas-service

Identifies the name of the service configured on the system performing Telephony Application Server (TAS) functions.

Product
SCM (S-CSCF, SIP Proxy)

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Serving-CSCF Configuration
configure > context context_name > cscf service service_name > serving-cscf

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-cscf-service-serving-cscf)#

Syntax

tas-service name

no tas-service

no

Removes the TAS name from the S-CSCF configuration.

name

Specifies the name of the service configured on the system performing TAS functions.
name must be from 1 to 63 alpha and/or numeric characters and be an existing service.

Usage

Use this command to identify the name of the service configured on the system performing TAS functions

Example

The following command identifies the TAS service name as scscf3:

tas-service scscf3
user-authorization

Enables sending user-authorization to HSS. User-authorization is disabled by default.

Product
SCM (S-CSCF, SIP Proxy)

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Serving-CSCF Configuration
configure > context context_name > cscf service service_name > serving-cscf

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-cscf-service-serving-cscf)#

Syntax

[ default | no ] user-authorization

default | no

Disables sending user-authorization to HSS.

Usage

If this command is enabled, and I-CSCF role is enabled in S-CSCF, I-CSCF will send UAR/UAA diameter message to HSS.
Chapter 96
CSCF Session Template Configuration Mode Commands

The CSCF Session Template Configuration Mode is used to classify users and/or domains (AoRs) within the system.

**Mode**

Exec > Global Configuration > Context Configuration > CSCF Session Template Configuration

configure > context context_name > cscf session-template { default | name template_name }

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-session-template)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

`exit`

**Usage**

Use this command to return to the parent configuration mode.
inbound-cscf-acl

Configures the ACL to use for inbound sessions using this template.

**Product**
SCM

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Session Template Configuration

```bash
configure > context context_name > cscf session-template { default | name template_name }
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-session-template)##
```

**Syntax**

```
inbound-cscf-acl { default | name acl_name }

no inbound-cscf-acl name acl_name
```

**Usage**

Use this command to identify an ACL to use on inbound sessions using this template.

**Example**

The following command sets the inbound ACL for this template to an ACL named `acl_in22`:

```bash
inbound-cscf-acl name acl_in22
```
outbound-cscf-acl

Configures the ACL to use for outbound sessions using this template.

Product
SCM

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > CSCF Session Template Configuration

configure > context context_name > cscf session-template { default | name template_name }

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-cscf-session-template)#

Syntax

outbound-cscf-acl { default | name acl_name }

no outbound-cscf-acl name acl_name

default | name acl_name

default: Specifies that the default ACL should be used for outbound sessions using this template.
name acl_name: Specifies an existing ACL to use for outbound sessions using this template. acl_name must be the name of an existing ACL.

no outbound-cscf-acl name acl_name

Removes the ACL from this template.

Usage

Use this command to identify an ACL to use on outbound sessions using this template.

Example

The following command sets the outbound ACL for this template to an ACL named acl_out22:

    outbound-cscf-acl name acl_out22
policy-profile

Configures an AoR policy group to be used for sessions using this template.

Product
SCM

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > CSCF Session Template Configuration

configure > context context_name > cscf session-template { default | name template_name }

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-cscf-session-template)#

Syntax

policy-profile { default | name profile_name }

no policy-profile name profile_name

default | name profile_name

default: Specifies that the default policy group will be used for sessions using this template.

name profile_name: Specifies an existing policy group. profile_name must be an existing CSCF policy group.

no policy-profile name profile_name

Removes the policy group from the template.

Usage

Use this command to specify a policy group for the template.

Example

The following command specifies that a policy group called aor_grp1 will be used for sessions using this template:

    policy-profile name aor_grp1
route-list

Configures a route group to be used for sessions using this template.

**Product**
SCM

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Session Template Configuration
```
configure > context context_name > cscf session-template { default | name template_name }
```

Entering the above command sequence results in the following prompt:
```
[context_name]host_name(config-cscf-session-template)#
```

**Syntax**
```
route-list { default | name group_name }

no route-list name group_name
```

- **default | name group_name**
  - default: Specifies that the default route group will be used for sessions using this template.
  - name group_name: Specifies an existing route group. group_name must be an existing peer server group.

- **no route-list name group_name**
  Removes the route group from this template.

**Usage**
Use this command to specify a route group for the template.

**Example**
The following command specifies an accounting server group called route_grp2 that will be used for sessions using this template:
```
route-list name route_grp2
```
translation-list

Configures a translation list to be used for sessions using this template.

**Product**
SCM

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Session Template Configuration

```bash
configure > context context_name > cscf session-template { default | name template_name }
```

Entering the above command sequence results in the following prompt:

```
[context_name] host_name(config-cscf-session-template)#
```

**Syntax**

```bash
translation-list { default | name list_name }
no translation-list name list_name
```

- **default | name list_name**
  - default: Specifies that the default translation list will be used for sessions using this template.
  - name **list_name**: Specifies an existing translation list. **list_name** must be an existing translation list.

```bash
no translation-list name list_name
```

Removes the translation list from this template.

**Usage**
Use this command to specify a translation list for the template.

**Example**
The following command specifies a translation list called **trans_list6**:

```bash
translation-list name trans_list6
```
urn-service-list

Configures an URN service list to be used for sessions using this template.

Product
SCM

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > CSCF Session Template Configuration
configure > context context_name > cscf session-template { default | name template_name }

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-cscf-session-template)#

Syntax

\texttt{urn-service-list \{ default | name list_name \}}

\texttt{no urn-service-list name list_name}

\underline{default | name list_name}

default: Specifies that the default URN service list will be used for sessions using this template.
name list_name: Specifies an existing URN service list name. list_name must be from 1 to 79 alpha
and/or numeric characters and be an existing URN service list.

\underline{no urn-service-list name list_name}

Removes the service list from this template.

Usage

Use this command to specify a URN service list for this template. URN service lists are configured in the
URN Service List Configuration Mode.

Example

The following command specifies that a URN service list named \texttt{urn_list5} will be used for sessions using
this template:

\texttt{urn-service-list name urn_list5}
The CSCF Signalling Compression Configuration Mode is used to set memory allocation parameters in support of SIP signalling compression. More information regarding signalling compression refer to the IETF RFC 3320 “Signaling Compression (SigComp)”.

**Mode**

Exec > Global Configuration > Context Configuration > CSCF Service Configuration > SIP Proxy Configuration > Signaling Compression Configuration

```bash
configure > context context_name > cscf service service_name > rfc3261-proxy > sigcomp
```

-or-

Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration > Signaling Compression Configuration

```bash
configure > context context_name > cscf service service_name > proxy-cscf > sigcomp
```

Entering the above command sequences results in the following prompt:

```
[context_name]host_name(config-sigcomp)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
compression-mode

Configures the dynamic compression mode to be used while sending a SigComp message. Simple dynamic mode is the default.

Product
SCM

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > SIP Proxy Configuration > Signaling Compression Configuration

configure > context context_name > cscf service service_name > rfc3261-proxy > sigcomp

-or-

Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration > Signaling Compression Configuration

configure > context context_name > cscf service service_name > proxy-cscf > sigcomp

Entering the above command sequences results in the following prompt:

[context_name]host_name(config-sigcomp)#

Syntax

compression-mode { multiple-dynamic | simple-dynamic | static | update-dynamic }

default compression-mode

multiple-dynamic | simple-dynamic | static | update-dynamic

Default: simple-dynamic

multiple-dynamic: A maximum of four dynamic states will be created per compartment. The dynamic states are updated for each message by deleting the oldest dynamic state and creating the new one. The dynamic states will be updated in FIFO (First In, First Out) order.

simple-dynamic: Only one dynamic state will be created per compartment. The same state will be used for compression.

static: No dynamic states will be created. Only static dictionary will be used for compression.

update-dynamic: Only one dynamic state will be created per compartment, but the dynamic state will be updated for every new message.

default compression-mode

Returns the dynamic compression mode to simple dynamic.

Usage

Use this command to configure the dynamic compression mode to be used.

Example

The following command sets the compression mode to multiple dynamic:

    compression-mode multiple-dynamic
The following command completely disables the creation of dynamic states for compression:

    compression-mode static
decompression-memory-size

Sets the amount of memory available for decompressing one SigComp message. A portion of the allocated memory is used to buffer the message before it is decompressed. The memory is allocated for each SigComp message and is reclaimed once decompression is completed.

**Product**
SCM

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > SIP Proxy Configuration > Signaling Compression Configuration

configure > context context_name > cscf service service_name > rfc3261-proxy > sigcomp

-or-

Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration > Signaling Compression Configuration

configure > context context_name > cscf service service_name > proxy-cscf > sigcomp

Entering the above command sequences results in the following prompt:

```
[context_name] host_name (config-sigcomp) #
```

**Syntax**

```
decompression-memory-size { 128k | 16k | 32k | 64k | 8k }
```

**Usage**

Use this command to set the memory size used to decompress a single SigComp message.

**Example**

The following command sets the memory size for decompressing SigComp messages to 16k:

```
decompression-memory-size 16k
```
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
```plaintext
end
```

**Usage**
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**
Use this command to return to the parent configuration mode.
state-memory-size

Sets the memory allocated to a compartment for the creation of state. Compartments are application-specific groupings of messages that relate to a peer endpoint. The system allocates memory per compartment. The memory is reclaimed when the system determines that the compartment is no longer required.

Product
SCM

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > SIP Proxy Configuration > Signaling Compression Configuration

configure > context context_name > cscf service service_name > rfc3261-proxy > sigcomp

–or–

Exec > Global Configuration > Context Configuration > CSCF Service Configuration > Proxy-CSCF Configuration > Signaling Compression Configuration

configure > context context_name > cscf service service_name > proxy-cscf > sigcomp

Entering the above command sequences results in the following prompt:

[context_name]host_name(config-sigcomp)#

Syntax

state-memory-size { 4k | 8k }

default state-memory-size

4k | 8k

Default: 4k

Specifies the amount of memory to allocate to a compartment for the creation of state.

default

Returns the command to the default settings.

Usage
Use this command to specify a memory size allocated to message groupings for the creation of state.

Example

The following command sets the state memory size to 8k:

state-memory-size 8k
Chapter 98
CSCF SIP Proxy Configuration Mode Commands

The SIP Proxy Configuration Mode is used to set various commands supporting the role of the CSCF service as a RFC3261-compliant SIP proxy server.

Mode

Exec > Global Configuration > Context Configuration > CSCF Service Configuration > SIP Proxy Configuration

configure > context context_name > cscf service service_name > rfc3261-proxy

Entering the above command sequences results in the following prompt:

[context_name]host_name(config-cscf-service-rfc3261-proxy)#

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
as-call

Enabling this command causes request-URIs in INVITE messages to be updated with the result of the translation before being passed to an Application Server. This command is disabled by default.

Product
SCM (S-CSCF, SIP Proxy)

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > SIP Proxy Configuration
configure > context context_name > cscf service service_name > rfc3261-proxy

Entering the above command sequences results in the following prompt:

[context_name]host_name(config-cscf-service-rfc3261-proxy)#

Syntax

[ default | no ] as-call invite-request-uri update

default | no

The translation result is ignored.

Usage

Use this command to update the request-URI in INVITE messages with the result of the translation before passing it to an AS.
**authentication**

Configures the authentication method used by the CSCF service.

**Product**
SCM (S-CSCF, SIP Proxy)

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > SIP Proxy Configuration

```
configure > context context_name > cscf service service_name > rfc3261-proxy
```

Entering the above command sequences results in the following prompt:

```
[context_name]host_name(config-cscf-service/rfc3261-proxy)#
```

**Syntax**

```
authentication { aka-v1 value | allow-noauth [ invite | re-register| register ] | allow-noipauth [ invite | re-register| register ] | allow-unsecure | aor-auth | md5 value }

no authentication { aka-v1 | allow-noauth [ invite | re-register| register ] | allow-noipauth [ invite | re-register| register ] | allow-unsecure | aor-auth | md5 }
```

---

**no**

Disables the specified authentication method for the CSCF service.

**aka-v1 value**

Specifies that AKA-v1 algorithm is used as the authentication type when accessing the CSCF service.

`value` specifies a preference - the lower the value, the higher the preference. `value` must be an integer from 1 to 1000.

---

**Important:** In order to change a priority level, you must remove the original value and configure a new one.

**allow-noauth [ invite | re-register| register ]**

Specifies that access to the CSCF service is allowed if authentication fails.

`invite`: Specifies that access to the CSCF service is allowed if authentication fails on INVITE requests only.

`re-register`: Specifies that access to the CSCF service is allowed if authentication fails on RE-REGISTER requests when the request is integrity-protected only.

`registration`: Specifies that access to the CSCF service is allowed if authentication fails on REGISTER requests only.

**allow-noipauth [ invite | re-register| register ]**

Specifies that access to the CSCF service is allowed if early IMS-based IP authentication fails.

`invite`: Specifies that access to the CSCF service is allowed if early IMS-based IP authentication fails on INVITE requests only.
**re-register**: Specifies that access to the CSCF service is allowed if authentication fails on RE-REGISTER requests when the request is integrity-protected only.

**registration**: Specifies that access to the CSCF service is allowed if early IMS-based IP authentication fails on REGISTER requests only.

---

**allow-unsecure**

Specifies that un-secure access is allowed to the CSCF service.

---

**aor-auth**

Specifies that authentication is based on the AoR when accessing the CSCF service.

---

**md5 value**

Specifies that the MD5 algorithm is used as the authentication type for accessing the CSCF service. `value` specifies a preference - the lower the value, the higher the preference. `value` must be an integer from 1 to 1000.

---

**Important**: In order to change a priority level, you must remove the original value and configure a new one.

---

**Usage**

Use this command to configure the authentication method used by the CSCF service.

---

**Important**: The S-CSCF supports multiple authorization schemes, but this requires disabling all authorization configured in the S-CSCF service so that it will send “Unknown” in the Sip-Authorization-Scheme AVP. This allows the HSS to dictate authorization. The following commands disable all authorization configured in the S-CSCF service to allow HSS to control authorization:

- `authentication allow-noipauth`
- `allow rfc3261-ua-interworking`
- `no authentication aka-v1`
- `no authentication md5`

---

**Example**

The following command configures the authentication method used by the CSCF service to MD5 with a preference of 3:

```
authentication md5 3
```
**diversion-info**

Enabling this command prompts the service to add a diversion header (draft-levy-sip-diversion-08) when the call is diverted to a different endpoint due to a call feature. By default diversion-info is disabled.

**Product**
SCM (S-CSCF, SIP Proxy)

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > SIP Proxy Configuration

```
configure > context context_name > cscf service service_name > rfc3261-proxy
```

Entering the above command sequences results in the following prompt:

```
[context_name]host_name(config-cscf-service-rfc3261-proxy)#
```

**Syntax**

```
[ default | no ] diversion-info
```

- **default | no**
  
  The service will not add a diversion header.

**Usage**

Use this command to enable the service to add a diversion header to call setup packets when calls are diverted due to the application of call features.
emergency

Configures the function to allow or disallow the emergency-session or emergency-registration of a particular type.

Product
SCM (P-CSCF, A-BG, SIP Proxy)

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > SIP Proxy Configuration

configure > context context_name > cscf service service_name > rfc3261-proxy

Entering the above command sequences results in the following prompt:

[context_name]host_name(config-cscf-service-rfc3261-proxy)#

Syntax

[ default | no ] emergency { registration [ visited-ue ] | session [ 3gpp-ims-xml-body | anonymous | non-emergency-registered | sdp-cs-media | visited-ue ] }

default
Specifies that the emergency-session or emergency-registration of a particular type can be allowed.

no
Disallows the emergency-session or emergency-registration of a particular type.

registration [ visited-ue ]

Allow emergency-registration. By default, it's allowed.

visited-ue: Allow emergency-registration from a visited UE. By default, it's allowed.

session [ 3gpp-ims-xml-body | anonymous | non-emergency-registered | sdp-cs-media | visited-ue ]

Specifies the type of emergency-session to be allowed or disallowed. By default, all are allowed.

3gpp-ims-xml-body: Allow 3GPP IM CN XML body to be added in 380 response messages.
anonymous: Allow anonymous subscribers (unregistered UEs) to initiate emergency sessions.
non-emergency-registered: Allow non-emergency registered subscribers to initiate emergency sessions.
sdp-cs-media: Allow emergency calls with SDP CS Media.
visited-ue: Allow emergency calls from visited UE.

Usage

Use this command to configure the function to allow or disallow the emergency-session or emergency-registration of a particular type.

Example

The following command configures the function to allow non-emergency registered subscribers to initiate emergency sessions:
emergency session non-emergency-registered
**end**

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
```
end
```

**Usage**
Use this command to return to the Exec mode.
**exit**

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**
Use this command to return to the parent configuration mode.
**registration**

Configures a registration lifetime for all subscribers to the service.

**Product**
SCM (S-CSCF, SIP Proxy)

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > SIP Proxy Configuration

```
configure > context context_name > cscf service service_name > rfc3261-proxy
```

Entering the above command sequences results in the following prompt:

```
[context_name]host_name(config-cscf-service-rfc3261-proxy)#
```

**Syntax**

```
registration lifetime { default sec | max sec | min sec }
```

**Usage**

Use this command to control the amount of time registrations are allowed to exist on this service. The system responds to registrations in the following manner:

Using default values:
- If a registration with an expiration value lower than the service’s minimum (60) is received, the service will respond with a 423 Interval Too Small message.
- If a registration with an expiration value higher than the service’s maximum (2147483646) is received, the service will automatically reduce the expiration value to the default value.
- If a registration is received missing the “Expires” value, or the value is malformed, the service will automatically respond with 3761 in the 200OK message.

**Example**

The following command configures the maximum registration lifetime to 43200 (12 hours):
registration lifetime max 43200
reliable-prov-resp

Enables/disables the reliability of provisional responses feature.

Product
SCM (S-CSCF, SIP Proxy)

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > SIP Proxy Configuration

configure > context context_name > cscf service service_name > rfc3261-proxy

Entering the above command sequences results in the following prompt:

[context_name]host_name(config-cscf-service-rfc3261-proxy)#

Syntax

reliable-prov-resp { mandatory | optional }

no reliable-prov-resp

no

Disables the reliability of provisional responses feature.

mandatory | optional

mandatory: Both inbound and outbound will request reliability.
optional (default): Reliability is imposed by inbound side. Only if inbound call requests reliability will outbound also request reliability.

Usage

Use this command to enable/disable the reliability of provisional responses feature.

Example

The following command sets the reliability of provisional responses feature to mandatory:

    reliable-prov-resp mandatory

The following command disables the reliability of provisional responses feature:

    no reliable-prov-resp
sifc

Enables Shared Initial Filter Criteria (SiFC) functionality. This command is disabled by default.

Product
SCM (S-CSCF, SIP Proxy)

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > SIP Proxy Configuration

configure > context context_name > cscf service service_name > rfc3261-proxy

Entering the above command sequences results in the following prompt:

[context_name]host_name(config-cscf-service-rfc3261-proxy)#

Syntax

[ default | no ] sifc

  default | no

Disables shared iFC functionality for this SIP Proxy.

Usage

Use this command to configure the SIP Proxy to share iFC functionality.
If both the HSS and the SIP Proxy support this feature, subsets of iFC may be shared by several service profiles. The HSS downloads the unique identifiers of the shared iFC sets to the SIP Proxy. The SIP Proxy uses a locally administered database to map the downloaded identifiers onto the shared iFC sets.
If the SIP Proxy does not support this feature, the HSS will not download identifiers of shared iFC sets.

Important: When using this feature option, the network operator is responsible for keeping the local databases in the S-CSCFs and HSSs consistent.
sigcomp

Enables signaling compression for the SIP Proxy service and enters the Signaling Compression Configuration Mode.

Product
SCM (S-CSCF, SIP Proxy)

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > SIP Proxy Configuration
configure > context context_name > cscf service service_name > rfc3261-proxy

Entering the above command sequences results in the following prompt:

[context_name]hostname(config-cscf-service-rfc3261-proxy)#

Syntax

[ no ] sigcomp

no

Disables signaling compression for the CSCF service.

Usage

Use this command to enable signaling compression for the SIP Proxy service and enter the CSCF Signaling Compression Configuration Mode.

Entering this command results in the following prompt:

[context_name]hostname(config-sigcomp)#

Signaling Compression Configuration Mode commands are defined in the CSCF Signaling Compression Configuration Mode Commands chapter in this guide.
tas

Configures the SIP Proxy to perform Telephony Application Server (TAS) functions.

Product
SCM (S-CSCF, SIP Proxy)

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > SIP Proxy Configuration

configure > context context_name > cscf service service_name > rfc3261-proxy

Entering the above command sequences results in the following prompt:

[context_name]host_name(config-cscf-service-rfc3261-proxy)#

Syntax

[ default | no ] tas

---

default | no

Disables the TAS feature for this SIP Proxy.

---

Usage

Use this command to configure the SIP Proxy to perform TAS functions.
tas-service

Identifies the name of the service configured on the system performing Telephony Application Server (TAS) functions.

Product
SCM (S-CSCF, SIP Proxy)

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > CSCF Service Configuration > SIP Proxy Configuration

configure > context context_name > cscf service service_name > rfc3261-proxy

Entering the above command sequences results in the following prompt:

[context_name]host_name(config-cscf-service-rfc3261-proxy)#

Syntax

tas-service name

[ default | no ] tas-service

default | no
Removes the TAS name from the SIP Proxy configuration.

name
Specifies the name of the service configured on the system performing TAS functions. name must be from 1 to 63 alpha and/or numeric characters and be an existing service.

Usage
Use this command to identify the name of the service configured on the system performing TAS functions. The ims-sh-service commands are defined in the Context Configuration Mode Commands chapter in this guide.

Example
The following command identifies the TAS service name as scscf3:

tas-service scscf3
Chapter 99
CSCF Subdomain-route List Configuration Mode Commands

The CSCF Subdomain-route List Configuration Mode is used to configure the subdomain-routes for the I-CSCF. These subdomain-routes are used to send messages over the Ma-interface (I-CSCF interface toward AS).

Mode

Exec > Global Configuration > Context Configuration > CSCF Subdomain-routes List Configuration

```
configure > context context_name > cscf subdomain-routes
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-subdomain-route)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
after

Places the subdomain-route at the bottom or end of the subdomain-routes list. Use this command in conjunction with the `route` command.

**Product**
SCM (I-CSCF)

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Subdomain-routes List Configuration

```bash
configure > context context_name > cscf subdomain-routes
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-subdomain-route)#
```

**Syntax**

```
after
```

**Usage**

Add this command before the `route` command to place the route at the end of the subdomain-routes list.
before

Places the subdomain-route at the beginning or top of the subdomain-routes list. Use this command in conjunction with the `route` command.

**Product**
SCM (I-CSCF)

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Subdomain-routes List Configuration

```
configure > context context_name > cscf subdomain-routes
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-subdomain-route)#
```

**Syntax**

```
before
```

**Usage**

Add this command before the `route` command to place the route at the beginning of the subdomain-routes list.
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**

Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

`exit`

**Usage**

Use this command to return to the parent configuration mode.
route

Creates a route entry to be used in the subdomain-routes list for the I-CSCF.

Product
SCM (I-CSCF)

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > CSCF Subdomain-routes List Configuration

configure > context context_name > csf subdomain-routes

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-csf-subdomain-route)#

Syntax

[ no ] route peer-servers name [ log ] base-criteria destination aor aor

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Removes specified route entry.</td>
</tr>
<tr>
<td>peer-servers</td>
<td>Specifies the name of a peer server group.</td>
</tr>
<tr>
<td>name</td>
<td>name must be an existing peer server group from 1 to 79 alpha and/or numeric characters in length.</td>
</tr>
<tr>
<td>log</td>
<td>Enables logging for CSCF sessions meeting the criteria specified. The logs can be viewed by executing the logging filter active facility csf command in the Exec mode.</td>
</tr>
<tr>
<td>base-criteria</td>
<td>Filters routes based on the destination AoR.</td>
</tr>
<tr>
<td>destination</td>
<td>aor must be an existing AoR from 1 to 79 alpha and/or numeric characters in length.</td>
</tr>
<tr>
<td>aor</td>
<td>aor</td>
</tr>
</tbody>
</table>

Important: AoR regular expressions are supported. Refer to the SCM Engineering Rules Appendix in the Session Control Manager Administration Guide for more information about regular expressions.

Usage

Use this command to create and order routes in the subdomain-routes list for the I-CSCF. I-CSCF, upon receiving the terminating request, checks the subdomain-route list for matches. If a match is found, the routing will happen based on it. Otherwise, I-CSCF performs a User Location Query (Location-Information-Request) before proceeding.

Example
The following command creates a route for the subdomain-routes list to peer server group `ps5` with a destination AoR of `$.@abc123.com`:

```bash
route peer-servers ps5 base-criteria destination aor $.@abc123.com
```
Chapter 100
CSCF Translation Configuration Mode Commands

The CSCF Translation Configuration Mode is used to configure session re-addressing within the system.

Mode

Exec > Global Configuration > Context Configuration > CSCF Translation Configuration

configure > context context_name > cscf translation name list_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-cscf-translation)#

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
after

Places the CSCF translation entry at the bottom or end of the translation list. Use this command in conjunction with the `uri-readdress` command.

Product

SCM

Privilege

Administrator

Mode

Exec > Global Configuration > Context Configuration > CSCF Translation Configuration

`configure > context context_name > cscf translation name list_name`

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-cscf-translation)#`

Syntax

`after`

Usage

Add this command before the `uri-readdress` command to place the entry at the end of the translation list.
before

Places the CSCF translation entry at the top or beginning of the translation list. Use this command in conjunction with the `uri-readdress` command.

**Product**
SCM

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Translation Configuration

```
configure > context context_name > cscf translation name list_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-cscf-translation)#
```

**Syntax**

```
before
```

**Usage**

Add this command before the `uri-readdress` command to place the entry at the beginning of the translation list.
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

exit

Usage
Use this command to return to the parent configuration mode.
uri-readdress

Configures readdress criteria for URI translations.

Product
SCM

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > CSCF Translation Configuration

configure > context context_name > cscf translation name list_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-cscf-translation)#

Syntax

uri-readdress type trans_type [ log ] { base-criteria criteria } [ filter-criteria1 criteria ] [ filter-criteria2 criteria ]

no uri-readdress type trans_type { base-criteria criteria } [ filter-criteria1 criteria ] [ filter-criteria2 criteria ]

Remove the readdress configuration.

type trans_type

Specifies that the translation list (trans_type) entry is to be identified as one of the following:
- blocking-cid: Identifies the translation list entry type as “call ID blocking”.
- cancel-blocking-cid: Identifies the translation list entry type as “cancel call ID blocking”.
- cancel-cid: Identifies the translation list entry type as “cancel call ID display”.
- cancel-cw: Identifies the translation list entry type as “cancel call-waiting”.
- cfb1-off: Identifies the translation list entry type as “call forward busy line off”.
- cfb1-on: Identifies the translation list entry type as “call forward busy line on”.
- cfna-off: Identifies the translation list entry type as “call forward no answer off”.
- cfna-on: Identifies the translation list entry type as “call forward no answer on”.
- cfu-off: Identifies the translation list entry type as “call forward unconditional off”.
- cfu-on: Identifies the translation list entry type as “call forward unconditional on”.
- cid: Identifies the translation list entry type as “call ID display”.
- cw-off: Identifies the translation list entry type as “call-waiting off”.
- cw-on: Identifies the translation list entry type as “call-waiting on”.
- directory-assistance: Identifies the translation list entry type as “directory assistance”.
- emergency: Identifies the translation list entry type as “emergency”.
- international: Identifies the translation list entry type as “international”.
- local: Identifies the translation list entry type as “local”.
- long-distance: Identifies the translation list entry type as “long-distance”.
- none: Identifies the translation list entry type as “any”.
- operator-assistance: Identifies the translation list entry type as “operator assistance”.

operator-assistance
**premium-service**: Identifies the translation list entry type as “premium service”.

**service**: Identifies the translation list entry type as “special service”.

**toll-free**: Identifies the translation list entry type as “toll free”.

**log**

Enables logging for CSCF sessions meeting the readdress criteria for URI translations.

**base-criteria criteria**

Specifies the base criteria that packets will be compared against. The following criteria is supported:

- **any**: Filters all CSCF sessions.
- **destination aor aor**: Filters sessions based on the destination AoR.
  
  *aor* must be an existing AoR from 1 to 79 characters in length.

**Important**: AoR regular expressions are supported. Refer to the SCM Engineering Rules Appendix in the Session Control Manager Administration Guide for more information about regular expressions.

- **plmn-id mcc mcc_code mnc mnc_code**: Filters sessions based on the mobile country and network codes.
  
  *mcc_code* must be a three-digit integer from 200 to 999.
  
  *mnc_code* must be either a two or three-digit integer from 00 to 999 or **any** (any MNC code).

- **source address ip_address**: Filters sessions based on source IP address.
  
  *ip_address* must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6.

- **source aor aor**: Filters sessions based on the source AoR.
  
  *aor* must be an existing AoR from 1 to 79 characters in length.

**filter-criteria criteria**

Specifies the filter criteria that packets that have passed the base criteria will be compared against. The following criteria is supported:

- **any**: Filters all CSCF sessions.

- **destination aor aor**: Filters sessions based on the destination AoR.
  
  *aor* must be an existing AoR from 1 to 79 characters in length.

**Important**: AoR regular expressions are supported. Refer to the SCM Engineering Rules Appendix in the Session Control Manager Administration Guide for more information about regular expressions.

- **plmn-id mcc mcc_code mnc mnc_code**: Filters sessions based on the mobile country and network codes.
  
  *mcc_code* must be a three-digit integer from 200 to 999.
  
  *mnc_code* must be either a two or three-digit integer from 00 to 999 or **any** (any MNC code).

- **source address ip_address**: Filters sessions based on source IP address.
  
  *ip_address* must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6.

- **source aor aor**: Filters sessions based on the source AoR.
uri-readdress

aor must be an existing AoR from 1 to 79 characters in length.

filter-criteria2 criteria

Specifies the filter criteria that packets that have passed the base criteria and filter criteria1 will be compared against. The following criteria is supported:

• any: Filters all CSCF sessions.
• destination aor aor: Filters sessions based on the destination AoR.
  aor must be an existing AoR from 1 to 79 characters in length.

Important: AoR regular expressions are supported. Refer to the SCM Engineering Rules Appendix in the Session Control Manager Administration Guide for more information about regular expressions.

• plmn-id mcc mcc_code mnc mnc_code: Filters sessions based on the mobile country and network codes.
  mcc_code must be a three-digit integer from 200 to 999.
  mnc_code must be either a two or three-digit integer from 00 to 999 or any (any MNC code).
• source address ip_address: Filters sessions based on source IP address.
  ip_address must be expressed in dotted decimal notation for IPv4 or colon notation for IPv6.
• source aor aor: Filters sessions based on the source AoR.
  aor must be an existing AoR from 1 to 79 characters in length.

Usage

Use this command to readdress URIs based on specified criteria and enters the URI Readdress Configuration Mode. Readdressing can be used for:

• Mobility: When roaming in a visited domain.
• Service Aliases: Resolving well-known addresses via SIP-AS.
• Number Translation: Adding or deleting prefixes such as +1 to/from PSTN numbers.
• Voice VPNs: Using inter-office extensions to dial remote offices.

Entering this command results in the following prompt:

[context_name]hostname(config-uri-readdress)#

URI readdress commands are defined in the CSCF URI Readdress Configuration Mode Commands chapter of this reference.

Example

The following command readdresses sessions to a domain named service.com, filters sessions with a base criteria of the source address (1.2.3.4) and a filter criteria of the destination AoR ($.@test.com):

uri-readdress type service base-criteria source address 1.2.3.4 filter-critical destination aor $.@test.com
Chapter 101
CSCF URI Readdress Configuration Mode Commands

The URI Readdress Configuration Mode is used to set URI translations.

Mode

Exec > Global Configuration > Context Configuration > CSCF Translation Configuration > URI Readdress Configuration

configure > context  context_name > cscf translation name  list_name > uri-readdress type  readdress_type  base-criteria  base_criteria

Entering the above command sequence results in the following prompt:

[context_name] host_name(config-uri-readdress)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
**action**

Adjusts a target address to route sessions to appropriate locations.

**Product**
SCM

**Privilege**
Administrator, Config-administrator

**Mode**
Exec > Global Configuration > Context Configuration > CSCF Translation Configuration > URI Readdress Configuration

```bash
configure > context context_name > cscf translation name list_name > uri-readdress type readaddress_type base-criteria base_criteria
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-uri-readdress)#
```

**Syntax**

```bash
action { add string | delete num_chars | modify string } position num length length

target { destination | source } { aor | domain | user }
```

**no action**

- **add string | delete num_chars | modify string**

  - **add string**: Adds a specified string to a location indicated by the `position` keyword for the targeted source or destination address component (aor, domain, or user). `string` must be from 1 to 79 alpha and/or numeric characters.
  - **delete num_chars**: Deletes a number of characters starting from a location specified by the `position` keyword for the targeted source or destination address component (aor, domain, or user). `num_chars` must be an integer from 1 to 79.
  - **modify string**: Modifies a specified string in a location starting with the `position` keyword for the targeted source or destination address component (aor, domain, or user). The number of characters in the `string` variable will replace the same number in the address. `string` must be from 1 to 79 alpha and/or numeric characters.

- **position num**

  Specifies the position in the target string where the action is to occur. `num` must be an integer from 1 to 79.

- **length length**

  Specifies the length of the target string where the action is to occur. `length` must be an integer from 1 to 79.

**Important**: The `length` keyword is only supported in `modify` actions.

- **target { destination | source }**

  Species that the action is to occur within the source or destination address.
The `action` command is used to manipulate SIP packets matching the criteria in the `uri-readdress` command. It allows for the manipulation of targets by specifying `aor`, `domain`, or `user`. The `no` option disables the target address to route sessions.

**Usage**

Use this command to manipulate SIP packets matching the criteria in the `uri-readdress` command.

**Example**

The following command prepends a “+1” to a destination AoR:

```
action add +1 position 1 target destination aor
```

The following command removes the first two characters from the destination AoR:

```
action delete 2 position 1 target destination aor
```

The following command replaces characters 2 through 4 with the characters “abc” in the destination AoR:

```
action modify abc position 2 target destination aor
```
end

Exits the current configuration mode and returns to the Exec mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

end

**Usage**

Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

exit

Usage
Use this command to return to the parent configuration mode.
Chapter 102
CSCF URN List Configuration Mode Commands

The CSCF URN List Configuration Mode is used to map URNs to URIs for emergency and local call services.

Mode

Exec > Global Configuration > Context Configuration > CSCF URN List Configuration

configure > context context_name > cscf urn-service-list name list_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-cscf-service-urn)#

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
cscf-urn-service-mapping

Adds an entry to the service URN mapping table that maps uniform resource names (URNs) to URIs in order to direct specific service-oriented identifiers to the proper location in a network. The table is used after CSCF translation if the result is a local service.

Product
SCM

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > CSCF URN List Configuration

configure > context context_name > cscf urn-service-list name list_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-cscf-service-urn)#

Syntax

[ no ] cscf-urn-service-mapping urn urn uri uri

-no
Removes an entry from the service URN mapping table.

-urn urn
Specifies the URN to be routed via a URL to the appropriate destination. urn must be from 1 to 79 alpha and/or numeric characters.

-uri uri
Specifies the URI used to route the URN to the appropriate location. uri must be from 1 to 79 alpha and/or numeric characters.

Usage
Use this command to add an entry to the service URN mapping table that routes a translated URN to a URI for local services.

Important: Service URN mapping tables are limited to 30 URN to URI mapping entries.

Example
The following command map URN business to URI corp@123.45.678.9:5020 and adds it to the service URN mapping table:

    cscf-urn-service-mapping urn business uri corp@123.45.678.9:5020
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
end
```

**Usage**

Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Use this command to return to the parent configuration mode.
Chapter 103
DHCP Client Profile Configuration Mode Commands

The Dynamic Host Configuration Protocol (DHCP) Client Profile Configuration Mode is used to create and manage DHCP client profile parameters. DHCP client profiles are associated with APNs.

Mode

Exec > Global Configuration > Context Configuration > DHCP Client Profile Configuration

configure > context context_name > dhcp-client-profile profile_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-dhcp-client-profile)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
**client-identifier**

Configures the client-identifier which is sent to the external DHCP server.

**Product**

GGSN
P-GW
SAEGW

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > DHCP Client Profile Configuration

```
counture > context context_name > dhcp-client-profile profile_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dhcp-client-profile)#
```

**Syntax**

```
client-identifier { imsi | msisdn }
```

```
default dhcp client-identifier
```

- **default**
  
  Specifies that the subscriber’s IMSI be included in the client-identifier option of relevant DHCP messages.

- **imsi**
  
  Specifies that the subscriber’s IMSI be included in the client-identifier option of relevant DHCP messages.

**Important:** The **imsi** option is not supported in this release.

- **msisdn**
  
  Specifies that the subscriber’s MSISDN be included in the client-identifier option of relevant DHCP messages.

**Usage**

Use this command to configure which information is included in the DHCP client-identifier option of DHCP messages to external DHCP servers.

**Example**

The following command specifies that a subscriber’s MSISDN be included in the DHCP client-identifier option of DHCP messages to external DHCP servers:

```
client-identifier msisdn
```
### disable

Disables the specified options on the DHCP client.

**Product**
- GGSN
- P-GW
- SAEGW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > DHCP Client Profile Configuration
```
configure > context context_name > dhcp-client-profile profile_name
```

Entering the above command sequence results in the following prompt:
```
[context_name]host_name(config-dhcp-client-profile)#
```

**Syntax**
```
disable { dhcp-message-spray | rapid-commit-dhcpv4 | rapid-commit-dhcpv6 }
```

- **dhcp-message-spray**
  Disables DHCP client from spraying a DHCP message to all configured DHCP servers in the PDN.

- **rapid-commit-dhcpv4**
  Disables support of the rapid commit feature for DHCPv4 client functionality.

- **rapid-commit-dhcpv6**
  Disables support of the rapid commit feature for DHCPv6 client functionality.

**Usage**

Use this command to disable options on the DHCP client.

**Example**

The following command disables support of the rapid commit feature for DHCPv6 client functionality:
```
disable rapid-commit-dhcpv6
```
enable

Enables the specified options on the DHCP client.

Product

GGSN
P-GW
SAEGW

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > Context Configuration > DHCP Client Profile Configuration
configure > context context_name > dhcp-client-profile profile_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-dhcp-client-profile)#

Syntax

enable { dhcp-message-spray | rapid-commit-dhcpv4 | rapid-commit-dhcpv6 }

**dhcp-message-spray**

Enables DHCP client to spray a DHCP message to all configured DHCP servers in the PDN.
By default, this is disabled. With rapid commit, there can only be one server to which this can be sent.

**rapid-commit-dhcpv4**

Enables support of the rapid commit feature for DHCPv4 client functionality.
By default, this is enabled.

**rapid-commit-dhcpv6**

Enables support of the rapid commit feature for DHCPv6 client functionality.
By default, this is enabled.

Usage

Use this command to enable options on the DHCP client.

Example

The following command enables support of the rapid commit feature for DHCPv6 client functionality:

```
enable rapid-commit-dhcpv6
```
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**

Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Use this command to return to the parent configuration mode.
request

Configures DHCP options which can be requested by the DHCP client.

**Product**
- GGSN
- P-GW
- SAEGW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > DHCP Client Profile Configuration
configure > context context_name > dhcp-client-profile profile_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dhcp-client-profile)#
```

**Syntax**

```
[ default ] request dhcp-option { dns-address | netbios-server-address | sip-server-address }
no { dns-address | netbios-server-address | sip-server-address }
```

- **default**
  Returns the command to its default setting.

- **no**
  Disables a DHCP option requested by the DHCP client.

- **dhcp-option { dns-address | netbios-server-address | sip-server-address }**
  The following DHCP options can be requested by the DHCP client:
  - `dns-address`: request for DNS address
  - `netbios-server-address`: request for NetBIOS server address
  - `sip-server-address`: request for SIP server address

**Usage**

Use this command to enable/disable options which can be requested by the DHCP client.

**Example**

The following command enables the DHCP client to request DNS address:

```
request dhcp-option dns-address
```
Chapter 104
DHCP Server Profile Configuration Mode Commands

The Dynamic Host Configuration Protocol (DHCP) Server Profile Configuration Mode is used to create and manage DHCP server profile parameters. DHCP server profiles are associated with APNs.

Mode

Exec > Global Configuration > Context Configuration > DHCP Server Profile Configuration

configure > context context_name > dhcp-server-profile profile_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-dhcp-server-profile)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
**dhcpv6-server-preference**

Specifies the waiting time for DHCPv6 client before response.

**Product**

GGSN
P-GW
SAEGW

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > DHCP Server Profile Configuration

```bash
configure > context context_name > dhcp-server-profile profile_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dhcp-server-profile)#
```

**Syntax**

```
dhcpv6-server-preference pref_value

default dhcpv6-server-preference
```

**default**

Returns the command to its default setting of 0.

**pref_value**

Specifies the DHCP server preference value as an integer from 1 through 255. If a DHCP server responds with a preference value of 255, DHCPv6 client need not wait any longer.

Default: 0

**Usage**

According to RFC-3315, DHCPv6 client should wait for a specified amount of time before considering responses to its queries from DHCPv6 servers. Use this command to specify the waiting time (DHCP server preference value) for DHCPv6 client before response.

**Example**

The following command sets the DHCP server preference value to 200:

```
dhcpv6-server-preference 200
```
disable

Disables the specified options on the DHCP server.

**Product**
- GGSN
- P-GW
- SAEGW

**Privilege**
- Security Administrator, Administrator

**Mode**
```
Exec > Global Configuration > Context Configuration > DHCP Server Profile Configuration
configure > context context_name > dhcp-server-profile profile_name
```

Entering the above command sequence results in the following prompt:
```
[context_name]host_name(config-dhcp-server-profile)#
```

**Syntax**
```
disable { dhcpv6-server-reconf | dhcpv6-server-unicast | rapid-commit-dhcpv4 | rapid-commit-dhcpv6 }
```

---

**Syntax**
- **dhcpv6-server-reconf**
  Disables support for reconfiguration messages from the DHCPv6 server.

- **dhcpv6-server-unicast**
  Disables server unicast option for DHCPv6 server.

- **rapid-commit-dhcpv4**
  Disables support of the rapid commit feature for DHCPv4 server functionality.

- **rapid-commit-dhcpv6**
  Disables support of the rapid commit feature for DHCPv6 server functionality.

**Usage**
Use this command to disable options on the DHCP server.

**Example**
The following command disables support of the rapid commit feature for DHCPv6 server functionality:
```
   disable rapid-commit-dhcpv6
```
enable

Enables the specified options on the DHCP server.

**Product**
- GGSN
- P-GW
- SAEGW

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration > Context Configuration > DHCP Server Profile Configuration

```
configure > context context_name > dhcp-server-profile profile_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dhcp-server-profile)#
```

**Syntax**

```
enable { dhcpv6-server-reconf | dhcpv6-server-unicast | rapid-commit-dhcpv4 | rapid-commit-dhcpv6 }
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dhcpv6-server-reconf</td>
<td>Enables support for reconfiguration messages from the DHCPv6 server. By default, this is disabled.</td>
</tr>
<tr>
<td>dhcpv6-server-unicast</td>
<td>Disables server unicast option for DHCPv6 server. By default, this is disabled.</td>
</tr>
<tr>
<td>rapid-commit-dhcpv4</td>
<td>Enables support of the rapid commit feature for DHCPv4 server functionality. By default, this is disabled.</td>
</tr>
<tr>
<td>rapid-commit-dhcpv6</td>
<td>Enables support of the rapid commit feature for DHCPv6 server functionality. By default, this is disabled; this is done to ensure that if there are multiple DHCPv6 servers in a network, with rapid-commit-option, they would all end up reserving resources for the UE.</td>
</tr>
</tbody>
</table>

**Usage**

Use this command to enable options on the DHCP server.

**Example**

The following command enables support of the rapid commit feature for DHCPv6 server functionality:

```
enable rapid-commit-dhcpv6
```
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

    end

**Usage**
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Use this command to return to the parent configuration mode.
process

Configures what order the configuration options should be processed for a given client request.

Product
GGSN
P-GW
SAEGW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > DHCP Server Profile Configuration
configure > context context_name > dhcp-server-profile profile_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-dhcp-server-profile)#

Syntax

process dhcp-option-from { AAA | LOCAL | PDN-DHCP } priority priority
default process dhcp-option-from

default
AAA (priority 1) is preferred over PDN-DHCP (priority 2) which is preferred over LOCAL (priority 3) configuration.

dhcp-option-from { AAA | LOCAL | PDN-DHCP }
For a given client request, configuration values can be obtained from the following:
•AAA
•LOCAL
•PDN-DHCP

priority priority
Specifies the priority for dhcp-option-from options.
priority is an integer from 1 through 3. 1 is the highest priority.

Usage
Use this command to configure what order the configuration options should be processed for a given client request.

Example
The following command sets configuration options from a PDN DHCP server at the highest priority of 1 for a given client request:

process dhcp-option-from PDN-DHCP priority 1
Chapter 105
DHCP Service Configuration Mode Commands

The Dynamic Host Control Protocol (DHCP) Configuration Mode is used to create and manage DHCP service instances for the current context.

Mode

Exec > Global Configuration > Context Configuration > DHCP Service Configuration

```
configure > context context_name > dhcp-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dhcp-service)#
```

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
allow

Allows the specified options on the DHCP service.

**Product**
P-GW
SAEGW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > DHCP Service Configuration
configure > context context_name > dhcp-service service_name

Entering the above command sequence results in the following prompt:

```bash
[context_name]host_name(config-dhcp-service)#
```

**Syntax**

```
[ no ] allow { dhcp-client rapid-commit | dhcp-inform | dhcp-parameter-request-list-option { router | subnet-mask } | dhcp-relay-agent-auth-suboption | dhcp-relay-agent-option | dhcp-server rapid-commit }
```

- **no**
  Disables an option on the DHCP service.

- **dhcp-client rapid-commit**
  Enables support of the rapid commit feature for DHCP client functionality, as defined in RFC 4039.

- **dhcp-inform**
  Enables the sending of DHCP inform after configuration for address recovery.

- **dhcp-parameter-request-list-option { router | subnet-mask }**
  Enables the sending of DHCP parameter request list option in all outgoing messages.
  *router*: Send DHCP parameter request list option with router flag in all outgoing messages.
  *subnet-mask*: Send DHCP parameter request list option with subnet mask flag in all outgoing messages.

- **dhcp-relay-agent-auth-suboption**
  Enables the sending of DHCP relay agent authentication suboption in all outgoing messages.

- **dhcp-relay-agent-option**
  Enables the sending of DHCP relay agent option in all outgoing messages.

- **dhcp-server rapid-commit**
  Enables support of the rapid commit feature for DHCP server functionality, as defined in RFC 4039.
Usage

Use this command to enable/disable options on the DHCP service.

Example

The following command enables support of the rapid commit feature for DHCP server functionality:

    allow dhcp-server rapid-commit
bind

Binds the DHCP service to a logical IP interface facilitating the system’s connection to the DHCP server. This command also configures traffic from the specified DHCP service bind address to use the specified Multiple Protocol Label Switching (MPLS) labels.

**Product**
- ASN-GW
- eWAG
- GGSN
- HA
- P-GW
- SAEGW

**Privilege**
- Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > DHCP Service Configuration

```
configure > context context_name > dhcp-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dhcp-service)#
```

**Syntax**

```
bind address ip_address [ nexthop-forwarding-address nexthop_ip_address [ mpls-label input in_mpls_label_value output out_mpls_label_value1 [ out_mpls_label_value2 ] ] ]

no bind address ip_address
```

- **no**
  - Removes a previously configured binding.

- **address ip_address**
  - Specifies the IP address of an interface in the current context through which communication with the DHCP server occurs.
  - `ip_address` must be expressed in IPv4 dotted-decimal notation.

---

**Important:** In the case of DeWAG service, this IP address must be the same as the IP address configured with the `dhcp server` CLI command under the same DHCP Service Configuration mode. Also, this IP address must match the DeWAG service’s IP address so that the WLC can relay the DHCP unicast packets to the DeWAG service IP address and are processed by this DHCP service.

```
nexthop-forwarding-address nexthop_ip_address
```

- Specifies the next hop gateway address for in MPLS network to which the packets with MPLS labels will be forwarded.
nexthop_ip_address must be expressed in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

**Important:** In the case of DeWAG service, this option must not be configured.

```
mpls-label input in_mpls_label_value
```

Specifies the MPLS label to identify inbound traffic destined for the configured DHCP service bind address ip_address.

in_mpls_label_value is the MPLS label that will identify inbound traffic destined for the configured DHCP service and must be an integer from 16 through 1048575.

**Important:** This keyword is license-enabled and available with valid MPLS feature license only.

**Caution:** For DHCP over MPLS feature to work in StarOS 9.0 onward the dhcp ip vrf command must be configured in DHCP service. Without dhcp ip vrf command the DHCP service using MPLS labels will not be started as a part of a DHCP over MPLS configuration. In release 9.0 onward this keyword is a critical parameter for the DHCP-Service. Any change in its value will result in DHCP-service restart and clearing of the existing calls.

**Important:** In the case of DeWAG, this option must not be configured.

```
output out_mpls_label_value1 [ out_mpls_label_value2 ]
```

Adds the MPLS label to the outbound traffic sent from the configured DHCP service bind address ip_address. The labels out_mpls_label_value1 and out_mpls_label_value2 identify the MPLS labels to be added to packets sent from the specified dhcp service bind address.

out_mpls_label_value1 is the inner output label and must be an integer from 16 through 1048575.

out_mpls_label_value2 is the outer output label and must be an integer from 16 through 1048575.

**Important:** This keyword is license-enabled and available with valid MPLS feature license only.

**Important:** In the case of DeWAG, this option must not be configured.

**Usage**

Use this command to associate or tie the DHCP service to a specific logical IP address previously configured in the current context and bound to a port. Once bound, the logical IP address or interface is used in the giaddr field of the DHCP packets.

When this command is executed, the DHCP service is started and begins the process of requesting addresses from the DHCP server and storing them in cache memory for allocation to PDP contexts.
This command can also be used to configure MPLS labels for inbound and outbound traffic through this
DHCP address.
Only one interface can be bound to a service.
For DHCP over MPLS feature to work in StarOS 9.0 onward `dhcp ip vrf` command must be configured in
DHCP service. Without `dhcp ip vrf` command the DHCP service using MPLS labels will not be started.

⚠️ Caution: As a part of DHCP over MPLS configuration, the `mpls-label input` keyword in the `bind
address` command is also a critical parameter for the DHCP-Service. Any change in its value will result in DHCP-
service restart and clearing of the existing calls.

Example

The following command binds the DHCP service to the interface with an IP address of 192.168.1.210:

```
bind address 192.168.1.210
```
default

Restores DHCP service parameters to their factory default settings.

Product
GGSN
ASN-GW
HA
P-GW
SAEGW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > DHCP Service Configuration
configure > context context_name > dhcp-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-dhcp-service)#

Syntax

default { T1-threshold | T2-threshold | dhcp { chaddr-validate | client-identifier |
deadtime | detect-dead-server { consecutive-failures } | server selection-algorithm } |
lease-duration | max-retransmissions | retransmission-timeout }

dhcp { deadtime | detect-dead-server { consecutive-failures } | server-selection-
algorithm }

Restores the following DHCP parameters to their respective default settings:
• deadtime: Default 10 minutes
• detect-dead-server { consecutive-failures }: Default 5
• server-selection-algorithm: Default First-server

lease-duration
Restores the lease-duration parameter to its default setting of 86400 seconds.

max-retransmissions
Restores the max-retransmissions parameter to its default setting of 5.

retransmission-timeout
Restores the retransmission-timeout parameter to its default setting of 3000 milli-seconds.

T1-threshold
Restores the T1-threshold parameter to its default setting of 50%.
**T2-threshold**

Restores the T2-threshold parameter to its default setting of 88%.

**Usage**

After system parameters have been modified, this command is used to set/restore specific parameters to their default values.

**Example**

The following command restores the DHCP deadtime parameter to its default setting of 10 minutes:

```sh
default dhcp deadtime
```
dhcp chaddr-validate

Configures the behavior of the client hardware address (chaddr) validation in DHCP messages.

**Product**
- GGSN
- HA
- P-GW
- SAEGW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > DHCP Service Configuration
```
configure > context context_name > dhcp-service service_name
```

Entering the above command sequence results in the following prompt:
```
[context_name]host_name(config-dhcp-service)#
```

**Syntax**

```
[ default | no ] dhcp chaddr-validate
```

- **default**
  Validates the chaddr value received in a DHCPACK message with the chaddr value sent in a DHCPREQUEST message.

- **no**
  Disables validation of the chaddr value received in DHCPACK message with the chaddr value sent in a DHCPREQUEST message.

**Important:** The chaddr information value in the DHCPACK message will be parsed but not be validated against the value maintained with client. The chaddr information value in DHCPACK will be ignored and not be stored internally.

**Usage**
Use this command to configure behavior relating to the validation of chaddr information validation in the DHCPACK messages.

**Example**
The following command specifies that the chaddr will not be validated in the DHCP messages:
```
no dhcp chaddr-validate
```
dhcp client-identifier

Configures the behavior relating to inclusion of a client identifier DHCP option in DHCP messages.

Product
GGSN
HA
P-GW
SAEGW
HNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > DHCP Service Configuration
configure > context context_name > dhcp-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-dhcp-service)#

Syntax

dhcp client-identifier { ike-id | mac-address | msisdn | none }

default dhcp client-identifier

default
Sets the behavior of DHCP client identifier to default – do not to include client identifier option in any DHCP message.

ike-id
Specifies the Internet Key Exchange Protocol version 2 id of HNB as the DHCP client-identifier option in any DHCP message to DHCP server in Discover and Request messages.

Important: This keyword is HNB-GW license controlled.

mac-address
Specifies the subscribers mac-address as the DHCP client-identifier option in any DHCP message.

msisdn
Specifies that the subscriber’s MSISDN be included in the client-identifier option of the relevant DHCP messages. Default: disabled

Important: This keyword is GGSN and P-GW/SAEGW license controlled.
none

Specifies that DHCP client-identifier option would not be included in any DHCP messages. This is the default behavior. Default: enabled

Usage

Use this command to configure behavior relating to inclusion or exclusion of DHCP client identifier option from DHCP messages.

Example

The following command specifies that DHCP client-identifier option be excluded from DHCP messages:

```
dhcp client-identifier none
```
dhcp deadtime

Configures the amount of time that the system waits prior to re-communicating with a DHCP server that was previously marked as down.

Product

GGSN
ASN-GW
HA
P-GW
SAEGW

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > Context Configuration > DHCP Service Configuration

configure > context context_name > dhcp-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-dhcp-service)#

Syntax

dhcp deadtime max_time

max_time

Specifies the maximum amount of time (in minutes) to wait before communicating with a DHCP server that was previously unreachable. max_time is an integer value from 1 through 65535. Default: 10

Usage

If the system is unable to communicate with a configured DHCP server, after a pre-configured number of failures the system marks the server as being down. This command specifies the amount of time that the system waits prior to attempting to communicate with the downed server.

Important: If all DHCP servers are down, the system will immediately treat all DHCP servers as active, regardless of the deadtime that is specified.

Refer to the dhcp detect-dead-server and max-retransmissions commands for additional information on the process the system uses to mark a server as down.

Example

The following command configures the system to wait 20 minutes before attempting to re-communicate with a dhcp server that was marked as down:

dhcp deadtime 20
dhcp detect-dead-server

Configures the number of consecutive communication failures that could occur before the system marks a DHCP server as down.

Product
GGSN
ASN-GW
HA
P-GW
SAEGW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > DHCP Service Configuration

configure > context context_name > dhcp-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-dhcp-service)#

Syntax

```
dhcp detect-dead-server consecutive-failures max_number
```

```
consecutive-failures max_number
```

Specifies the number of failures that could occur before marking a DHCP server as down as an integer from 1 through 1000. Default: 5

Usage

This command works in conjunction with the max-retransmissions parameter to set a limit to the number of communication failures that can occur with a configured DHCP server.

The max-retransmissions parameter limits the number of attempts to communicate with a server. Once that limit is reached, the system treats it as a single failure. This parameter limits the number of consecutive failures that can occur before the system marks the server as down and communicate with the server of next highest priority.

If all of the configured servers are down, the system ignores the detect-dead-server configuration and attempt to communicate with highest priority server again.

If the system receives a message from a DHCP server that was previously marked as down, the system immediately treats it as being active.

Example

The following command configures the system to allow 8 consecutive communication failures with a DHCP server before it marks it as down:

```
dhcp detect-dead-server consecutive-failures 8
```
dhcp ip vrf

Enables DHCP-over-MPLS support and associates the specific DHCP service with a pre-configured Virtual Routing and Forwarding (VRF) Context instance for virtual routing and forwarding.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > DHCP Service Configuration
configure > context context_name > dhcp-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-dhcp-service)#

Syntax

dhcp ip vrf vrf_name

no dhcp ip vrf

no

Removes/disassociates configured IP Virtual Routing and Forwarding (VRF) context instance.

vrf_name

Specifies the name of a pre-configured VRF context instance to be associated with a DHCP service.

vrf_name is the name of a pre-configured VRF context configured in Context Configuration mode and associated with the IP Pool used by the DHCP service.

Usage

Use this command to enable the DHCP-over-MPLS support and to associate/disassociate a pre-configured VRF context to a DHCP service for this feature.

By default the VRF is NULL, which means that DHCP service is bound with binding address given by bind address command only.

VRF is not a critical parameter for the DHCP Service but bind address is a critical parameter for DHCP Service, and while starting DHCP Service, if this command is configured, then the bind address should be present in that VRF, and If this command is not configured, bind address should be present in the context where DHCP Service is configured.

For the DHCP over MPLS feature to work in StarOS 9.0 onward this command must be configured in the DHCP service. Without this command the DHCP service using MPLS labels will not be started.

⚠️ Caution: As a part of this configuration the mpls-label input keyword in the bind address command is also a critical parameter for the DHCP-Service. Any change in its value will result in DHCP-service restart and clearing of the existing calls.

Example
Following command associates VRF context instance `dhcp_vrf1` with this DHCP service:

```
dhcp ip vrf dhcp_vrf1
```
dhcp server

Configures DHCP servers with which the DHCP service is to communicate.

**Product**

ASN-GW
eWAG
GGSN
HA
P-GW
SAEGW
HNB-GW

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > DHCP Service Configuration

```
configure > context context_name > dhcp-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dhcp-service)#
```

**Syntax**

```
dhcp server { ip_address | port port_num [ priority priority ]

no dhcp server ip_address

default dhcp port
```

**Syntax——default**

Sets the default value of UDP port on DHCP server; 67 for DHCP messaging.

**Syntax——no**

Deletes a previously configured DHCP server.

```
ip_address
```

**Syntax——ip_address**

Specifies the IP address of the DHCP server expressed in IPv4 dotted-decimal notation.

**Important:** In the case of DeWAG service, this IP address must be the same as the IP address configured with the **bind address** CLI command under the same DHCP Service Configuration mode.

```
port port_num
```

**Syntax——port**

Specifies the port number to send DHCP messages to non-standard UDP ports of the server if multiple servers are configured.
**port_num** is an integer from 0 through 65535.

**Important:** While configuring HNB-GW for DHCP proxy support, operator must define 61610 as UDP port for DHCP server. The source port used by HNBGW will be standard DHCP port, irrespective of the server port that is configured.

```
priority priority
```

Specifies the priority of the server if multiple servers are configured. 

**priority** is an integer from 1 through 1000. 1 is the highest priority.

**Important:** In the case of DeWAG, this option must not be configured.

**Usage**

Use this command to configure the DHCP server(s) that the system is to communicate with. Multiple servers can be configured each with their own priority. Up to 20 DHCP servers can be configured. All DHCP messages are sent/received on UDP port 67.

**Important:** If a server is removed, all calls having an IP address allocated from the server will be released.

**Example**

The following command configures a DHCP server with an IP address of **192.168.1.200** and a priority of **1**:

```
dhcp server 192.168.1.200 priority 1
```
dhcp server selection-algorithm

Specifies the algorithm used to select DHCP servers with which to communicate when multiple servers are configured.

**Product**
- GGSN
- ASN-GW
- HA
- P-GW
- SAEGW
- HNB-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > DHCP Service Configuration

```
configure > context context_name > dhcp-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dhcp-service)#
```

**Syntax**

```
dhcp server selection-algorithm { first-server | round-robin | use-all }
```

- **first-server**
  Uses the first-server algorithm. This algorithm dictates that the system select the DHCP servers according to their priority starting with the highest priority server. The system communicates with the server of the next highest priority only when the previous server is unreachable. Default: Enabled

- **round-robin**
  Uses the round-robin algorithm. This algorithm dictates that the system communicates with the servers in a circular queue according to the server’s configured priority starting with the highest priority server. The next request is communicated with the next highest priority server, and so on until all of the servers have been used. At this point, the system starts from the highest priority server. Default: Disabled

- **use-all**
  Default: Disabled
  This algorithm dictates that the system to communicate with the all the DHCP servers configured on system.

**Usage**

Use this command to determine how configured DHCP servers are utilized by the system.

**Example**

The following command configures the DHCP service to use the round-robin selection algorithm:

```
dhcp server selection-algorithm round-robin
```
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Use this command to return to the parent configuration mode.
**lease-duration**

Configures the minimum and maximum allowable lease times that are accepted in responses from DHCP servers.

**Product**
- GGSN
- ASN-GW
- HA
- P-GW
- SAEGW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > DHCP Service Configuration

```bash
configure > context context_name > dhcp-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dhcp-service)#
```

**Syntax**

```
lease-duration min min_time max max_time
```

- **min min_time**
  Specifies the minimum acceptable lease time (in seconds) as an integer from 600 trough 3600. Default: 600

- **max max_time**
  Specifies the maximum acceptable lease time (in seconds) as an integer from 10800 through 4294967295. Default: 86400

**Usage**

To reduce the call setup time, the system requests IP addresses from the DHCP server in blocks rather than on a call-by-call basis. Each address received has a corresponding lease time, or time that it is valid. The values configured by command represent the minimum and maximum times that the system allows and negotiates for the lease(s).

If the DHCP server responds with values that are out of the range specified by the min and max values, the system accumulates warning statistics. Responses that fall below the minimum value are rejected by the system and the system contacts the DHCP server with the next highest priority. Responses that are greater than the maximum value are accepted.

When half of the lease time has expired, the system automatically requests a lease renewal from the DHCP server. This is configured using the T1-threshold command.

**Example**

The following command configures the minimum allowable lease time for the system to be **1000** and the maximum to be **36000**:
lease-duration min 1000 max 36000
lease-time

Configures the local DHCP Server lease time in seconds.

Product
ASN-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > DHCP Service Configuration

configure > context context_name > dhcp-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-dhcp-service)#

Syntax

lease-time time

default lease-time

 default

 Returns the command to its default setting of 600.

time

 Specifies the IP address lease time from the local DHCP server (in seconds) as an integer from 600 through 4294967295. Default: 600

Usage

Use this command to configure the lease time of the IP address from the local DHCP server

Example

The following command sets the lease time of the IP address from the local DHCP server to 20 minutes (1200 seconds):

 lease-time 1200
max-retransmissions

Configures the maximum number of times that the system attempts to communicate with an unresponsive DHCP server before it is considered a failure.

**Product**

GGSN
ASN-GW
HA
P-GW
SAEGW

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > DHCP Service Configuration

```
configure > context context_name > dhcp-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dhcp-service)#
```

**Syntax**

```
max-retransmissions max_number
```

- `max_number`

  Specifies the maximum number of re-attempts the system tries when no response is received from a DHCP server. `max_number` is an integer from 1 through 20. Default: 5

**Usage**

This command works in conjunction with the `dhcp detect-dead-server` parameter to set a limit to the number of communication failures that can occur with a configured DHCP server. When the value specified by this parameter is met, a failure is logged. The `dhcp detect-dead-server` parameter specifies the number of consecutive failures that could occur before the server is marked as down. In addition, the `retransmission-timeout` command controls the amount of time between re-tries.

**Example**

The following command configures the maximum number of times the system re-attempts communication with a DHCP server that is unresponsive to 5:

```
max-retransmissions 5
```
retransmission-timeout

Configures the amount of time that must pass with no response before the system re-attempts to communicate with the DHCP server.

Product
- GGSN
- ASN-GW
- HA
- P-GW
- SAEGW

Privilege
- Security Administrator, Administrator

Mode
- Exec > Global Configuration > Context Configuration > DHCP Service Configuration
- configure > context context_name > dhcp-service service_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dhcp-service)#
```

Syntax

```
retransmission-timeout time
```

- **time**
  - Specifies the time that the system waits (in milliseconds) before reattempting communication with the DHCP server. *time* is an integer from 100 through 20000. Default: 10000

Usage

This command works in conjunction with the `max-retransmissions` command to establish a limit on the number of times that communication with a DHCP server is attempted before a failure is logged.

This parameter specifies the time between retries.

Example

The following command configures a retry timeout of 1000 milliseconds:

```
retransmission-timeout 1000
```
T1-threshold

Configures the DHCP T1 timer as a percentage of the allocated IP address lease.

Product
GGSN
ASN-GW
HA
P-GW
SAEGW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > DHCP Service Configuration
configure > context context_name > dhcp-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-dhcp-service)#

Syntax

T1-threshold percentage

percentage

Specifies the percentage of the allocated IP address lease time at which the DHCP call-line state is changed to “RENEWING”. percentage is an integer from 40 through 66. Default: 50

Usage

This command is used to identify the time at which a subscriber must renew their DHCP lease as a percentage of the overall lease time. (Refer to the lease-duration command in this chapter for information on configuring the IP address lease period.)

For example, if the lease-duration was configured to have a maximum value of 12000 seconds, and this command is configured to 40%, then the subscriber would enter the RENEWING state after 4800 seconds.

Example

The following command configures the T1 threshold to 40%:

T1-threshold 40
T2-threshold

Configures the DHCP T2 timer as a percentage of the allocated IP address lease.

Product

GGSN
ASN-GW
HA
P-GW
SAEGW

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > Context Configuration > DHCP Service Configuration
configure > context context_name > dhcp-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-dhcp-service)#

Syntax

T2-threshold percentage

`percentage`

Specifies the percentage of the allocated IP address lease time at which the DHCP call-line state is changed to “REBINDING”. `percentage` is an integer from 67 through 99. Default: 88

Usage

This command is used to identify the time at which a subscriber re-binds their DHCP leased IP address as a percentage of the overall lease time. (Refer to the `lease-duration` command in this chapter for information on configuring the IP address lease period.)

For example, if the lease-duration was configured to have a maximum value of 12000 seconds, and this command is configured to 70%, then the subscriber would enter the REBINDING state after 8400 seconds.

Example

The following command configures the T2 threshold to 70%:

```none
T2-threshold 70 70
```
Chapter 106
DHCPv6 Client Configuration Mode Commands

The Dynamic Host Configuration Protocol (DHCP) for Internet Protocol Version 6 (IPv6) Client Configuration Mode is used to create and manage DHCPv6 client parameters to support DHCPv6-based address assignment.

Mode

Exec > Global Configuration > Context Configuration > DHCPv6 Service Configuration > DHCPv6 Client Configuration

`configure > context context_name > dhcpv6-service service_name > dhcpv6-client`

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-dhcpv6-client)#`

⚠️ **Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**
Use this command to return to the parent configuration mode.
max-retransmissions

Configures the maximum number of times that the system attempts to communicate with an unresponsive DHCPv6 server before it is considered a failure.

### Product
- GGSN
- P-GW
- SAEGW

### Privilege
- Security Administrator, Administrator

### Mode

`Exec > Global Configuration > Context Configuration > DHCPv6 Service Configuration > DHCPv6 Client Configuration

configure > context context_name > dhcpv6-service service_name > dhcpv6-client`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dhcpv6-client)#
```

### Syntax

```
max-retransmissions max_number

default max-retransmissions
```

**default**

Returns the command to its default setting of 20.

**max_number**

Specifies the maximum number of re-attempts the system tries when no response is received from a DHCPv6 server. `max_number` is an integer from 1 through 20. Default: 20

### Usage

This command works in conjunction with the `detect-dead-server` DHCPv6 service command to set a limit to the number of communication failures that can occur with a configured DHCPv6 service. When the value specified by this parameter is met, a failure is logged. The `detect-dead-server` DHCPv6 service parameter specifies the number of consecutive failures that could occur before the server is marked as down.

### Example

The following command configures the maximum number of times the system re-attempts communication with a DHCPv6 server that is unresponsive to 5:

```
max-retransmissions 5
```
server-dead-time

Configures the amount of time that the client attempts to communicate with an unresponsive DHCPv6 server. DHCPv6 server is considered to be dead if it doesn't respond after given tries from client.

Product
GGSN
P-GW
SAEGW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > DHCPv6 Service Configuration > DHCPv6 Client Configuration

configure > context context_name > dhcpv6-service service_name > dhcpv6-client

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-dhcpv6-client)#

Syntax

server-dead-time dead_time

default server-dead-time

default

Returns the command to its default setting of 5.

default

Specifies the maximum amount of time (in seconds) that the client attempts to communicate with an unresponsive DHCPv6 server.

default must be an integer value from 1 through 1932100.
Default: 5

Usage

Use this command to specify the maximum amount of time (in seconds) that the client attempts to communicate with an unresponsive DHCPv6 server.

This command works in conjunction with the max-retransmissions command to set a limit to the number of times that the system attempts to communicate with an unresponsive DHCPv6 server before it is considered a failure.

Example

The following command configures the client to continue trying to communicate with an unresponsive DHCPv6 server for no more than 10 seconds:

server-dead-time 10
**server-ipv6-address**

Configures DHCPv6 server(s) with which the DHCPv6 client is to communicate.

**Product**
- GGSN
- P-GW
- SAEGW

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration > Context Configuration > DHCPv6 Service Configuration > DHCPv6 Client Configuration

configure > context context_name > dhcpv6-service service_name > dhcpv6-client

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-dhcpv6-client)#

**Syntax**

```
server-ipv6-address ipv6_address [ port port_number ] [ priority priority ] [ -noconfirm ]

no server-ipv6-address ipv6_address
```

- **no**
  - Deletes a previously configured DHCPv6 server.

- **ipv6_address**
  - Specifies the IP address of the DHCPv6 server expressed in IPv6 colon-separated-hexadecimal notation.
  - Default: FF02::1:2

- **port port_number**
  - Specifies the port used for communicating with the DHCPv6 server.
  - `port_number` must be an integer from 1 through 65535. If unspecified, the default port is 547.

- **priority priority**
  - Specifies the priority of the server if multiple servers are configured.
  - `priority` is an integer from 1 through 1000. 1 is the highest priority.

- **-noconfirm**
  - Executes the command without prompting for further input from the user.
Usage

Use this command to configure the DHCPv6 server(s) that the client is to communicate with. Multiple servers can be configured, each with their own priority.

Example

The following command configures a DHCPv6 server with an IP address of 1234:245:3456:4567:5678:6789:7890:8901, a port of 300, and a priority of 1:

```
server-ipv6-address 1234:245:3456:4567:5678:6789:7890:8901 port 300
priority 1
```
server-resurrect-time

Configures the amount of time that a DHCPv6 client waits before considering a dead DHCPv6 server alive again.

**Product**
- GGSN
- P-GW
- SAEGW

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration > Context Configuration > DHCPv6 Service Configuration > DHCPv6 Client Configuration

```
configure > context context_name > dhcpv6-service service_name > dhcpv6-client
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dhcpv6-client)#
```

**Syntax**

```
server-resurrect-time revive_time
```

```
default server-resurrect-time
```

**Usage**

Use this command to specify the amount of time that a DHCPv6 client waits before considering a dead DHCPv6 server alive again.

**Example**

The following command configures the client to wait 25 seconds before considering a dead DHCPv6 server alive again:

```
server-resurrect-time 25
```
Chapter 107
DHCPv6 Server Configuration Mode Commands

The Dynamic Host Configuration Protocol (DHCP) for Internet Protocol Version 6 (IPv6) Server Configuration Mode is used to create and manage DHCPv6 server parameters to support DHCPv6-based address assignment.

Mode

Exec > Global Configuration > Context Configuration > DHCPv6 Service Configuration > DHCPv6 Server Configuration

`configure > context context_name > dhcpv6-service service_name > dhcpv6-server`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dhcpv6-server)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**

Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
    All

Privilege
    Security Administrator, Administrator

Syntax
    exit

Usage
    Use this command to return to the parent configuration mode.
ipv6

Configures M/O flag for neighbor discovery protocol.

Product
- GGSN
- P-GW
- SAEGW

Privilege
- Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > DHCPv6 Service Configuration > DHCPv6 Server Configuration

configure > context context_name > dhcpv6-service service_name > dhcpv6-server

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-dhcpv6-server)#

Syntax

```
ipv6 nd { managed-config-flag | other-config-flag }
```

```
nd { managed-config-flag | other-config-flag }
```

Configure M/O flag for neighbor discovery protocol.

- **managed-config-flag**: Configure M flag.
- **other-config-flag**: Configure O flag.

Usage

Use this command to specify the M/O flag for neighbor discovery protocol.

Example

The following command configures the M flag for neighbor discovery protocol:

```
ipv6 nd managed-config-flag
```
preferred-lifetime

Configures the preferred lifetime for prefixes assigned by the DHCPv6 service.

**Product**
- GGSN
- P-GW
- SAEGW

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration > Context Configuration > DHCPv6 Service Configuration > DHCPv6 Server Configuration
- `configure > context context_name > dhcpv6-service service_name > dhcpv6-server`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dhcpv6-server)#
```

**Syntax**

```
preferred-lifetime pref_lifetime
```

```
default preferred-lifetime
```

**default preferred-lifetime**

- `default`
  - Returns the command to its default setting of 900.

- `pref_lifetime`
  - Specifies the preferred lifetime (in seconds) for prefixes assigned by the DHCPv6 service.
    - `pref_lifetime` must be an integer value from 1 through 1932100.
    - Default: 900

**Usage**

Use this command to specify the preferred lifetime for prefixes assigned by the DHCPv6 service.

**Example**

The following command configures the preferred lifetime for 1001 seconds:

```
preferred-lifetime 1001
```
prefix-delegation

Configures the lifetime parameters that can be used by a particular DHCPv6 service to allocate delegated prefixes.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > DHCPv6 Service Configuration > DHCPv6 Server Configuration

```bash
configure > context context_name > dhcpv6-service service_name > dhcpv6-server
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dhcpv6-server)#
```

**Syntax**

```bash
prefix-delegation valid-lifetime valid_lifetime preferred-lifetime pref_lifetime
```

**valid-lifetime valid_lifetime**

Specifies the valid lifetime (in seconds) for prefixes for which the delegated prefix is valid. After this is exhausted, delegated prefix is deemed invalid.

- `pref_lifetime` must be an integer value from 1 through 1932100.
- Default: 900

**preferred-lifetime pref_lifetime**

Specifies the preferred lifetime (in seconds) for which new connections can be established by these delegated prefixes. Once it is exhausted, no new connections can be made.

- `pref_lifetime` must be an integer value from 1 through 1932100.
- Default: 900

**Usage**

Use this command to specify the valid and preferred lifetime for prefixes assigned by the DHCPv6 service for prefix delegation.

**Example**

The following command configures the valid lifetime to 1500 seconds and preferred lifetime to 1200 seconds for prefix delegation:

```bash
prefix-delegation valid-lifetime 1500 preferred-lifetime 1200
```
**rebind-time**

Configures the rebind time for prefixes assigned by the DHCPv6 service.

**Product**
GGSN
P-GW
SAEGW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > DHCPv6 Service Configuration > DHCPv6 Server Configuration  
```ruby
configure > context context_name > dhcpv6-service service_name > dhcpv6-server
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dhcpv6-server)#
```

**Syntax**

```
rebind-time  rebind_time

default  rebind-time
```

**default rebind-time**

<table>
<thead>
<tr>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Returns the command to its default setting of 900.</td>
</tr>
</tbody>
</table>

**rebind_time**

<table>
<thead>
<tr>
<th>rebind_time</th>
</tr>
</thead>
</table>
| Specifies the rebind time (in seconds) for prefixes assigned by the DHCPv6 service.  
`rebind_time` must be an integer value from 1 through 1932100.  
Default: 900 |

**Usage**

Use this command to specify the rebind time for prefixes assigned by the DHCPv6 service.

**Example**

The following command configures the rebind time for 1001 seconds:

```
rebind-time 1001
```
renew-time

Configures the renewal time for prefixes assigned by the DHCPv6 service.

### Product
- GGSN
- P-GW
- SAEGW

### Privilege
Security Administrator, Administrator

### Mode
Exec > Global Configuration > Context Configuration > DHCPv6 Service Configuration > DHCPv6 Server Configuration

```
configure > context context_name > dhcpv6-service service_name > dhcpv6-server
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dhcpv6-server)#
```

### Syntax

```
renew-time renewal_time

default renew-time
```

```
default

Returns the command to its default setting of 900.
```

```
renewal_time

Specifies the renewal time (in seconds) for prefixes assigned by the DHCPv6 service.

renewal_time must be an integer value from 1 through 1932100.

Default: 900
```

### Usage
Use this command to specify the renewal time for prefixes assigned by the DHCPv6 service.

### Example

The following command configures the renewal time for 1001 seconds:

```
renew-time 1001
```
valid-lifetime

Configures the valid lifetime for prefixes assigned by the DHCPv6 service.

**Product**
- GGSN
- P-GW
- SAEGW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > DHCPv6 Service Configuration > DHCPv6 Server Configuration

```bash
configure > context context_name > dhcpv6-service service_name > dhcpv6-server
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dhcpv6-server)#
```

**Syntax**

```
valid-lifetime valid_lifetime
default valid-lifetime
```

**default valid-lifetime**

- **default**
  Returns the command to its default setting of 900.

- **valid_lifetime**
  Specifies the valid lifetime (in seconds) for prefixes assigned by the DHCPv6 service.
  `valid_lifetime` must be an integer value from 1 through 1932100.
  Default: 900

**Usage**

Use this command to specify the valid lifetime for prefixes assigned by the DHCPv6 service.

**Example**

The following command configures the valid lifetime for 1001 seconds:

```
valid-lifetime 1001
```
Chapter 108
DHCPv6 Service Configuration Mode Commands

The Dynamic Host Configuration Protocol (DHCP) for Internet Protocol Version 6 (IPv6) Service Configuration Mode is used to create and manage DHCPv6 service instances for the current context.

Mode

Exec > Global Configuration > Context Configuration > DHCPv6 Service Configuration
configure > context context_name > dhcpv6-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-dhcpv6-service)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
bind

Binds the DHCPv6 service to a logical IP interface facilitating the system’s connection to the DHCPv6 server.

Product
GGSN
P-GW
SAEGW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > DHCPv6 Service Configuration

configure > context context_name > dhcpv6-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-dhcpv6-service)#

Syntax

bind address ipv6_address [ port port_number ]

no bind address

no

Removes a previously configured binding.

address ipv6_address

Specifies the IP address of an interface in the current context through which the communication with the DHCPv6 server occurs. ipv6_address must be expressed in IPv6 colon-separated-hexadecimal notation.

port port_number

Specifies the listen port and is used to start the DHCPv6 server bound to it.
port_number must be an integer from 1 through 65535. If unspecified, the default port is 547.

Usage

Use this command to associate or tie the DHCPv6 service to a specific logical IP address previously configured in the current context and bound to a port.

When this command is executed, the DHCPv6 service is started and begins the process of requesting addresses from the DHCPv6 server and storing them in cache memory for allocation to PDP contexts. Only one interface can be bound to a service.

Example

The following command binds the DHCPv6 service to the interface with an IP address of 1234:245:3456:4567:5678:6789:7890:8901:

deadtime

Configures the amount of time that the system waits prior to re-communicating with a DHCPv6 server that was previously marked as down.

**Product**
- GGSN
- P-GW
- SAEGW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > DHCPv6 Service Configuration
`configure > context context_name > dhcpv6-service service_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dhcpv6-service)#
```

**Syntax**

```
deadtime  max_time

default  deadtime
```

```
default
Returns the command to its default setting of 120.
```

```
max_time
Specifies the maximum amount of time (in seconds) to wait before communicating with a DHCPv6 server that was previously unreachable.
`max_time` must be an integer value from 1 through 1932100.
Default: 120
```

**Usage**
If the system is unable to communicate with a configured DHCPv6 server, after a pre-configured number of failures the system marks the server as being down.
This command specifies the amount of time that the system waits prior to attempting to communicate with the downed server.

**Important:** If all DHCPv6 servers are down, the system will immediately treat all DHCPv6 servers as active, regardless of the `deadtime` that is specified.

Refer to the `detect-dead-server` and `max-retransmissions` commands for additional information on the process the system uses to mark a server as down.
The following command configures the system to wait 600 seconds before attempting to re-communicate with a DHCPv6 server that was marked as down:

```
deadtime 600
```
detect-dead-server

Configures the number of consecutive communication failures that could occur before the system marks a DHCPv6 server as down.

Product
- GGSN
- P-GW
- SAEGW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > DHCPv6 Service Configuration

Syntax

detect-dead-server consecutive-failures max_number

default detect-dead-server consecutive-failures

default
Returns the command to its default setting of 5.

consecutive-failures max_number
Specifies the number of failures that could occur before marking a DHCPv6 server as down.
max_number must be an integer from 1 through 1000.
Default: 5

Usage
This command works in conjunction with the max-retransmissions DHCPv6 client command to set a limit to the number of communication failures that can occur with a configured DHCPv6 server. The max-retransmissions DHCPv6 client parameter limits the number of attempts to communicate with a server. Once that limit is reached, the system treats it as a single failure. This parameter limits the number of consecutive failures that can occur before the system marks the server as down and communicate with the server of next highest priority.
If all of the configured servers are down, the system ignores the detect-dead-server configuration and attempts to communicate with the highest priority server again.
If the system receives a message from a DHCPv6 server that was previously marked as down, the system immediately treats it as being active.

Example
The following command configures the system to allow 8 consecutive communication failures with a DHCPv6 server before it marks it as down:
detect-dead-server consecutive-failures 8
**dhcv6-client**

Enters the DHCPv6 Client Configuration Mode.

**Product**
- GGSN
- P-GW
- SAEGW

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration > Context Configuration > DHCPv6 Service Configuration

configure > context context_name > dhcv6-service service_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dhcv6-service)#
```

**Syntax**

```
dhcv6-client
```

**Usage**

Use this command to cause the system to enter the DHCPv6 Client Configuration Mode where parameters are configured for the DHCPv6 client.

Entering this command results in the following prompt:

```
[context_name]host_name(config-dhcv6-client)#
```

DHCPv6 Client Configuration Mode commands are defined in the *DHCPv6 Client Configuration Mode Commands* chapter.
dhcv6-server

Enters the DHCPv6 Server Configuration Mode.

**Product**

GGSN

P-GW

SAEGW

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > DHCPv6 Service Configuration

configure > context context_name > dhcv6-service service_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dhcv6-service)#
```

**Syntax**

```
dhcv6-server
```

**Usage**

Use this command to cause the system to enter the DHCPv6 Server Configuration Mode where parameters are configured for the DHCPv6 server.

Entering this command results in the following prompt:

```
[context_name]host_name(config-dhcv6-service)#
```

DHCPv6 Server Configuration Mode commands are defined in the *DHCPv6 Server Configuration Mode Commands* chapter.

**Important:** Multiple DHCPv6 servers can be configured by entering the `dhcv6-server` command multiple times. A maximum of 3 DHCPv6 servers can be configured.
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**

Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Use this command to return to the parent configuration mode.
server

Configures DHCPv6 servers with which the DHCPv6 service is to communicate and specifies the algorithm used to select DHCPv6 servers with which to communicate when multiple servers are configured.

Product

GGSN
P-GW
SAEGW

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > Context Configuration > DHCPv6 Service Configuration
configure > context context_name > dhcpv6-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-dhcpv6-service)#

Syntax

server { ipv6_address [ priority priority ] | selection-algorithm { first-server | round-robin } }

default server selection-algorithm

no server ipv6_address

default
Uses the first-server algorithm.

no
Deletes a previously configured DHCPv6 server.

ipv6_address
Specifies the IP address of the DHCPv6 server expressed in IPv6 colon-separated-hexadecimal notation.

priority priority
Specifies the priority of the server if multiple servers are configured.
priority is an integer from 1 through 1000. 1 is the highest priority.

selection-algorithm { first-server | round-robin }
Specifies the algorithm used to select DHCPv6 servers with which to communicate when multiple servers are configured.
first-server: Uses the first-server algorithm. This algorithm dictates that the system select the DHCPv6 servers according to their priority, starting with the highest priority server. The system communicates with the server of the next highest priority only when the previous server is unreachable.
Default: Enabled

**round-robin:** Uses the round-robin algorithm. This algorithm dictates that the system communicates with the servers in a circular queue according to the server’s configured priority, starting with the highest priority server. The next request is communicated with the next highest priority server, and so on until all of the servers have been used. At this point, the system starts from the highest priority server.

Default: Disabled

---

**Usage**

Use this command to configure the DHCPv6 server(s) that the system is to communicate with. Multiple servers can be configured, each with their own priority. Up to 20 DHCPv6 servers can be configured. In addition, use this command to determine how configured DHCPv6 servers are utilized by the system.

---

**Important:** If a server is removed, all calls having an IP address allocated from the server will be released.

---

**Example**

The following command configures a DHCPv6 server with an IP address of 1234:245:3456:4567:5678:6789:7890:8901 and a priority of 1:

```
server 1234:245:3456:4567:5678:6789:7890:8901 priority 1
```
Diameter Endpoint Configuration Mode is accessed from the Context Configuration Mode. The base Diameter protocol operation is configured in this mode.

**Mode**

Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

```plaintext
configure > context context_name > diameter endpoint endpoint_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-diameter)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
app-level-retransmission

This command enables/disables setting “T” bit and retaining the same End-to-End Identifier (E2E ID) for application-level retransmissions.

Product
- eHRPD
- GGSN
- P-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration
configure > context context_name > diameter endpoint endpoint_name

Entering the above command sequence results in the following prompt:

[context_name] host_name(config-ctx-diameter)#

Syntax

[ default | no ] app-level-retransmission { retain-e2e | set-retransmission-bit }

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Configures this command with the default setting.</td>
</tr>
<tr>
<td></td>
<td>The default behavior is not to set the retransmission bit for a retried Diameter message.</td>
</tr>
<tr>
<td>retain-e2e</td>
<td>Sends the same End-to-End Identifier for a retried Diameter message.</td>
</tr>
<tr>
<td>set-retransmission-bit</td>
<td>Sets the retransmission bit for retried Diameter messages.</td>
</tr>
</tbody>
</table>

Usage

Use this command to enable application-level transmission with “T” bit set.
'T' bit setting is done only for DIABASE protocol-based rerouting and not for application-based retransmissions. In order to identify such retransmissions, the server expects the T bit to be set at all levels (both DIABASE and application) of retransmission, which can be achieved with this CLI command.
In addition to using this CLI command for setting the T-bit in a retried message, it is also possible to retain the same End-to-End ID. With this feature turned on, the server can detect any duplicate/re-transmitted messages sent by Diameter clients or agents. Note that this feature is applicable to Gy and Rf messages as well.
Similar CLI command for setting T-bit is also present under Credit Control Group configuration mode, which when configured will take effect for Gy messages else endpoint configuration will be used.

Example

The following command specifies to set retransmission bit and retain e2e:

```bash
configure > context context_name > diameter endpoint endpoint_name
set-retransmission-bit
retain-e2e
```
app-level-retransmission set-retransmission-bit retain-e2e
**associate**

This command associates/disassociates a Stream Control Transmission Protocol (SCTP) parameter template with the Diameter endpoint.

**Product**
MME

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

```
configure > context context_name > diameter endpoint endpoint_name
```

Entering the above command sequence results in the following prompt:

```
/context_name/host_name(config-ctx-diameter)#
```

**Syntax**

```
associate sctp-parameters-template template_name

no associate sctp-parameters-template
```

*no*

Disassociates an SCTP parameter template with the Diameter endpoint.

```
sctp-parameters-template template_name
```

Associates a previously created SCTP parameter template with the Diameter endpoint. `template_name` specifies the name for a pre-configured SCTP parameter template. For more information on SCTP parameter templates, refer to the `sctp-param-template` command in the **Global Configuration Mode Commands** chapter.

**Usage**

Use this command to associate a configured SCTP parameter template with the Diameter endpoint. The SCTP parameter template allows for SCTP timer values to be configured for the interface using the Diameter endpoint configuration. For more information on SCTP parameters, refer to the **SCTP Parameter Template Configuration Mode Commands** chapter.

**Important:** Only one SCTP parameter template can be associated with the Diameter endpoint configuration. The SCTP parameter template should be configured prior to issuing this command.

Only the following parameters from the template will be associated with the endpoint. When no SCTP parameter template is associated with the endpoint, the following default values are used:

- `sctp-cookie-life 60000` (default for the parameter template as well)
- `sctp-max-init-retx 5` (default for the parameter template as well)
- `sctp-max-path-retx 10` (default in the parameter template is 5)
- `sctp-rto-initial 3000` (default for the parameter template as well)
- `sctp-rto-max 60000` (default for the parameter template as well)
\texttt{sctp-rto-min} \texttt{1000} (default for the parameter template as well)
\texttt{sctp-sack-period} \texttt{200} (default for the parameter template as well)
\texttt{timeout sctp-heart-beat} \texttt{30} (default for the parameter template as well)

Example

The following command associates a pre-configured SCTP parameter template called \texttt{sctp1} to the Diameter endpoint:

\begin{verbatim}
associate sctp-parameters-template sctp1
\end{verbatim}
Diameter Endpoint Configuration Mode Commands

**cea-timeout**

This command configures the Capabilities-Exchange-Answer (CEA) message timeout duration for Diameter sessions.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

`configure > context context_name > diameter endpoint endpoint_name`

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-ctx-diameter)#`

**Syntax**

`cea-timeout timeout`

`default cea-timeout`

- **default**
  
  Configures this command with the default setting.
  Default: 30 seconds

- **timeout**
  
  Specifies the timeout duration (in seconds) to make the system wait for this duration for a CEA message. `timeout` must be an integer from 1 through 120.

**Usage**

Use this command to configure the CEA timer, i.e., how long to wait for the Capabilities-Exchange-Answer message.

**Example**

The following command sets the Diameter CEA timeout to 16 seconds:

`cea-timeout 16`
connection retry-timeout

This command configures the Diameter Connection Retry Timeout parameter.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

```bash
configure > context context_name > diameter endpoint endpoint_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-diameter)#
```

**Syntax**

```bash
connection retry-timeout timeout

default connection retry-timeout
```

**Usage**

Use this command to configure the Diameter Connection Retry Timeout parameter.

**Example**

The following command sets the Diameter Connection Retry Timer to 120 seconds:

```bash
connection retry-timeout 120
```
connection timeout

This command configures the Diameter Connection Timeout parameter.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

configure > context context_name > diameter endpoint endpoint_name

Entering the above command sequence results in the following prompt:

\[context_name\]host_name(config-ctx-diameter)#

**Syntax**

connection timeout timeout

default connection timeout

**Usage**
Use this command to configure the Diameter Connection Timeout parameter.

**Example**
The following command sets Diameter connection timeout to 16 seconds:

connection timeout 16
**destination-host-avp**

This command controls encoding of the Destination-Host AVP in initial/retried requests.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

```
configure > context context_name > diameter endpoint endpoint_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-diameter)#
```

**Syntax**

```
destination-host-avp { session-binding | always | initial-request | retried-request }
```

```
default destination-host-avp
```

**default**

Configures this command with the default setting. Default: session-binding

**session-binding**

Includes the Destination-Host AVP when the Diameter session is bound with a host.

**always**

Includes the Destination-Host AVP in all types of request messages.

**initial-request**

Includes the Destination-Host AVP in an initial request but not in a retried request.

**retried-request**

Includes the Destination-Host AVP in a retried request but not in an initial request.

**Usage**

Use this command to control encoding of the Destination-Host AVP in initial/retried requests. This command has been introduced in release 12.0, in earlier releases, the Destination-Host AVP is not sent in session-setup/initial request (first message sent on that interface for that subscriber. The message will vary with different interfaces. For example, CCR-Initial for Gy, ACR-start for Rf, and so on). Also, Destination-Host AVP was not sent in retried requests. For example, CCR-Update failed to be responded by server. The message was retransmitted to alternate server. In both these scenarios, it is not known which server will respond to the initial/retried message, so the Destination-Realm is encoded but not the Destination-Host. Only after a response for this message is received...
from one of the hosts present in that realm, the session is considered to be BOUND with that server. Any message sent after this binding will have the Destination-Host AVP encoded. If the application has selected one of the servers using application-level commands like the peer-select command for credit-control or the diameter authentication or accounting server command in a AAA group, encoding of this AVP in initial/retried request is configurable.

**Example**

The following command specifies to include the Destination-Host AVP in initial request but not in retried request:

```
destination-host-avp initial-request
```
device-watchdog-request

This command manages the transport failure algorithm and configures the number of Device Watchdog Requests (DWRs) that will be sent before a connection is closed.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

configure > context context_name > diameter endpoint endpoint_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx-diameter)#

Syntax

device-watchdog-request max-retries retry_count

default device-watchdog-request max-retries

default

Configures this command with the default setting. Default: 1

retry_count

Specifies the maximum number of DWRs, and must be an integer from 1 through 10.

Usage

Use this command to configure the number of DWRs to be sent before closing the connection from a Diameter endpoint.

Example

The following command sets the DWRs to 3:

device-watchdog-request max-retries 3
**dpa-timeout**

This command configures the Disconnect-Peer-Answer (DPA) message timeout duration for Diameter sessions.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

```
configure > context context_name > diameter endpoint endpoint_name
```

Entering the above command sequence results in the following prompt:

```
/context_name/host_name(config-ctx-diameter)#
```

**Syntax**

```
dpa-timeout timeout
```

```
default dpa-timeout
```

- **default**
  Configures this command with the default setting.
  Default: 30 seconds

- **timeout**
  Specifies the DPA message timeout duration (in seconds) as an integer from 1 through 60.

**Usage**

Use this command to set the timer for DPA message timeout during Diameter connection session. This makes the system wait for this duration for DPA message.

**Example**

The following command sets the Diameter DPA timeout to 16 seconds:

```
dpa-timeout 16
```
**dscp**

This command sets the Differential Services Code Point (DSCP) value in the IP header of the Diameter messages sent from the Diameter endpoint.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

`configure > context context_name > diameter endpoint endpoint_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-diameter)#
```

**Syntax**

```
dscp { value | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42
   | af43 | be | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef }
```

**default dscp**

<table>
<thead>
<tr>
<th>value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies to configure a unique DSCP as an integer in the range of 0 through 63.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>af xx</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the use of an assured forwarding xx per hop behavior (PHB).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>be</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the use of best effort forwarding PHB. This is the default.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>cs x</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the use of class selector x per PHB.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ef</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the use of expedited forwarding PHB.</td>
</tr>
</tbody>
</table>

**Usage**

Use this command to set the DSCP in the IP header of the diameter messages sent from the diameter endpoint. In addition to the recommended PHBs the user may configure their own DSCP as an integer in the range of 0 through 63.

**Example**

The following command sets the DSCP to `be`:

```
dscp be
```
**dynamic-peer-discovery**

This command configures the system to dynamically locate peer Diameter servers by means of DNS.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

```
configure > context context_name > diameter endpoint endpoint_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-diameter)#
```

**Syntax**

```
dynamic-peer-discovery [ protocol { sctp | tcp } ]

{ default | no } dynamic-peer-discovery
```

- **default**
  Configures this command with the default setting.
  Default: disabled

- **no**
  Removes the configuration.

- **protocol { sctp | tcp }**
  Configures peer discovery to use a specific protocol. Default: TCP
  **sctp**: Uses Streaming Control Transmission Protocol (SCTP) for peer discovery.
  **tcp**: Uses Transmission Control Protocol (TCP) for peer discovery.

**Usage**

Use this command to configure the system to dynamically locate peer Diameter servers by means of DNS.

Configure the `dynamic-peer-realm` command to locate Diameter servers using Naming Authority Pointer (NAPTR) queries. If the peer realm command is not configured, configuring this command will still allow applications to trigger an NAPTR query on their chosen realms.

The preferred transport protocol is TCP to resolve instances were multiple NAPTR responses with the same priority are received. The one using the TCP transport protocol will be chosen. If the transport protocol is configured through the CLI, then the configured protocol is given preference.

The IP address version will be the same as that of the origin host address configured for the endpoint. For IPv4 endpoints, A-type DNS queries will be sent to resolve Fully Qualified Domain Names (FQDNs). For IPv6 endpoints, AAAA-type queries are sent.

**Example**

The following command configures the system to dynamically locate peer Diameter servers using SCTP:
dynamic-peer-discovery protocol sctp
**dynamic-peer-failure-retry-count**

This command configures the number of times the system will attempt to connect to a dynamically discovered Diameter peer.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

```
configure > context context_name > diameter endpoint endpoint_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-diameter)#
```

**Syntax**

```
dynamic-peer-failure-retry-count no_of_retries
```

**default dynamic-peer-failure-retry-count**

<table>
<thead>
<tr>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configures this command with the default setting.</td>
</tr>
<tr>
<td>Default: 8</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>no_of_retries</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the number of retry attempts to connect to a dynamically discovered Diameter peer. The value must be an integer from 0 through 255.</td>
</tr>
</tbody>
</table>

**Usage**
Use this command to configure the number of times the system attempts to connect to a dynamically discovered Diameter peer.

After the specified number of attempts if the peer is still not open, the peer is moved into blacklist and other peers are tried. The blacklisted peer will be retried after a time period of one hour.

**Example**

The following command sets the retry attempts to 10:

```
dynamic-peer-failure-retry 10
```
**dynamic-peer-realm**

This command configures the name of the realm where peer Diameter servers can be dynamically discovered.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

`configure > context context_name > diameter endpoint endpoint_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-diameter)#
```

**Syntax**

```
[ no ] dynamic-peer-realm realm_name
```

- **no**
  Removes the specified dynamic peer realm name from this endpoint configuration.

- **realm_name**
  Specifies the name of the peer realm where peer Diameter server are to be dynamically discovered.
  *realm_name* must be an existing realm, and must be an alphanumeric string of 1 through 127 characters.

**Usage**

Use this command to locate Diameter servers using Naming Authority Pointer (NAPTR) queries.
Multiple realms can be configured. Even if the `dynamic-peer-discovery` command is not enabled, the realm configuration(s) will trigger dynamic peer discovery on all diabase instances.

**Example**

The following command configures a peer realm, used for dynamic peer discovery, with a name of `service-provider.com`:

```
dynamic-peer-realm service-provider.com
```
**dynamic-route**

This command configures the expiration time for dynamic routes created after a Diameter destination host is reached.

**Product**  
All

**Privilege**  
Security Administrator, Administrator

**Mode**  
Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration  
configure > context context_name > diameter endpoint endpoint_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-diameter)#
```

**Syntax**

```
dynamic-route expiry-timeout value

default dynamic-route expiry-timeout
```

**default dynamic-route expiry-timeout**

**default**

Configures this command with the default setting. Default: 86400 seconds (1 day)

**value**

Specifies the time (in seconds) that a dynamic route to a Diameter host will expire. The value must be an integer from 1 through 86400000.

**Usage**

Use this command to set expiration times for dynamic routes that are set up after a Diameter host has been reached.

**Example**

The following command sets the dynamic route expiration to 43200 seconds:

```
dynamic-route expiry-timeout 43200
```
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Use this command to return to the parent configuration mode.
load-balancing-algorithm

This command configures the behavior for load balancing Diameters peers in the event of a failure of an active server.

Product

All

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

configure > context context_name > diameter endpoint endpoint_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config_CTX-diameter)#

Syntax

load-balancing-algorithm { highest-weight | lowest-weight-borrowing min-active-servers number } default load-balancing-algorithm

default

Configures this command with the default setting.
Default: highest-weight

highest-weight

Selects an idle server with the highest weight in failure scenarios. If multiple servers have the same high weight, load balancing is performed among those servers.

lowest-weight-borrowing min-active-servers number

Borrows an idle server with the lowest weight and adds it to the group of servers where load balancing is performed. number specifies the number of servers that must always be available as active for load balancing. number must be an integer from 2 through 4000.

Usage

Use this command to configure the behavior for load balancing Diameter peers in the event of a failure of an active server.

Example

The following command configures the load balancing behavior for Diameter peers to borrowing minimally active servers (lower weight) and maintaining an active server group of 30 servers:

    load-balancing-algorithm lowest-weight-borrowing min-active-servers 30
max-outstanding

This command configures the maximum number of Diameter messages that any application can send to any one peer, while awaiting responses.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

`configure > context context_name > diameter endpoint endpoint_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-diameter)#
```

**Syntax**

```
max-outstanding messages

{ default | no } max-outstanding

no
Disables the maximum outstanding messages configuration.

default
Configures this command with the default setting.
Default: 256

messages
Specifies the maximum outstanding peer transmit window size setting. The input must be an integer from 1 through 4096.
Note that, in StarOS 14.1 and later releases, though the configuration allows up to 4K Diameter messages, it is restricted to queue up to 512 Diameter messages per peer to avoid any delay in the recovery of Diameter sessions.
```

**Usage**
Use this command to set the unanswered Diameter messages that any application may send to any one peer, while awaiting responses. An application will not send any more Diameter messages to that peer until it has disposed of at least one of those queued messages. It disposes a message by either receiving a valid response or by discarding the message due to no response.

**Example**
The following command sets the Diameter maximum outstanding messages setting to 1024:

```
max-outstanding 1024
```
**origin address**

This command has been deprecated. See the `origin host` and `origin realm` commands.
**origin host**

This command sets the origin host for the Diameter endpoint.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

configure > context context_name > diameter endpoint endpoint_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-diameter)#
```

**Syntax**

```
origin host host_name address ipv4/ipv6_address [ port port_number ] [ accept-incoming-connections ] [ address ipv4/ipv6_address_secondary ]

no origin host host_name address ipv4/ipv6_address [ port port_number ]
```

- **no**
  Removes the origin host configuration.

- **origin host host_name**
  Specifies the host name to bind the Diameter endpoint. `host_name` must be the local Diameter host name. In releases prior to 16.0, the host name must be an alphanumeric string of 1 through 64 characters.

- **address ipv4/ipv6_address**
  Specifies the IP address to bind the Diameter endpoint using IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation. This address must be one of the addresses of a chassis interface configured within the context in which Diameter is configured.

- **port port_number**
  Specifies the port number for the Diameter endpoint (on inbound connections). The port number must be an integer from 1 through 65535. Default: 3868
  Port number in the origin host should be configured only when the chassis is running in server mode, i.e. when `accept-incoming-connections` is configured.
  In this case it will open a listening socket on the specified port. For configurations where chassis is operating as a client, port number should not be included. In this case, a random source port will be chosen for outgoing connections. This is applicable for both with or without multi-homing.

- **Important:** Currently if multi-homing is configured, then the specified port is used instead of randomly chosen port. This is done so that application knows which port is used by the kernel as it will have to use the same port while
adding/removing IP address from the association. Nevertheless, configuring port number in origin host for client mode is not supported.

```
accept-incoming-connections
```

Accepts inbound connection requests for the specified host (enables server mode).

**Important:** MME only: This keyword is not supported. The MME acts only in client mode; setting the S6a (HSS) endpoint to ‘accept-incoming-connections’ will prevent the initialization of the S6a connection to the HSS.

```
address ipv4/ipv6_address_secondary
```

Specifies the secondary bind address for the Diameter endpoint in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation. This address must be one of the addresses of a chassis interface configured within the context in which Diameter is configured.

In 12.3 and earlier releases, when an SCTP association is established and secondary IP addresses are dynamically added or removed, the SCTP connection will be terminated. However, in release 14.0 and later, whenever a secondary IP address is dynamically added or removed from an SCTP association, the affected host notifies its peer of the change in configuration using the Address Configuration Change Chunk (ASCONF) chunk without terminating the SCTP connection.

**Usage**

Use this command to set the bind address for the Diameter endpoint. Diameter agent on the chassis listens to standard TCP port 3868 and also supports the acceptance of any incoming TCP connection from external server.

The command `origin host host-name` must be entered exactly once. Alternatively, the `origin host host-name address ipv4/ipv6_address [ port port_number ]` command may be entered one or more times.

In 12.3 and earlier releases, when two (or more) Diameter endpoints are configured with origin hosts having same origin host name, a failure message “Failure: FAILED due to duplicate entry” is displayed on the CLI console.

In14.0 and later releases, this restriction will no longer be present as it will now allow the user to configure multiple endpoints with the same origin host name. Thus, it allows multiple endpoints (specifically that are used under S6a, S13 and SLg) to share the same Origin Host/Origin Realm.

**Important:** Please be noted it is not possible to associate/map origin-host across endpoints to a specific diamproxy instance or maintain a constant origin host–instance mapping. Origin hosts are a pool of host entries and will be assigned on need basis. Endpoint in itself is an independent encapsulated entity.

**Example**

The following command sets the origin host name to `test` and the IP address to `10.1.1.1`:

```
origin host test address 10.1.1.1
```
origin realm

This command configures the realm to use in conjunction with the origin host.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration
configure > context context_name > diameter endpoint endpoint_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx-diameter)#

Syntax

[ no ] origin realm realm_name

no
Removes the origin realm configuration.

realm_name
Specifies the realm to bind the Diameter endpoint. The realm_name must be an alphanumeric string of 1 through 127 characters. The realm is the Diameter identity. The originator’s realm must be present in all Diameter messages. The origin realm can typically be a company or service name.

Usage
Use this command to set the realm for the Diameter endpoint.
Diameter agent on the chassis listens to standard TCP port 3868 and also supports the acceptance of any incoming TCP connection from external server.

Example
The following command sets the origin realm to companyx:

origin realm companyx
peer

This command specifies a peer address for the Diameter endpoint.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

```
configure > context context_name > diameter endpoint endpoint_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-diameter)#
```

**Syntax**

```
peer [*] peer_name [*] [ realm realm_name ] { address ipv4/ipv6_address [ [ port port_number ] [ connect-on-application-access ] [ send-dpr-before-disconnect disconnect-cause disconnect_cause ] [ sctp ] ] + | fqdn fqdn [ [ port port_number ] [ send-dpr-before-disconnect disconnect-cause disconnect_cause ] [ rlf-template rlf_template_name ] ] } 

no peer peer_name [ realm realm_name ]
```

The Diameter server endpoint can now be a wildcarded peer name (with * as a valid wildcard character). Client peers which satisfy the wild-carded pattern are treated as valid peers and the connection will be accepted. The wildcarded token indicates that the peer name is wildcarded and any '*' in the preceding string is treated as a wildcard.

**realm realm_name**

Specifies the realm of this peer as an alphanumeric string of 1 through 127 characters. The realm name can be a company or service name.

**address ipv4/ipv6_address**

Specifies the Diameter peer IP address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation. This address must be the IP address of the device with which the chassis is communicating.

**fqdn fqdn**

Specifies the Diameter peer FQDN as an alphanumeric string of 1 through 127 characters.
port port_number
Specifies the port number for this Diameter peer. The port number must be an integer from 1 through 65535.

connect-on-application-access
Activates peer on first application access.

send-dpr-before-disconnect
Sends Disconnect-Peer-Request (DPR).

disconnect-cause
Sends Disconnect-Peer-Request to the specified peer with the specified disconnect reason. The disconnect cause must be an integer from 0 through 2, for one of the following:
  • REBOOTING(0)
  • BUSY(1)
  • DO_NOT_WANT_TO_TALK_TO_YOU(2)

rlf-template rlf_template_name
Specifies the RLF template to be associated with this Diameter peer. rlf_template_name must be an alphanumeric string of 1 through 127 characters.

Important: Rate Limiting Function (RLF) is a license-controlled feature. A valid feature license must be installed prior to configuring this feature. Contact your Cisco account representative for more information.

Important: Peer level RLF template takes precedence over the endpoint level template.

sctp
Uses Stream Control Transmission Protocol (SCTP) for this peer.

+
Indicates that more than one of the previous keywords can be entered within a single command.

Usage
Use this command to add a peer to the Diameter endpoint. If the Diameter server side endpoint is catering to multiple peers, there has to be an entry for each peer in the peer list for that endpoint. In cases where the client like GGSN does not use a diameter proxy, the peer list can be as large as the number of session managers on a GGSN. This might lead to a very complex configuration at the Diameter server endpoint. To simplify the configurations, the Diameter server endpoint accepts a wildcarded peer name (with * as a valid wildcard character). The client peers which satisfy the wild-carded pattern are treated as valid peers and the connection will be accepted. The new token ‘wildcarded*’ indicates that the peer name is wildcarded and any ‘*’ in the preceding string should be treated as a wildcard.
For example, if the peer name is prefixed and suffixed with *ggsn* (* wildcard character) and an exact match is not found for the peer name portions peers like 0001-sessmgr.ggsn-gx, 0002-sessmgr.ggsn-gx, will be treated as valid peers at the Diameter server endpoint.

**Example**

The following command adds the peer named *test* with IP address 10.1.1.1 using port 126:

```
peer test address 10.1.1.1 port 126
```
peer-backoff-timer

This command configures the time interval after which the Diameter peer will resume sending CCR-I messages to the PCRF server.

Product
GGSN
HA
P-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

configure > context context_name > diameter endpoint endpoint_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx-diameter)#

Syntax

peer-backoff-timer timeout [ send-app-level-term-req ]

{ default | no } peer-backoff-timer

| default | no |
|----------------|
| Removes the configured peer backoff timer from Diameter endpoint configuration. Default value of peer-backoff-timer is 7 seconds. |

<table>
<thead>
<tr>
<th>timeout</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the peer backoff timeout duration in seconds, and must be an integer from 1 through 3600.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>send-app-level-term-req</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sends termination request from application irrespective of whether or not the peer-backoff-timer is running.</td>
</tr>
</tbody>
</table>

Usage
Use this command to configure a peer backoff timer which will be started when the server (primary or secondary PCRF) is busy. That is, the backoff-timer is started when the result code DIAMETER_TOO_BUSY (3004) is received from the PCRF. This PCRF is then marked as unavailable for the period configured by the backoff timer.
No CCR-I messages will be sent to the server until this timer expires. This timer will be per session manager level and will be applicable only to that instance.

Example
The following command sets the peer backoff timeout to 20 seconds:

    peer-backoff-timer 20
reconnect-timeout

This command configures the time interval after which the Diameter peer will be reconnected automatically when DO_NOT_WANT_TO_TALK_TO_YOU disconnect cause is received.

Product
GGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration
configure > context context_name > diameter endpoint endpoint_name

Entering the above command sequence results in the following prompt:

<context_name>host_name(config-ctx-diameter)#

Syntax

reconnect-timeout timeout

no reconnect-timeout

no

Disables auto reconnect of peer after receiving the disconnect cause "DO_NOT_WANT_TO_TALK_TO_YOU".
The default configuration is no reconnect-timeout. The connection to peer will not be retried until it is enabled by the administrator using the diameter enable endpoint command in the Exec mode.

timeout

Specifies the reconnect timeout duration in seconds, and must be an integer from 30 through 86400.

Usage

Use this command to configure a timer which is started at the reception of the "DO_NOT_WANT_TO_TALK_TO_YOU" disconnect cause from the Diameter peer in Disconnect-Peer-Request message. After the timer expiry, the Diameter endpoint will automatically try to reconnect to the disconnected peer.
Currently in the system, the "DO_NOT_WANT_TO_TALK_TO_YOU" in the disconnect peer request is treated as an admin disable. Hence when the system gets into this state the connection will not be retried and the connection must be enabled by the administrator using the diameter enable endpoint command in the Exec mode.

Example

The following command sets the reconnect timeout to 100 seconds:

reconnect-timeout 100
response-timeout

This command configures the Response Timeout parameter. Response timeout specifies the maximum allowed response time for request messages sent from Diameter applications to Diameter server. On failure of reception of response for those request message within this specified time, this will be handled as failure by the corresponding applications and appropriate failure action will be initiated.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

```bash
configure > context context_name > diameter endpoint endpoint_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-diameter)#
```

Syntax

```
response-timeout timeout

default response-timeout
```

```
default

  Configures this command with the default setting.
  Default: 60 seconds
```

```
timeout

  Specifies the response timeout duration in seconds, and must be an integer from 1 through 300.
```

Usage

Use this command to configure the Response Timeout parameter.

Example

The following command sets the response timeout to 100 seconds:

```
response-timeout 100
```
rlf-template

This command configures the RLF template to be used for the Diameter endpoint for throttling and rate control.

Important: RLF template cannot be deleted if it is bound to any application (peers/endpoints).

Product
GGSN
P-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration
configure > context context_name > diameter endpoint endpoint_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx-diameter)#

Syntax

[ no ] rlf-template rlf_template_name

no

Remove the specified RLF template from global configuration.

Important: Do not use “no rlf-template rlf_template_name” in endpoint configuration mode. This CLI attempts to delete the specified RLF template. This CLI is part of global configuration, and not endpoint configuration.

rlf_template_name

The name of the RLF template to be used for Diameter endpoint configuration. rlf_template_name must be an alphanumeric string of 1 through 127 characters.

Usage

Use this command to configure the RLF Template to be used for the Diameter endpoint for throttling and rate control. This CLI command should be defined in the Diameter endpoint application to enable RLF module.

Important: Rate Limiting Function (RLF) is a license-controlled feature. A valid feature license must be installed prior to configuring this feature. Contact your Cisco account representative for more information.

Important: This CLI command takes effect only if the RLF template is defined in the Global Configuration mode and the connection to the peer is open.
Currently in the deployment of the Diameter applications (Gx, Gy, etc.), many operators make use of “\texttt{max-outstanding \ <number>\}” as a means of achieving some rate-limiting on the outgoing control traffic. With RLF in place, this is no longer required since RLF takes care of rate-limiting in all cases. If RLF is used and \texttt{max-outstanding} is also used, there might be undesirable results.

\textbf{Important:} If RLF is being used with an ”\texttt{diameter endpoint}, then set the \texttt{max-outstanding} value of the peer to be 255.

RLF provides only the framework to perform the rate limiting at the configured Transactions Per Second (TPS). The applications (like Diameter) should perform the configuration specific to each application. For more information on this feature, refer to the \texttt{rlf-template} command in the Global Configuration Mode Commands chapter. For more information on RLF template configuration commands, refer to the RLF Template Configuration Mode Commands chapter.

\textbf{Example}

The following command configures an RLF template named \texttt{rlf_1} for Diameter endpoint:

\begin{verbatim}
rlf-template rlf_1
\end{verbatim}
route-entry

This command creates an entry in the route table for Diameter peer.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

configure > context context_name > diameter endpoint endpoint_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx-diameter)#

Syntax

route-entry { [ host host_name ] [ peer peer_id [ weight priority ] ] [ realm realm_name [ application credit-control peer peer_id ] [ weight value ] | peer peer_id [ weight value ] ] }

no route-entry { [ host host_name ] [ peer peer_id ] [ realm realm_name [ application credit-control peer peer_id | peer peer_id ] ] }

no
Disables the specified route-entry table configuration.

host host_name
Specifies the Diameter server’s host name as an alphanumeric string of 1 through 63 characters.

realm realm_name
Specifies the realm name as an alphanumeric string of 1 through 127 characters. The realm may typically be a company or service name.

application credit-control
Specifies the credit control application — DCCA or RADIUS.

peer peer_id
Specifies the peer ID of the Diameter endpoint route as an alphanumeric string of 1 through 63 characters.

weight priority
Specifies the priority for a peer in the route table as an integer from 0 through 255. Default: 10
The peer with the highest weight is used. If multiple peers have the highest weight, selection is by round-robin mechanism.
**Usage**

Use this command to create a route table for Diameter application. When a Diameter client starts to establish a session with a realm/application, the system searches the route table for the best match. If an entry has no host specified, the entry is considered to match the requested value. Similarly, if an entry has no realm or application specified, the entry is considered to match any such requested value. The best match algorithm is to prefer specific matches for whatever was requested, either realm/application or host/realm/application. If there are no such matches, then system looks for route table entries that have wildcards.

If the message’s destination realm is `abc.com` then the message will be routed to `peer1`. If the message’s destination realm is `def.com` then the message will be routed to `peer2`. If the destination realm is `xyz.com` then the message will be routed to “peer-default”.

**Example**

The following command creates a route entry with the host name `dcca_host1` and peer ID `dcca_peer` with priority weight of `10`:

```
route-entry host dcca_host1 peer dcca_peer weight 10
```
route-failure

This command controls what action is performed for the route table after failure or recovery after failure.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

configure > context context_name > diameter endpoint endpoint_name

Entering the above command sequence results in the following prompt:

```
[context_name] host_name(config-ctx-diameter)#
```

**Syntax**

```
route-failure { deadtime seconds | recovery-threshold percent percentage | result-code result_code | threshold counter }

default route-failure { deadtime | recovery-threshold | threshold }

no route-failure result-code result_code
```

---

**Syntax**

```
no
```

Disables the route-failure configuration.

---

**Syntax**

```
default
```

Configures the default setting for the specified parameter.

---

**Syntax**

```
deadtime seconds
```

Specifies the time duration (in seconds) for which the system keeps the route in FAILED status. When this time expires, the system changes the status to AVAILABLE.

seconds must be an integer from 1 through 86400. Default: 60

---

**Syntax**

```
recovery-threshold percent percentage
```

Specifies the percentage value at which the failure counter is reset when provisionally changing the status from FAILED to AVAILABLE.

For example, if a failure counter of 16 caused the status to change to FAILED. After the configured deadtime expires, the status changes to AVAILABLE. If this keyword is configured with 75 percent, the failure counter will be reset to 12 (75 percent of 16).

percentage must be an integer from 1 through 99. Default: 90

---

**Syntax**

```
result-code result_code
```

Configures which answer messages are to be treated as failures, in addition to requests that time out. Up to 16 different result codes can be specified.

result_code must be an integer from 0 through 4294967295.
threshold counter

Configures the number of errors that causes the status to become FAILED. The counter value must be an integer from 0 through 4294967295. Default: 16
The error counter begins at zero, and whenever there is a good response it decrements (but not below zero) or increments (but not above this threshold).

Usage

Use this command to control how failure/recovery is performed for the route table. After a session is established, it is possible for the session to encounter errors or Diameter redirection messages that cause the Diameter protocol to re-use the route table to switch to a different route.
Each Diameter client within the chassis maintains counters relating to the status of each of its connections to different hosts (when the destination is realm/application without a specific host, the host name is kept as “”, i.e., blank).
Moreover, those counters are further divided according to which peer is used to reach each host. Each Diameter client maintains a status of each peer-to-host combination. Under normal good conditions the status will be AVAILABLE, while error conditions might cause the status to be FAILED.
Only combinations that are AVAILABLE will be used. If none are AVAILABLE, then system attempts the secondary peer if failover is configured and system can find an AVAILABLE combination there. If nothing is AVAILABLE, the system uses a FAILED combination.

Example

The following command configures the time duration for route failure to 90 seconds:

    route-failure deadtime 90
server-mode

This command configures the Diameter endpoint to establish the system as the server side endpoint of the connection.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

```bash
configure > context context_name > diameter endpoint endpoint_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-diameter)#
```

**Syntax**

```bash
server-mode [ demux-mode ]
```

**demux-mode**

Specifies that the Diameter proxy is to use the demux manager to identify the appropriate session manager. If this keyword is not enabled, the proxy will route the request directly to a session manager.

**Usage**

Use this command to configure the Diameter endpoint to establish this system as the server side endpoint of the connection. When the Diameter proxy receives an incoming request, the proxy identifies the endpoint for the request. If the system is in client mode, the proxy extracts the instance ID of the session manager which serves as the session-ID of the request. If this command is enabled, the extraction of the instance ID is disabled.

**Example**

The following command sets the system as the server side of the Diameter endpoint and instructs the Diameter proxy to use the demux manager to identify the appropriate session manager where the request is to be routed:

```bash
server-mode demux-mode
```
tls

This command enables/disables the Transport Layer Security (TLS) support between a Diameter client and Diameter server node.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

```plaintext
configure > context context_name > diameter endpoint endpoint_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-diameter)#
```

**Syntax**

```
tls { certificate certificate | password password | privatekey private_key }
```

**default tls**

- **default**
  Disables the TLS support at Diameter endpoint.

- **certificate certificate**
  Specifies the certificate for TLS support. The certificate must appear encrypted, and must be an alphanumeric string of 700 through 900 characters.

- **password password**
  Specifies the password for TLS support. The password must be encrypted, and must be an alphanumeric string of 6 through 50 characters.

- **privatekey private_key**
  Specifies the private key for TLS support. The private key must be encrypted, and must be an alphanumeric string of 900 through 1500 characters.

**Usage**

Use this command to configure TLS support between a Diameter client and Diameter server node. By default, TLS is disabled.

**Important:** Both the Diameter client and server must be configured with TLS enabled or TLS disabled; otherwise, the Diameter connection will be rejected.

**Example**

The following commands enable the TLS between a Diameter client and Diameter server node:
Diameter Endpoint Configuration Mode Commands

tls certificate "-----BEGIN CERTIFICATE-----
\nMIICdyAwIBAgIQC1mRcWN5ZgIwRQYDMBQGCCsGAQUFBwEB\n\n-----END CERTIFICATE-----"

tls privatekey BEGIN RSA PRIVATE KEY-----
\nProc-Type: 4,ENCRYPTED
\nDEK-Info: DES-EDE3-CBC,5772A2A7BE34B611\n\n-----END RSA PRIVATE KEY-----"

tls password TLSpassword_3B167E
**use-proxy**

This command enables/disables Diameter proxy for the Diameter endpoint. By default this command is disabled.

**Product**
IPCF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

```configure > context context_name > diameter endpoint endpoint_name```

Entering the above command sequence results in the following prompt:

```[context_name]host_name(config-ctx-diameter)#```

**Syntax**

```
use-proxy [ server-mode [ demux-mode ] ]
```

**no use-proxy**

```
no
```

Disables Diameter proxy for the current endpoint. This command at endpoint level will equip an application to use Diameter proxy to route all its messages to an external peer.

```
server-mode
```

Specifies that the Diameter endpoint to establish the Diameter proxy as the server side endpoint of the connection.

```
demux-mode
```

Specifies that the Diameter endpoint to establish the Diameter proxy to use the Demux manager to identify the appropriate session manager. If this keyword is not enabled, the proxy will route the request directly to a session manager.

IPCF uses BindMux to identify the appropriate session manager.

**Usage**

Use this command to establish a Diameter proxy to route all its messages to an external peer. The proxy acts as an application gateway for Diameter. It gets the configuration information at process startup and decides which Diameter peer has to be contacted for each application. It establishes the peer connection upon finding no peer connection already exists.

IPCF uses Bindmux as a Demux manager to help distribute new incoming sessions across available Sessmgrs on the system.

All the incoming Diameter requests/responses land on Diamproxy. Diamproxy checks if a Sessmgr is already serving this session based on parameters like session-id and peer-id of the request/response.

If no Sessmgr is allocated to the request and the Demux mode is ON, the DiamProxy forwards the new request to Demux/Bindmux for sessmgr allocation. Demux/Bindmux has updated information about the load...
on all the Sessmgrs and assigns the optimal Sessmgr to the Diameter session. Once a Sessmgr is allocated for the session, a mapping of session-id to Sessmgr is added at Diamproxy. All further requests for this session will be directly routed to Sessmgr.

Each proxy task will automatically select one of the host names configured with the `origin host` command. Multiple proxy tasks will not use the same host names, so there should be at least as many host names as proxy tasks. Otherwise, some proxy tasks will not be able to perform Diameter functionality. The chassis automatically selects which proxy tasks are used by which managers (i.e., ACSMgrs, Sessmgrs), without verifying whether the proxy task is able to perform Diameter functionality.

To be able to run this command, the Diameter proxy must be enabled. In the `Global Configuration Mode Commands` chapter, see the description of the `require diameter-proxy` command.

**Example**

The following command enables Diameter proxy for the current endpoint:

```plaintext
use-proxy
```

The following command disables Diameter proxy for the current endpoint:

```plaintext
no use-proxy
```
vsa-support

This command allows DIABASE to use vendor IDs configured in the dictionary for negotiation of the Diameter peers’ capabilities regardless of the supported vendor IDs received in Capabilities-Exchange-Answer (CEA) messages.

Product

GGSN
PDSN

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

configure > context context_name > diameter endpoint endpoint_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx-diameter)#

Syntax

vsa-support { all-from-dictionary | negotiated-vendor-ids }

default vsa-support

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Configures this command with the default setting. Default: negotiated-vendor-ids</td>
</tr>
<tr>
<td>all-from-dictionary</td>
<td>Allows DIABASE to use the vendor IDs from the dictionary as indicated in the Capabilities-Exchange-Request (CER) messages from Diameter peers.</td>
</tr>
<tr>
<td>negotiated-vendor-ids</td>
<td>Allows DIABASE to use the supported vendor IDs satisfying capability negotiation.</td>
</tr>
</tbody>
</table>

Usage

Use this command to set DIABASE to use the vendor IDs from the dictionary or use the vendor IDs satisfying the capabilities negotiation.

Example

The following command enables DIABASE to use the vendor IDs specified in the dictionary:

vsa-support all-from-dictionary
**watchdog-timeout**

This command configures the Watchdog Timeout parameter.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Diameter Endpoint Configuration

```
configure > context context_name > diameter endpoint endpoint_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-diameter)#
```

**Syntax**

```
watchdog-timeout timeout
```

```
{ default | no } watchdog-timeout
```

- **no**
  Disables the watchdog timeout configuration.

- **default**
  Configures this command with the default setting.
  Default: 30 seconds

- **timeout**
  Specifies the timeout duration (in seconds) as an integer from 6 through 30.

**Usage**

Use this command to configure the Watchdog Timeout parameter for the Diameter endpoint. If this timer expires before getting a response from the destination, other route to the same destination is tried, as long as the retry count setting has not exceeded (see the device-watchdog-request CLI command) and as long as the response timer has not expired (see the response-timeout CLI command).

**Example**

The following command sets the watchdog timeout setting to 15 seconds:

```
watchdog-timeout 15
```
Chapter 110
Diameter Failure Handling Template Configuration Mode Commands

Diameter Failure Handling Template Configuration Mode is accessed from the Global Configuration Mode. This mode allows an operator to configure failure handling template that can be associated to different Diameter services.

Mode

Exec > Global Configuration > Failure Handling Template Configuration

configure > failure-handling-template template_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-fh-template)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Use this command to return to the parent configuration mode.
**msg-type**

This command specifies the failure handling behavior in the event of a communication failure with the prepaid server.

**Product**

GGSN
HA
HSGW
IPSG
PDSN
P-GW
S-GW
SAEGW

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Failure Handling Template Configuration

`configure > failure-handling-template template_name`

Entering the above command sequence results in the following prompt:

`[local]host_name(config-fh-template)#`

**Syntax**

```
msg-type { any | authentication info request | authorization-request | check-identity-request | credit-control-initial | credit-control-terminate | credit-control-update | eap-request | eap-termination-request | notify-request | profile-update-request | purge-ue-request | update-location-request | user-data-request } failure-type { any | diabase-error | diameter result-code { any-error | result-code [ to end-result-code ] } |
                   diameter exp-result-code { any-error | result-code [ to end-result-code ] } | resp-timeout | tx-expiry } action { continue [ local-fallback | retry-server-on-event | send-csr-t-on-call-termination | without-retry ] | retry-and-terminate [ without-term-req ] |
                terminate [ without-term-req ] }
```

```
no msg-type { any | authentication info request | authorization-request | check-identity-request | credit-control-initial | credit-control-terminate | credit-control-update | eap-request | eap-termination-request | notify-request | profile-update-request | purge-ue-request | update-location-request | user-data-request } failure-type { any | diabase-error | diameter result-code { any-error | result-code [ to end-result-code ] } |
               diameter exp-result-code { any-error | result-code [ to end-result-code ] } | resp-timeout | tx-expiry }
```

```
no
```

Removes the configuration associated with the failure handling template.
Diameter Failure Handling Template Configuration Mode Commands

```c
{ any | authentication-info-request | authorization-request | check-identity-request | credit-control-initial | credit-control-terminate | credit-control-update | eap-request | eap-termination-request | notify-request | profile-update-request | purge-ue-request | update-location-request | user-data-request }
```

Defines the failure handling behavior based on the failures in the following request messages:

- Any request
- Authentication-Information Request through S6a or S13 Diameter interface
- Authorization Request through PDIF-EAP, STA, S6b, or WM interface
- Check-Identity-Information-Request through S6a or S13 interface
- Credit-Control-Initial-Request (CCR-I) through GX, GY or TY interface
- Credit-Control-Terminate-Request (CCR-T) through GX, GY or TY interface
- Credit-Control-Update-Request (CCR-U) through GX, GY or TY interface
- EAP request through Cx, PDIF-EAP, STA, S6b, or WM interface
- EAP Termination request through Cx, PDIF-EAP, STA, S6b, or WM interface
- Notify-Request through S6a or S13 interface
- Profile-Update-Request through SH interface
- Purge-UE-Request through S6a or S13 interface
- Update-Location-Request through S6a or S13 interface
- User-Data-Request through SH interface

```c
failure-type { any | diabase-error | diameter-result-code { any-error | result-code [ to end-result-code ] } | diameter-exp-result-code { any-error | result-code [ to end-result-code ] } | resp-timeout | tx-expiry }
```

Defines the failure handling behavior based on the different types of failure, for example, Diabase error or any error due to expiry of response timeout or Tx timer, etc.

`result-code [ to end-result-code ]`: result-code specifies the result code number, must be an integer from 3000 through 9999. end-result-code specifies the upper limit of a range of result codes. end-result-code must be greater than result-code.

```c
```

Configures the action to be taken in the event of a communication failure with the server from one of the following:

- `continue` – In the event of a failure the user session continues. DCCA/Diameter will make periodic request and/or connection retry attempts and/or will attempt to communicate with a secondary peer depending on the peer config and session-binding setting.
  
  - `local-fallback` – Continue the session with the PCC rules defined in the local policy.
  - `retry-server-on-event` – Reconnects to PCRF server on update and termination requests or re-authorization from server, for failure-handling CONTINUE sessions.

**Important:** This option is valid only for credit-control-update request though it is allowed to configure for all the requests.
Diameter Failure Handling Template Configuration Mode Commands

- **send-ccrt-on-call-termination** – Sends CCR-T to PCRF on call termination for failure-handling CONTINUE.

**Important:** This option is valid only for credit-control-update request though it is allowed to configure for all the requests.

- **without-retry** – Continue the session without retrying to the secondary PCRF.
- **retry-and-terminate** – In the event of a failure the user session continues for the duration of one retry attempt with the server. If this retry attempt also fails, the session is terminated.
- **without-term-req** – Terminate the session without sending the termination request (CCR-T).
- **terminate** – In the event of a failure the user session is terminated.
- **without-term-req** – Terminate the session without sending the termination request (CCR-T).

**Usage**

Use this command to specify the behavior in the event of a communication failure with the prepaid server. If there are different failure handling configurations present within the template for the same message type, the action is applied as per the latest error encountered.

Lookup is done first to identify if there is an exact match for **message-type** and **failure-type**. If not present, lookup is done for 'any' match for message and failure type.

That is, when there are multiple matches, it is preferred to find a match to a specifically configured value over a match to something configured with **any** or **any-error**. If there are multiple best matches, the one with a specifically configured **msg-type** over a match to **msg-type any** is preferred.

There are two levels of possible communication failure:

- The TCP connection failed
- DIAMETER routing failed to deliver a request or failed to receive a response.

The specified behavior is used for sessions when no behavior is specified by the server, such as by the CC-Failure-Handling AVP in DIAMETER messages. This command may be entered once for each type of message.

The following are the default action for Diameter result codes:

- For all protocol error codes 3000 to 3999, the default action is **terminate**. For all transient error codes 4000, 4001, 4004 to 4180, and 4182 to 4999, the default action is **continue**.
- For transient error codes 4002, 4003, and 4181, the default action is retry-and-terminate.
- For error code 4001, the default action is **terminate**.
- For permanent error codes 5000 to 5999, the default action is **terminate**.

**Example**

The following command configures to terminate the session when the Diameter application encounters a failure due to Diabase error in the Credit-Control Initial Request (CCR-I) message:

```plaintext
msg-type credit-control-initial failure-type diabase-error action terminate
```
Chapter 111
Diameter Host Select Configuration Mode Commands

Diameter Host Select Configuration Mode is accessed from the Global Configuration Mode. This mode allows an operator to configure Diameter host tables of peer servers that can be shared by different services.

Mode

Exec > Global Configuration > Diameter Host Select Configuration

configure > diameter-host-template template_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-host-template)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Use this command to return to the parent configuration mode.
host-select row-precedence

This command configures individual rows of peer servers within the Diameter host table.

Product

GGSN
HA
HSGW
IPSG
PDSN
P-GW
SCM
SAEGW
S-GW

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > Diameter Host Select Configuration
configure > diameter-host-template template_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-host-template)#

Syntax

In StarOS 14.1 and earlier releases:

host-select row-precedence precedence table { 1 | 2 } host host_name [ realm realm_id ] [ secondary host sec_host_name realm sec_realm_id ] [ -noconfirm ]

host-select row-precedence precedence table prefix-table { 1 | 2 } msisdn-prefix-from msisdn-prefix-to host host_name [ realm realm_id ] [ secondary host sec_host_name realm sec_realm_id ] [ -noconfirm ]

no host-select row-precedence precedence table { 1 | 2 | prefix-table { 1 | 2 } } [ -noconfirm ]

In StarOS 15.0 and later releases:

host-select row-precedence precedence table { 1 | 2 } host host_name [ realm realm_id ] [ secondary host sec_host_name realm sec_realm_id ] [ -noconfirm ]

host-select row-precedence precedence table { { range-table { 1 | 2 } { imsi-based { [ prefix | suffix ] imsi-value [ to imsi-value ] } | msisdn-based { [ prefix | suffix ] msisdn-value [ to msisdn-value ] } } host host_name [ realm realm_id ] [ secondary host sec_host_name realm sec_realm_id ] algorithm { active-standby | round-robin } } } [ -noconfirm ]
no host-select row-precedence precedence table { 1 | 2 | range-table { 1 | 2 } } [ -noconfirm ]

no
Removes the specified row from the primary or secondary table or primary/secondary MSISDN prefix table for 14.0 and earlier releases, or IMSI/MSISDN range table for 15.0 and later releases.

row-precedence precedence
Specifies the row in the table as an integer from 1 through 128. Note that the row precedence number in IMSI/MSISDN configuration must be unique.

Important: In StarOS release 14.0 and later, precedence may be an integer from 1 through 256 for SCM.

table { 1 | 2 }
Specifies the Diameter host table that will be edited.

• 1: Specifies the primary table
• 2: Specifies the secondary table

table prefix-table { 1 | 2 } msisdn-prefix-from msisdn_prefix_from msisdn-prefix-to msisdn_prefix_to host host_name [ realm realm_id ] [ secondary host sec_host_name realm sec_realm_id ]

Important: This command syntax is applicable to StarOS release 14.1 and earlier.

prefix-table { 1 | 2 }: Specifies a primary or secondary table containing ranges of MSISDN prefixes.
msisdn-prefix-from msisdn_prefix_from msisdn-prefix-to msisdn_prefix_to: Specifies the starting and ending Mobile Station International Subscriber Directory Number (MSISDN) prefixes for a row in the prefix-table.
host host_name: Identifies the primary Diameter peer server to be added to this row by its host name. host_name can be entered as an IP address or a DNS hostname (1 through 128 alphanumeric characters).
secondary host host_name: Identifies the secondary Diameter peer server to be added to this row by its host name. host_name can be entered as an IP address or a DNS hostname (1 through 128 alphanumeric characters).
realm realm_id: Specifies an optional realm ID as an alphanumeric string of 1 through 128 characters.

Important: This command syntax is applicable to StarOS release 15.0 and later.

range-table { 1 | 2 }: Specifies a primary or secondary table containing ranges of IMSI or MSISDN prefix/suffix.
imsi-based { [ prefix | suffix ] imsi-value [ to imsi-value ] } msisdn-based { [ prefix | suffix ] msisdn-value [ to msisdn-value ] } host host_name [ realm realm_id ] [ secondary host sec_host_name realm sec_realm_id ] algorithm { active-standby | round-robin } ]

Important: This command syntax is applicable to StarOS release 15.0 and later.

range-table { 1 | 2 }: Specifies a primary or secondary table containing ranges of IMSI or MSISDN prefix/suffix.
imsi-based { [ prefix | suffix ] imsi-value [ to imsi-value ] } msisdn-based { [ prefix | suffix ] msisdn-value [ to msisdn-value ] } host host_name [ realm realm_id ] [ secondary host sec_host_name realm sec_realm_id ] algorithm { active-standby | round-robin } ]

Important: This command syntax is applicable to StarOS release 15.0 and later.

range-table { 1 | 2 }: Specifies a primary or secondary table containing ranges of IMSI or MSISDN prefix/suffix.
imsi-based { [ prefix | suffix ] imsi-value [ to imsi-value ] } msisdn-based { [ prefix | suffix ] msisdn-value [ to msisdn-value ] } host host_name [ realm realm_id ] [ secondary host sec_host_name realm sec_realm_id ] algorithm { active-standby | round-robin } ]

Important: This command syntax is applicable to StarOS release 15.0 and later.

range-table { 1 | 2 }: Specifies a primary or secondary table containing ranges of IMSI or MSISDN prefix/suffix.
imsi-based { [ prefix | suffix ] imsi-value [ to imsi-value ] } msisdn-based { [ prefix | suffix ] msisdn-value [ to msisdn-value ] } host host_name [ realm realm_id ] [ secondary host sec_host_name realm sec_realm_id ] algorithm { active-standby | round-robin } ]

Important: This command syntax is applicable to StarOS release 15.0 and later.
**host-select row-precedence**

```plaintext
msisdn-based { [ prefix | suffix ] } msisdn-value [ to msisdn-value]: Specifies to use the prefix/suffix/range values of MSISDN of the subscriber for Diameter peer selection.
host host_name: Identifies the primary Diameter peer server to be added to this row by its host name.
host_name can be entered as an IP address or a DNS hostname (1 through 128 alphanumeric characters).
secondary host host_name: Identifies the secondary Diameter peer server to be added to this row by its host name. host_name can be entered as an IP address or a DNS hostname (1 through 128 alphanumeric characters).
realm realm_id: Specifies an optional realm ID as an alphanumeric string of 1 through 128 characters.
algorithm { active-standby | round-robin }: Specifies to select the algorithm to pick the primary and the secondary hosts either in an active standby mode or in round robin fashion.
[ -noconfirm ]
Executes the command without prompting for further input from the user.
```

**Usage**

Use this command to add or modify individual rows in Diameter host server tables. Each table may contain up to 256 rows.
In Releases 15.0 and later, the existing CLI command “host-select row-precedence” in the Diameter Host Template Configuration mode is modified to enable the selection of Diameter peer based on the configured prefix/suffix/range values of IMSI or MSISDN of subscriber. This configuration change allows the overlapping range of IMSI or MSISDN values.
PCRF peer selection is based on the first match of prefix/suffix/range on row precedence priorities. If the subscriber's IMSI/MSISDN does not match with any configured IMSI/MSISDN range, then IMS Authorization application selects the default peer.

**Important:** The length of IMSI or MSISDN range is same in any IMSI or MSISDN host template configuration list.

Once a row is selected the failure handling for the subscriber is done based on this configuration. With this feature being turned on, the primary and the secondary hosts configured can be picked up in an active standby mode or in round robin fashion.

**Example**

The following command adds a row to a Diameter peer server table with the following parameters:
- row (precedence) = 1
- table = 1 (primary)
- Diameter peer server hostname = minid
- realm = namerica

```
host-select row-precedence 1 table 1 host minid realm namerica
```
**host-select table**

This command configures a table of peer servers associated with the Diameter host template.

**Product**
- GGSN
- HA
- HSGW
- IPSG
- PDSN
- P-GW
- SCM
- SAEGW
- S-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Diameter Host Select Configuration

```
configure > diameter-host-template template_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-host-template)#
```

**Syntax**

In StarOS 14.1 and earlier releases:

```
host-select table { 1 | 2 | prefix-table { 1 | 2 } } algorithm { ip-address-modulus [ prefer-ipv4 | prefer-ipv6 ] | msisdn-modulus | round-robin }
```

```
no host-select table
```

In StarOS 15.0 and later releases:

```
host-select table { 1 | 2 | range-table { 1 | 2 } } algorithm { ip-address-modulus [ prefer-ipv4 | prefer-ipv6 ] | msisdn-modulus | round-robin }
```

```
no host-select table
```

```
no
```

Removes the table associated with the Diameter host template.

```
table { 1 | 2 | prefix-table { 1 | 2 } }
```

---

**Important:** This command syntax is applicable to StarOS release 14.1 and earlier.
Specifies the Diameter host table that will be edited.

- **1**: Specifies the primary table
- **2**: Specifies the secondary table

**prefix-table { 1 | 2 }**: Specifies a primary or secondary table containing ranges of MSISDN prefixes.

This keyword option enables activating the configured table.

```plaintext
table { 1 | 2 | range-table { 1 | 2 } }
```

**Important**: This command syntax is applicable to StarOS release 15.0 and later.

Specifies the Diameter host table that will be edited.

- **1**: Specifies the primary table
- **2**: Specifies the secondary table

**range-table { 1 | 2 }**: Specifies a primary or secondary table containing ranges of IMSI or MSISDN prefix/suffix.

This keyword option enables activating the configured table.

```plaintext
algorithm { ip-address-modulus [ prefer-ipv4 | prefer-ipv6 ] | msisdn-modulus | round-robin }
```

Specifies the algorithm to be used when selecting a row in this table.

- **ip-address-modulus**: Use an IP address (in binary) to select a row.
  - **prefer-ipv4**: If both IPv4 and IPv6 addresses are available, use the IPv4 address.
  - **prefer-ipv6**: If both IPv4 and IPv6 addresses are available, use the IPv6 address.

- **msisdn-modulus**: Use an MSISDN (without leading “+”) to select a row.
- **round-robin**: Select a row in round-robin manner for each new session.

**Important**: The Round Robin algorithm is effective only over a large number of selections, and not at a granular level.

**Usage**

Use this command to add or modify a Diameter host server table associated with a Diameter host template.

**Example**

The following command adds a primary table that uses the `ip-address-modulus` algorithm for selecting a row:

```plaintext
host-select table 1 algorithm ip-address-modulus
```
Chapter 112
DLCI Configuration Mode Commands

The DLCI configuration mode provides the commands to configure, bind and manage the DLCI associated with a specific port defined in the parent configuration mode, Channelized Port configuration mode.

Mode

Exec > Global Configuration > Channelized Port Configuration > DLCI Configuration

configure > port channelized slot_number/port_number > dlci path path_id { ds1 | e1 }
num_con dlci dlci_id

Entering the above command sequence results in the following prompt:

[local]host_name(config-port-slot_number/port_number-dlci-path_id/framing-timeslot/dlci_id)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
bind link

This command configures an association (binds) between an IP interface or a pre-configured routing SS7/Frame Relay link and the specific port being configured with the Channelized Port configuration commands.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Channelized Port Configuration > DLCI Configuration

```
configure > port channelized slot_number/port_number > dlci path path_id { dsl | e1 }
num_con dlci dlci_id
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-port-slot_number/port_number-dlci-path_id/framing-
timeslot/dlci_id)#
```

**Syntax**

```
[ no ] bind link peer-nsei nse_id ns-vci ns-vcid
```

- **peer-nsei nse_id**
  Defines the end-point network service entity identifier (NSEI). The NSEI must be an integer from 0 to 65535.

- **ns-vci ns-vcid**
  Defines the network service virtual circuit identifier (NSVCI). The NSVCI must be an integer from 0 to 65535.

- **no**
  Deletes the bind configuration from the Operator Policy.

**Usage**

Bind this port to network service entity 2 and network service VC 234.

```
bind link peer-nsei 2 ns-vci 234
```
end

Exits this sub-configuration mode and returns to the Exec mode.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
dend
```

**Usage**
Change the mode and return to the Exec mode.
exit

Exits the this sub-configuration mode and returns to the parent configuration mode.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Return to the previous configuration mode.
shaping

Defines egress traffic shaping to control flow for this DLCI.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Channelized Port Configuration > DLCI Configuration

configure > port channelized slot_number/port_number > dlci path path_id { ds1 | e1 }
num_con dlci dlci_id

Entering the above command sequence results in the following prompt:
[local]host_name(config-port-slot_number/port_number-dlci-path_id/framing-
timeslot/dlci_id)#

Syntax

shaping type

default shaping

shaping type

The following types of shaping provide flow management:
• cir: Committed Info Rate
• cir-eir: Committed Info Rate with Excess Rate
• ppr: Peak Packet Rate
• wfq: Weighted Fair Queuing

default

Resets the DLCI configuration to the system default.

Usage

Use this command to identify the type of signal shaping to be used on the DLCI.

Example

shaping cir
shutdown

Terminates all processes supporting the port or blocks the shutting down of the port. Conversely, this command with the no keyword enables the port.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Channelized Port Configuration > DLCI Configuration

```
configure > port channelized slot_number/port_number > dlci path path_id { ds1 | el } num_con dlci dlci_id
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-port-slot_number/port_number-dlci-path_id/framing-timeslot/dlci_id)#
```

**Syntax**

```
[ no ] shutdown
```

- **no**

  Enables the port’s administrative state. When omitted the card is shutdown (removed from service).

**Usage**

Shut down a port prior to re-cabling and/or other maintenance activities.
This command with the no keyword is required to bring a port into service.

**Example**

Use the following command to disable the DLCI:

```
no shutdown
```
Chapter 113
DNS Client Configuration Mode Commands

The DNS Client Configuration Mode is used to manage the system’s DNS interface and caching parameters.

**Mode**

Exec > Global Configuration > Context Configuration > DNS Client Configuration

```
configure > context context_name > dns-client client_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dns-client)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
bind

Binds the DNS client to a pre-configured logical IP interface.

Product
MME
SCM
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > DNS Client Configuration
configure > context context_name > dns-client client_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-dns-client)#

Syntax

bind { address ip_address [ port number ] | query-over-gtp }
no bind address

no

Removes the binding of the client to a specified interface.

bind address ip_address

Specifies the IP address of the interface to which the DNS client is being bound in IPv4 dotted-decimal notation.

bind port number

Specifies the UDP port number of the interface to which the DNS client is being bound as an integer from 1 to 65535. Default: 6011

bind query-over-gtp

Specifies that DNS client query is to be performed over GTP.

Usage

Use this command to associated the client with a specific logical IP address.

Example

The following command binds the DNS client to a logical interface with an IP address of 10.2.3.4 and a port number of 6000:

    bind address 10.2.3.4 port 6000
cache algorithm

Configures the method of use for the DNS VPN and session cache.

Product
MME
SCM
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > DNS Client Configuration
configure > context context_name > dns-client client_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-dns-client)#

Syntax

cache algorithm { central | local } { FIFO | LRU | LFU }

default cache algorithm { central | local }

default
Sets the DNS VPN and session cache method to default setting.

central | local
central: Specifies the central proclet (VPN manager)
local: Specifies the local proclet (session manager)

FIFO | LRU | LFU
FIFO: First in first out. This is the default setting for the central proclet.
LRU: Least recently used. This is the default value for the local proclet.
LFU: Least frequently used.

Usage
Use this command to configure the method by which entries are added and removed from the DNS cache.

Example
The following command configures the cache algorithm for the central proclet to least frequently used (LFU):

cache algorithm central lfu
**cache size**

Configures the maximum number of entries allowed in the DNS cache.

**Product**

MME  
SCM  
SGSN

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > DNS Client Configuration

```
configure > context context_name > dns-client client_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-dns-client)#
```

**Syntax**

```
cache size { central | local } max_size

default cache size { central | local }
```

**Usage**

Use this command to configure the maximum number of entries allowed in the DNS cache.

**Example**

The following command configures the cache size of the central proclet to 20000:

```
cache size central 20000
```
cache ttl

Configures the DNS cache time to live (TTL) for positive and negative responses.

Product
MME
SCM
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > DNS Client Configuration

configure > context context_name > dns-client client_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-dns-client)#

Syntax

```
cache ttl { negative | positive } seconds

default cache ttl { negative | positive }

no cache [ ttl { negative | positive } ]
```

**no**
Disables any or all configured DNS cache parameters.

**default**
Sets the DNS cache time to live for positive and negative responses to the default setting.

```
{ negative | positive } seconds

negative seconds: Specifies the time to live for negative responses as an integer from 60 through 86400. Default: 60.
positive seconds: Specifies the time to live for positive responses as an integer from 60 through 86400. Default: 86400 (1 day).
```

Usage
Use this command to adjust the DNS cache time to live.

Example
The following commands set the TTL DNS cache to 90 seconds for negative responses and 43200 seconds for positive responses:

```
cache ttl negative 90

cache ttl positive 43200
```
case-sensitive

Configures the case sensitivity requirement for responses to DNS requests.

Product
MME
SCM
SGSN

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > DNS Client Configuration

configure > context context_name > dns-client client_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-dns-client)#

Syntax

[ default | no ] case-sensitive response

default
Returns the command to its default setting of disabled.

no
Disables the requirement for case sensitivity in DNS responses.

case-sensitive response
Enables the requirement for case sensitivity in DNS responses.

Usage
Use this command to require case sensitivity (identical case usage between request and response) on all responses to DNS request messages.
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Use this command to return to the parent configuration mode.
resolver

Configures the number of DNS query retries and the retransmission interval once the response timer expires.

Product
MME
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > DNS Client Configuration

configure > context context_name > dns-client client_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-dns-client)#

Syntax

resolver { number-of-retries retries | retransmission-interval time }
default { number-of-retries | retransmission-interval }

default
Resets the specified resolver configuration to the default.

number-of-retries retries
Configures the number of DNS query retries on DNS response timeout as an integer from 0 through 4. Default: 2.

retransmission-interval time
Configures the initial retransmission interval (in seconds) for retransmission after the DNS response timeout as an integer from 2 to 5. Default is 3 seconds. The retransmission interval doubles after each retry when only one server is configured. In case both primary and secondary servers are configured, the retransmission time is doubled for the last retry.

Usage
Set the DNS retransmission retries or the retransmission interval. Issue the command twice to configure both parameters, one-at-a-time.

Example
The following command sets the DNS resolver retries to 4:

    resolver number-of-retries 4
round-robin answers

Configures the DNS client to return the DNS results in round-robin fashion if multiple results are available for a DNS query.

Product
MME
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > DNS Client Configuration
configure > context context_name > dns-client client_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-dns-client)#

Syntax

[ no | default ] round-robin-answers

no
Removes the configured round robin method for DNS answer.

default
Disables the round robin method for DNS answer.

round-robin-answers
Enables the round robin method for DNS answer.

Usage
Use this command to configure the DNS client to return the DNS results in round-robin fashion if multiple results are available for a DNS query.

Example
The following command configures the DNS client to use round robin method for DNS query answers:

   default ] round-robin-answers
Chapter 114
DSCP Template Configuration Mode Commands

The DSCP Template Configuration Mode provides the commands to configure DSCP marking for control packets and data packets for Gb over IP. Any number of DSCP templates can be generated in the SGSN Global configuration mode and then a template can be associated with one or more GPRS Services via the commands in the GPRS Service configuration mode.

Mode

Exec > Global Configuration > SGSN Global Configuration > DSCP Template Configuration

configure > context context_name > sgsn-global > dscp-template template_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-dscp-template-template_name)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
control-packet

Configures the diffserv code point marking (DSCP) value for 3GPP quality of service (QoS) class downlink control packets.

Product
SGSN
HNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > SGSN Global Configuration > DSCP Template Configuration

configure > context context_name > sgsn-global > dscp-template template_name

Entering the above command sequence results in the following prompt:

[local] host_name(config-dscp-template-template_name)#

Syntax

control-packet qos-dscp { af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef }

default control-packet

default

Resets the quality of service (QoS) DSCP setting to the ‘BE’ (best effort) default value.

DSCP marking option

Select one of the following downlink DSCP options for the control packets:

<table>
<thead>
<tr>
<th>• af11: Assured Forwarding 11 per-hop-behavior (PHB)</th>
<th>• be: Best Effort for Forwarding</th>
</tr>
</thead>
<tbody>
<tr>
<td>• af12: Assured Forwarding 12 PHB</td>
<td>• cs1: Class Selector 1 PHB</td>
</tr>
<tr>
<td>• af13: Assured Forwarding 13 PHB</td>
<td>• cs2: Class Selector 2 PHB</td>
</tr>
<tr>
<td>• af21: Assured Forwarding 21 PHB</td>
<td>• cs3: Class Selector 3 PHB</td>
</tr>
<tr>
<td>• af22: Assured Forwarding 22 PHB</td>
<td>• cs4: Class Selector 4 PHB</td>
</tr>
<tr>
<td>• af23: Assured Forwarding 23 PHB</td>
<td>• cs5: Class Selector 5 PHB</td>
</tr>
<tr>
<td>• af31: Assured Forwarding 31 PHB</td>
<td>• cs6: Class Selector 6 PHB</td>
</tr>
<tr>
<td>• af32: Assured Forwarding 32 PHB</td>
<td>• cs7: Class Selector 7 PHB</td>
</tr>
<tr>
<td>• af33: Assured Forwarding 33 PHB</td>
<td>• ef: Expedited forwarding PHB</td>
</tr>
</tbody>
</table>
- **af41**: Assured Forwarding 41 PHB
- **af42**: Assured Forwarding 42 PHB
- **af43**: Assured Forwarding 43 PHB

**Usage**

This command configures the QoS DSCP marking type for downlink control packets.

**Related commands for SGSN:**

- To create/delete a DSCP template, use the `dscp-template` in the SGSN Global configuration mode (see the *SGSN Global Configuration Mode Commands* section).
- To associate a specific DSCP template with a specific GPRS service configuration, use the `associate-dscp-template downlink` documented in the *GPRS Service Configuration Mode Commands* section.
- To check values configured for DSCP templates, use the `show sgsn-mode` command documented in the *Exec Mode Commands* section.

**Related commands for HNB-GW:**

- To create/delete a DSCP template, use the `dscp-template` in the *SGSN Global Configuration Mode*.
- To associate a specific DSCP template with a system for a PSP instance in SS7 routing domain, use `associate-dscp-template downlink` documented in the *SGSN PSP Configuration Mode Commands* section.

**Example**

Use a command similar to the following to set expedited forward per-hop behavior for the downlink control packets:

```
control-packet qos-dscp ef
```

Use the following command to reset the default best effort per-hop behavior:

```
default control-packet
```
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Use this command to return to the parent configuration mode.
data-packet

Configures the diffserv code point marking (DSCP) value for 3GPP quality of service (QoS) class downlink data packets.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > SGSN Global Configuration > DSCP Template Configuration
configure > context context_name > sgsn-global > dscp-template template_name

Entering the above command sequence results in the following prompt:
[local]host_name(config-dscp-template-template_name)#

Syntax

control-packet { background | conversationa | interactive { priority1 | priority2 | priority3 } | streaming } qos-dscp { af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef }

default data-packet { background | conversationa | interactive { priority1 | priority2 | priority3 } | streaming }

default

Resets the quality of service (QoS) DSCP setting to the be (best effort) default value.

background | conversationa | interactive | streaming

Select the QoS traffic class of service for the downlink data packets.

priority1 | priority2 | priority3

Select the traffic handling priority to be applied to the specified traffic class.

DSCP option

Select one of the following DSCP settings for the selected traffic class. Default is best effort (be) for all traffic classes settings.

<table>
<thead>
<tr>
<th></th>
<th>Assured Forwarding 11 per-hop-behavior (PHB)</th>
<th>Assured Forwarding 12 PHB</th>
<th>Assured Forwarding 13 PHB</th>
<th>Assured Forwarding 21 PHB</th>
<th>Assured Forwarding 22 PHB</th>
<th>Best Effort for Forwarding</th>
<th>Class Selector 1 PHB</th>
<th>Class Selector 2 PHB</th>
<th>Class Selector 3 PHB</th>
<th>Class Selector 4 PHB</th>
</tr>
</thead>
</table>
Usage

This command configures the QoS DSCP marking type for downlink data packets. DSCP levels indicate how packets are to be handled.

Related commands:

• To create/delete a DSCP template, use the `dscp-template` in the SGSN Global configuration mode (see the `SGSN Global Configuration Mode Commands` section).

• To associate a specific DSCP template with a specific GPRS service configuration, use the `associate-dscp-template downlink` documented in the `GPRS Service Configuration Mode Commands` section.

• To check values configured for DSCP templates, use the `show sgsn-mode` command documented in the `Exec Mode Commands` section.

Example

Use a command similar to the following to set expedited forward per-hop behavior for the downlink control packets:

```
control-packet qos-dscp ef
```

Use the following command to reset the default best effort per-hop behavior:

```
default control-packet
```
Chapter 115  
EAP Authentication Configuration Mode Commands

The EAP Authentication Configuration Mode is used to configure the Extensible Authentication Protocol (EAP) authentication methods for the crypto template.

**Mode**

Exec > Global Configuration > Context Configuration > Crypto Template Configuration > EAP Authentication Configuration

```plaintext
configure > context context_name > crypto template template_name ikev2-dynamic > authentication eap-profile profile_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-crypto-tmpl-ikev2-tunnel)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
eap-aka

Configures shared key values for the Extensible Authentication Protocol-Authentication and Key Agreement (EAP-AKA) authentication method used by subscribers using this crypto template.

Product  PDIF
Privilege  Security Administrator, Administrator
Mode  Exec > Global Configuration > Context Configuration > Crypto Template Configuration > EAP Authentication Configuration

configure > context context_name > crypto template template_name ikev2-dynamic > authentication eap-profile profile_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(cfg-crypto-tmpl-ikev2-tunnel)#

**Syntax**

```
eap-aka { encrypted key hex | key hex }
```

**encrypted key hex**

Specifies that the shared key is to be encrypted as a 16-character alphanumeric string or a hexadecimal number beginning with “0x”.

**key hex**

Specifies that the shared key is to be transmitted in clear text as a 16-character alphanumeric string or a hexadecimal number beginning with “0x”.

**Usage**

Use this command to set shared key parameters for subscribers using the EAP-AKA authentication method.

**Example**

The following command configures a clear-text shared key value for the EAP-AKA method:

```
eap-aka key a1234567890123456
```
eap-gtc

Configures shared key values for the EAP-GTC authentication method used by subscribers using this crypto template.

Product
PDIF
ASN-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Crypto Template Configuration > EAP Authentication Configuration

configure > context context_name > crypto template template_name ikev2-dynamic > authentication eap-profile profile_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(cfg-cryptotmpl-ikev2-tunnel)#

Syntax

eap-gtc { encrypted key value | key value }

encrypted key value
Specifies that the shared key is to be encrypted as a 16-character alphanumeric string.

key value
Specifies that the shared key is to be transmitted in clear text as a 16-character alphanumeric string.

Usage
Use this command to set shared key parameters for subscribers using the EAP-GTC authentication method.

Example

The following command configures a clear-text shared key value for the EAP-GTC method:

eap-GTC key aa1223344556677
**eap-md5**

Configures shared key values for the EAP-MD5 authentication method used by subscribers using this crypto template.

**Product**

PDIF

ASN-GW

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > Crypto Template Configuration > EAP Authentication Configuration

```
configure > context context_name > crypto template template_nameikev2-dynamic > authentication eap-profile profile_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-crypto-tmpl-ikev2-tunnel)#
```

**Syntax**

```
eap-md5 { encrypted key value | key value }
```

- **encrypted key value**
  Specifies that the shared key is to be encrypted as a 16-character alphanumeric string.

- **key value**
  Specifies that the shared key is to be transmitted in clear text as a 16-character alphanumeric string.

**Usage**

Use this command to set shared key parameters for subscribers using the EAP-MD5 authentication method.

**Example**

The following command configures a clear-text shared key value for the EAP-MD5 method:

```
eap-md5 key aa11223344556677
```
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
end

**Usage**
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

`exit`

**Usage**

Use this command to return to the parent configuration mode.
Chapter 116
EAP Configuration Mode Commands

The EAP Configuration Mode is used to configure parameters comprising an Extensible Authentication Protocol (EAP) used to support authentication on the system.

Mode

Exec > Global Configuration > Context Configuration > EAP Profile Configuration

`configure > context context_name > eap-profile profile_name`

Entering the above command sequence results in the following prompt:

`[context_name]host_name(cfg-ctx-eap-profile)#`

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
**end**

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**

Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Use this command to return to the parent configuration mode.
**max-retry**

Configures the maximum number of times the system will retry communicating with another EAP device.

**Product**

PDIF

ASN-GW

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > EAP Profile Configuration

```bash
configure > context context_name > eap-profile profile_name
```

Entering the above command sequence results in the following prompt:

```
{context_name}host_name(cfg-ctx-eap-profile)#
```

**Syntax**

```
max-retry num
```

```
default max-retry
```

```
max-retry num
```

Specifies the number of times to retry EAP communication with another device as an integer from 1 to 65535. Default: 16

**Usage**

Use this command to set a maximum retry number for communicating with other EAP devices.

**Example**

The following command sets the maximum number of retries to **50**:

```
max-retry 50
```
mode

Configures the system as one of three types of EAP devices: authenticator pass-through, authenticator server, or peer.

**Product**
PDIF
ASN-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > EAP Profile Configuration

context > context context_name > eap-profile profile_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(cfg-ctx-eap-profile)#

**Syntax**

mode { authenticator-pass-through | authenticator-server | peer }

default mode

- **default**
  Configures the default mode of Authenticator-pass-through.

- **authenticator-pass-through**
  Configures the system as an authenticator pass-through allowing EAP authentication to be performed by another server.
  This is the default setting for this command.

- **authenticator-server**
  Configures the system as an authenticator server. This allows the system to respond to EAP requests.

- **peer**
  Configures the system as a peer device requiring it to make EAP requests of another server or pass-through device.

**Usage**

Use this command to configure the system to perform as one of three types of EAP devices and configure settings in an EAP mode.
EAP Mode Configuration Mode commands are defined in the EAP Mode Configuration Mode Commands chapter.

**Example**
The following command configures the system to perform as an authenticator pass-through:

    mode authenticator-pass-through
The EAP Mode Configuration Mode is used to configure the Extensible Authentication Protocol (EAP) authentication method supported by the system.

**Mode**

Exec > Global Configuration > Context Configuration > EAP Profile Configuration

`configure > context context_name > eap-profile profile_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-ctx-eap-profile)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
exit
```

Usage
Use this command to return to the parent configuration mode.
method

Configures the EAP method used for authentication.

Product
PDIF
ASN-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > EAP Profile Configuration

configure > context context_name > eap-profile profile_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(cfg-ctx-eap-profile)#

Syntax

```
method { eap-aka | eap-gtc | eap-md5 } [ priority num ]
```

- **eap-aka**: Specifies that the EAP-AKA method is to be used for authentication.
- **eap-gtc**: Specifies that the EAP-GTC method is to be used for authentication.
- **eap-md5**: Specifies that the EAP-MD5 method is to be used for authentication.

```
priority num
```

Specifies a priority order for a specific EAP authentication method an integer from 1 though 65535.

Usage
Use this command to specify the EAP authentication method(s) to use and to place multiple methods in priority order.

Example
The following command sets EAP-AKA as one of the EAP authentication methods and places it as priority of 3:

```
method eap-aka priority 3
```
Chapter 118
EDR Format Configuration Mode Commands

The EDR Format Configuration Mode enables configuring Event Data Record (EDR) formats.

**Mode**

Exec > ACS Configuration > EDR Format Configuration

```
active-charging service service_name > edr-format format_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-acs-edr)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
attribute

This command allows you to specify the fields and their order in EDRs.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > EDR Format Configuration

active-charging service service_name > edr-format format_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-acs-edr)#

Syntax

attribute attribute { [ format { MM/DD/YY-HH:MM:SS | MM/DD/YYYY-HH:MM:SS | YYYY/MM/DD-HH:MM:SS | YYYYMMDDHHMMSS | seconds } ] [ localtime ] | [ { ip | tcp } { bytes | pkts } { downlink | uplink } ] priority priority }

no attribute attribute [ { ip | tcp } { bytes | pkts } { downlink | uplink } ] [ priority priority ]

If added previously, removes the specified attribute from the EDR format.

attribute

Specifies the attribute.

attribute must be one of the following:

<table>
<thead>
<tr>
<th>Attributes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bandwidth-policy</td>
<td>This attribute reports the bandwidth policy name of subscriber. Bandwidth policy can be configured or applied to subscriber by —</td>
</tr>
<tr>
<td></td>
<td>• binding with APN (static)</td>
</tr>
<tr>
<td></td>
<td>• binding with Rulebase (static)</td>
</tr>
<tr>
<td></td>
<td>• receiving from AAA server (dynamic)</td>
</tr>
<tr>
<td></td>
<td><strong>Important:</strong> This attribute field is customer specific. For more information, contact your Cisco account representative.</td>
</tr>
<tr>
<td>radius-called-station-id</td>
<td>This attribute reports the Called Station ID of the mobile handling the flow.</td>
</tr>
<tr>
<td>radius-calling-station-id</td>
<td>This attribute reports the Calling Station ID of the mobile handling the flow.</td>
</tr>
</tbody>
</table>
## Attributes

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>radius-fa-nas-identifier</td>
<td>This attribute reports the RADIUS NAS identifier of Foreign Agent (FA).</td>
</tr>
<tr>
<td>radius-fa-nas-ip-address</td>
<td>This attribute reports the RADIUS IP address of Foreign Agent (FA).</td>
</tr>
<tr>
<td>radius-nas-identifier</td>
<td>This attribute reports the RADIUS NAS identifier.</td>
</tr>
<tr>
<td>radius-nas-ip-address</td>
<td>This attribute reports the RADIUS NAS IP address.</td>
</tr>
<tr>
<td>radius-user-name</td>
<td>This attribute reports the user name associated with the flow.</td>
</tr>
<tr>
<td>sn-3gpp2-always-on</td>
<td>This option has been deprecated.</td>
</tr>
<tr>
<td>sn-3gpp2-bsid</td>
<td>To configure this attribute see the <code>rule-variable</code> command.</td>
</tr>
<tr>
<td>sn-3gpp2-esn</td>
<td>This option has been deprecated.</td>
</tr>
<tr>
<td>sn-3gpp2-ip-qos</td>
<td>To configure this attribute see the <code>rule-variable</code> command.</td>
</tr>
<tr>
<td>sn-3gpp2-ip-technology</td>
<td>This option has been deprecated.</td>
</tr>
<tr>
<td>sn-3gpp2-release-indicator</td>
<td>To configure this attribute see the <code>rule-variable</code> command.</td>
</tr>
<tr>
<td>sn-3gpp2-service-option</td>
<td>This option has been deprecated.</td>
</tr>
<tr>
<td>sn-3gpp2-session-begin</td>
<td>To configure this attribute see the <code>rule-variable</code> command.</td>
</tr>
<tr>
<td>sn-3gpp2-session-continue</td>
<td>This option has been deprecated.</td>
</tr>
<tr>
<td>sn-acct-session-id</td>
<td>To configure this attribute see the <code>rule-variable</code> command.</td>
</tr>
<tr>
<td>sn-acct-session-id</td>
<td>This attribute reports the unique session identifier for accounting.</td>
</tr>
<tr>
<td>Attributes</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>sn-app-protocol</td>
<td>This attribute reports the application protocol for the flow. A value indicating the protocol, such as one of the following:</td>
</tr>
<tr>
<td></td>
<td>- ACSPROTO_UNKNOWN = 0</td>
</tr>
<tr>
<td></td>
<td>- ACSPROTO_GTP = 1</td>
</tr>
<tr>
<td></td>
<td>- ACSPROTO_IP = 2</td>
</tr>
<tr>
<td></td>
<td>- ACSPROTO_TCP = 3</td>
</tr>
<tr>
<td></td>
<td>- ACSPROTO_UDP = 4</td>
</tr>
<tr>
<td></td>
<td>- ACSPROTO_HTTP = 5</td>
</tr>
<tr>
<td></td>
<td>- ACSPROTO_HTTPS = 6</td>
</tr>
<tr>
<td></td>
<td>- ACSPROTO_FTP = 7</td>
</tr>
<tr>
<td></td>
<td>- ACSPROTO_FTP_CONTROL = 8</td>
</tr>
<tr>
<td></td>
<td>- ACSPROTO_FTP_DATA = 9</td>
</tr>
<tr>
<td></td>
<td>- ACSPROTO_WTP = 10</td>
</tr>
<tr>
<td></td>
<td>- ACSPROTO_WSP = 11</td>
</tr>
<tr>
<td></td>
<td>- ACSPROTO_WTP_WSP_CONNECTION_ORIENTED = 12</td>
</tr>
<tr>
<td></td>
<td>- ACSPROTO_WSP_CONNECTION_LESS = 13</td>
</tr>
<tr>
<td></td>
<td>- ACSPROTO_DNS = 14</td>
</tr>
<tr>
<td></td>
<td>- ACSPROTO_ICMP = 15</td>
</tr>
<tr>
<td></td>
<td>- ACSPROTO_POP3 = 16</td>
</tr>
<tr>
<td></td>
<td>- ACSPROTO_SIP = 17</td>
</tr>
<tr>
<td></td>
<td>- ACSPROTO_SDIP = 18</td>
</tr>
<tr>
<td></td>
<td>- ACSPROTO_SMP = 19</td>
</tr>
<tr>
<td></td>
<td>- ACSPROTO_EMAIL = 20</td>
</tr>
<tr>
<td></td>
<td>- ACSPROTO_MMS = 21</td>
</tr>
<tr>
<td></td>
<td>- ACSPROTO_FILE_TRANSFER = 22</td>
</tr>
<tr>
<td></td>
<td>- ACSPROTO_WWW = 23</td>
</tr>
<tr>
<td></td>
<td>- ACSPROTO_RTP = 24</td>
</tr>
<tr>
<td></td>
<td>- ACSPROTO_RTSP = 25</td>
</tr>
<tr>
<td></td>
<td>- ACSPROTO_IMAP = 26</td>
</tr>
<tr>
<td></td>
<td>- ACSPROTO_FLOW = 27</td>
</tr>
<tr>
<td></td>
<td>- ACSPROTO_CCA = 28</td>
</tr>
<tr>
<td></td>
<td>- ACSPROTO_P2P = 29</td>
</tr>
<tr>
<td></td>
<td>- ACSPROTO_RTCP = 30</td>
</tr>
<tr>
<td></td>
<td>- ACSPROTO_ICMPV6 = 31</td>
</tr>
<tr>
<td></td>
<td>- ACSPROTO_TFTP = 32</td>
</tr>
<tr>
<td></td>
<td>- ACSPROTO_PPTP = 33</td>
</tr>
<tr>
<td>Attributes</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>sn-cf-category-classification-used</td>
<td>For Category-based Content Filtering, this attribute reports the last classification used by system for the flow, or blank if classification was never successfully performed. For URL Blacklisting, specifies category of the blacklisted URL in the Blacklist database.</td>
</tr>
</tbody>
</table>
| sn-cf-category-flow-action     | For Category-based Content Filtering, this attribute reports the last action taken for the flow, or blank if content filtering was never performed. The following are the possible values:  
  - allow  
  - content-insert  
  - discard  
  - redirect-url  
  - terminate-flow  
  For URL Blacklisting, this attribute reports the last action taken for the flow, or blank if Blacklist matching was never performed. The following are the possible values:  
  - discard  
  - terminate-flow  
  - redirect-url  
  - www-reply-code-terminate-flow |
| sn-cf-category-policy         | For Category-based Content Filtering, this attribute reports the category policy identifier that was used for the flow, or blank if content filtering was never attempted for the flow. |
| sn-cf-category-rating-type    | For Category-based Content Filtering, this attribute reports the type, either “static” or “dynamic” that was last successfully performed for the flow, or blank if content filtering was never successful for the flow.  
  For URL Blacklisting, specifies “blacklisting”. |
| sn-cf-category-unknown-url    | This attribute reports the identifier for unknown URL under content filtering action. It holds either “1” for unknown URLs or “0” for the URLs having static rating in its database. |
| sn-charge-volume              | This attribute reports the total charge volume excluding bytes/packets dropped/retransmitted by ECS.  
  This behavior can be changed by configuring to allow dropped/retransmitted bytes/packets to be included in the net volume. See the edr sn-charge-volume command in the ACS Rulebase Configuration Mode Commands chapter. |
<table>
<thead>
<tr>
<th>Attributes</th>
<th>Description</th>
</tr>
</thead>
</table>
| sn-closure-reason      | This attribute reports the reason for termination of the flow/EDR:  
  - 0: Normal end of flow  
  - 1: End of flow by handoff processing  
  - 2: Subscriber session terminated  
  - 3: Inter-chassis Session Recovery switchover  
  - 12: Completion of transaction  
  - 13: End of VoIP call event  
    This is supported only in release 12.2.  
  - 14: End of VoIP call event  
    This is supported in 14.0 and later releases. |
| sn-correlation-id      | This attribute reports the RADIUS correlation identifier.                                                                                                                                                   |
| sn-direction           | This attribute reports the direction of the first packet for the flow. It has following values:  
  - toMobile: This value appears when direction of first packet is towards mobile node.  
  - fromMobile: This value appears when direction of first packet is towards mobile node.  
  - unknown: This value appears when the original originator of a flow can not be determined (for example, a flow that is interrupted due to a Inter-chassis Session Recovery switchover). |
| sn-duration            | This attribute reports the duration between the last and first packet for the record.                                                                                                                        |
| sn-end-time [ format | This attribute reports the timestamp for last packet of flow in UTC.                                                                                                                                          |
| format ] localtime     |                                                                                                                                                                                                              |
| sn-fa-correlation-id   | This attribute reports the RADIUS Correlation Identifier of the Foreign Agent (FA).                                                                                                                            |
| sn-fa-ip-address       | This attribute reports IP address of the Foreign Agent (FA).                                                                                                                                                 |
| sn-filler-blank        | This attribute inserts a blank filler field, generates an empty EDR field.                                                                                                                                     |
| sn-filler-zero         | This attribute inserts a “0” in the EDR field.                                                                                                                                                              |
## Attributes

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>sn-flow-end-time</code></td>
<td>This attribute reports the time of flow-end EDR generation—when EDRs are generated at hagr, session-end, timeout, or normal-end-signaling conditions. <code>sn-start-time</code> and <code>sn-end-time</code> fields of flow end-condition EDRs cannot be used to determine the duration of the flow if intermediate EDRs are generated (rule-match or transaction-complete or any other intermediate EDR). <code>sn-start-time</code> field in an EDR gives the time the first packet was received after the last EDR was generated. So, whenever an EDR is generated, this field is reset to the time the EDR gets generated. So the <code>sn-start-time</code> field in flow end-condition EDRs may not have the time of the first packet received on that flow. It will have the time at which the last EDR was generated or the first packet time if no EDR was generated for that flow. <code>sn-end-time</code> field gives the time at which the last packet on the flow was received. Flow end-condition EDRs may not be generated immediately after receiving the last packet. For example, in case of session-end or timeout EDRs, last packet time and EDR generation time may be different. <code>sn-flow-start-time</code> gives the time of the first packet of the flow (irrespective of whether intermediate EDRs were generated), and <code>sn-flow-end-time</code> gives the time when EDRs are generated at hagr, session-end, timeout or normal-end-signaling conditions. The values of these fields will be populated in EDRs only for hagr, session-end, timeout and normal-end-signaling EDRs.</td>
</tr>
<tr>
<td><code>sn-flow-id</code></td>
<td>This attribute reports the flow-id assigned internally by the ECS module to each flow.</td>
</tr>
<tr>
<td><code>sn-flow-start-time</code></td>
<td>This attribute reports the time of the first packet of the flow (irrespective of whether intermediate EDRs were generated). Also see, <code>sn-flow-end-time</code>.</td>
</tr>
<tr>
<td><code>sn-format-name</code></td>
<td>This attribute reports the name of the EDR/UDR format used.</td>
</tr>
<tr>
<td><code>sn-group-id</code></td>
<td>This attribute reports the sequence group ID of the record.</td>
</tr>
<tr>
<td><code>sn-ha-ip-address</code></td>
<td>This attribute reports IP address of the Home Agent (HA).</td>
</tr>
<tr>
<td><code>sn-ip-protocol-name</code></td>
<td>This attribute reports the IP protocol name for the flow. For IANA registered IP Protocol (Layer 4 Protocol) name, like TCP, UDP, AH, ESP, ICMP, etc.</td>
</tr>
<tr>
<td><code>sn-nat-binding-timer</code></td>
<td>For Network Address Translation (NAT) in-line service, this attribute reports the port chunk hold timer.</td>
</tr>
<tr>
<td><code>sn-nat-gmt-offset</code></td>
<td>For NAT in-line service, this attribute reports the GMT offset of the node generating NAT bind record.</td>
</tr>
<tr>
<td><code>sn-nat-ip</code></td>
<td>For NAT in-line service, this attribute reports the NAT IP address of the port chunk.</td>
</tr>
<tr>
<td><code>sn-nat-last-activity-time-gmt</code></td>
<td>For NAT in-line service, this attribute reports the time when the last flow in a specific NAT set of flows was seen.</td>
</tr>
<tr>
<td><code>sn-nat-port-block-end</code></td>
<td>For NAT in-line service, this attribute reports the last port number of the port chunk.</td>
</tr>
<tr>
<td><code>sn-nat-port-block-start</code></td>
<td>For NAT in-line service, this attribute reports the starting port number of the port chunk.</td>
</tr>
<tr>
<td><code>sn-nat-port-chunk-alloc-dealloc-flag</code></td>
<td>For NAT in-line service, this attribute reports whether the port chunk is allocated or released.</td>
</tr>
<tr>
<td><code>sn-nat-port-chunk-alloc-time-gmt</code></td>
<td>For NAT in-line service, this attribute reports when the port chunk was allocated.</td>
</tr>
<tr>
<td><code>sn-nat-port-chunk-dealloc-time-gmt</code></td>
<td>For NAT in-line service, this attribute reports when the port chunk was released.</td>
</tr>
</tbody>
</table>
### Attributes

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sn-nat-realm-name</td>
<td>For NAT in-line service, this attribute reports the name of the NAT realm.</td>
</tr>
<tr>
<td>sn-nat-subscribers-per-ip-address</td>
<td>For NAT in-line service, this attribute reports the subscriber(s) per NAT IP address.</td>
</tr>
<tr>
<td>sn-parent-protocol</td>
<td>This attribute reports the parent protocol of the flow. An integer value like in <code>sn-app-protocol</code>; for RTCP/RTP flows, the parent protocol may be RTSP or SIP; for GRE flows, the parent protocol will be PPTP, and so on.</td>
</tr>
<tr>
<td>sn-port-service-name</td>
<td>This attribute reports the registered name for the server port. For IANA registered/Well Known Transport Port name mapping for the Server Port like SSL, HTTP, DNS, FTP, TELNET, SSH, Diablo, Rainbow six, UnReal_UT etc. This port service name mapping is done based on the Server port, which means if the flow is &quot;FromMobile&quot;, the sn-server-port is mapped as the service name port. If the flow is &quot;ToMobile&quot;, the sn-subscriber-port is mapped as the service name.</td>
</tr>
<tr>
<td>sn-rulebase</td>
<td>This attribute reports the name of the ECS rulebase applied.</td>
</tr>
<tr>
<td>sn-sequence-no</td>
<td>This attribute reports the unique sequence number (per <code>sn-sequence-group</code> and <code>radius-nas-ip-address</code>) of EDR identifier and linearly increasing in EDR file.</td>
</tr>
<tr>
<td>sn-server-port</td>
<td>This attribute reports the TCP/UDP port number of the server in a subscriber’s data flow.</td>
</tr>
<tr>
<td>sn-start-time [format format] localtime</td>
<td>This attribute reports the timestamp for last packet of flow in UTC.</td>
</tr>
<tr>
<td>sn-subscriber-nat-flow-ip</td>
<td>For NAT in-line service, this attribute reports the NAT IP address of NAT-enabled subscriber.</td>
</tr>
<tr>
<td>sn-subscriber-nat-flow-port</td>
<td>For NAT in-line service, this attribute reports the NAT port number of NAT-enabled subscriber.</td>
</tr>
<tr>
<td>sn-subscriber-port</td>
<td>This attribute reports the TCP/UDP port number of the Mobile handling subscriber data flow.</td>
</tr>
<tr>
<td>sn-volume-amt {ip</td>
<td>tcp} {bytes</td>
</tr>
<tr>
<td>sn-volume-dropped-amt {ip</td>
<td>tcp} {bytes</td>
</tr>
<tr>
<td>sn-volume-ip-with-rtsp-or-rtp bytes {downlink</td>
<td>priority</td>
</tr>
<tr>
<td>subscriber-ipv4-address</td>
<td>For NAT in-line service, this attribute generates the subscriber IPv4 address in the NBR.</td>
</tr>
<tr>
<td>subscriber-ipv6-address</td>
<td>For NAT in-line service, this attribute generates the subscriber IPv6 prefix in the NBR.</td>
</tr>
<tr>
<td>transaction-downlink-bytes</td>
<td>This attribute reports the total downlink bytes for the transaction.</td>
</tr>
<tr>
<td>transaction-downlink-packets</td>
<td>This attribute reports the total downlink packets for the transaction.</td>
</tr>
</tbody>
</table>
### Attributes

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>transaction-uplink-bytes</td>
<td>This attribute reports the total uplink bytes for the transaction.</td>
</tr>
<tr>
<td>transaction-uplink-packets</td>
<td>This attribute reports the total uplink packets for the transaction.</td>
</tr>
</tbody>
</table>

### format

```
```

Specifies the timestamp format.

### localtime

Specifies timestamps with the local time. By default, timestamps are displayed in GMT/UTC.

### { ip | tcp } { bytes | pkts } { downlink | uplink }

Specifies bytes/packets sent/received from/by mobile.

### priority priority

Specifies the position priority of the value within the EDR record. Lower numbered priorities (across all attribute, event-label, and rule-variable) occur first. `priority` must be an integer from 1 through 65535. Up to 50 position priorities (across all attribute, event-label, and rule-variable) can be configured.

### Usage

Use this command to set the attributes and priority for EDR file format. A particular field in EDR format can be entered multiple times at different priorities. While removing the EDR field using the `no attribute` command either you can remove all occurrences of a particular field by specifying the field name or a single occurrence by additionally specifying the optional `priority` keyword.

### Example

The following is an example of this command:

```
attribute radius-user-name priority 12
```
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
event-label

This command allows you to specify an optional event label/identifier to be used as an attribute in the EDRs.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > EDR Format Configuration
active-charging service service_name > edr-format format_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-acs-edr)#

Syntax

```
event-label event_label priority priority
no event-label
```

**no**

If previously configured, removes the event label configuration.

```
event_label
```

Specifies the event label/identifier to be used as EDR attribute.

```
event_label
```

must be an alphanumeric string of 1 through 63 characters.

```
priority priority
```

Specifies the Comma Separated Value (CSV) position of the attribute (label/identifier) in the EDR.

```
priority
```

must be an integer from 1 through 65535.

Usage

Use this command to configure an optional event label/identifier as an attribute in the EDR and its position in the EDR.

Example

The following is an example of this command:

```
event-label radius_csv1 priority 23
```
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**
Use this command to return to the parent configuration mode.
rule-variable

This command allows you to specify fields and their order in EDRs.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > EDR Format Configuration

```
active-charging service service_name > edr-format format_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-acd-edr)#
```

Syntax

```
rule-variable rule_variable priority priority [ in-quotes ]
no rule-variable rule_variable [ priority priority ]
```

no

If previously configured, removes the specified rule variable configuration.

```
rule_variable
```

Specifies the rule variable for the EDR format.

```
rule_variable must be one of the following options:
```
- **bearer 3gpp**: 3GPP bearer-related fields:
  - **charging-id**: Charging ID of the bearer flow
  - **imei**: IMEI or IMEISV (depending on the case) associated with the bearer flow. Only available in StarOS 8.1 and later releases.
  - **imsi**: Specific Mobile Station Identification number.
  - **rat-type**: RAT type associated with the bearer flow. Only available in StarOS 8.1 and later releases.
  - **sgsn-address**: SGSN associated with the bearer flow. Only available in StarOS 8.1 and later releases. For MIPv6 calls, sgsn-address field is populated with HSGW address.
  - **user-location-information**: User location information associated with the bearer flow. Only available in StarOS 8.1 and later releases.

- **bearer 3gpp2**: 3GPP2 bearer-related fields:
  - **always-on**: 3GPP2 always on indicator
  - **bsid**: 3GPP2 BSID
  - **esn**: 3GPP2 ESN
  - **ip-qos**: 3GPP2 IP QoS
*ip-technology*: 3GPP2 IP technology
*release-indicator*: 3GPP2 release indicator
*service-option*: 3GPP2 service option
*session-begin*: 3GPP2 session begin indicator
*session-continue*: 3GPP2 session continue indicator

*bearer ggsn-address*: GGSN IP address field. For MIPv6 calls, ggsn-address field in EDR will be populated with PGW address.

*dns*: Domain Name System (DNS) related fields:
  *answer-name*: DNS answer name. This depends upon query type.
  *previous-state*: DNS previous state information
  *query-name*: DNS query name
  *return-code*: DNS query response code
  *state*: DNS current state information
  *tid*: DNS Transaction Identifier

*file-transfer*: File Transfer related fields:
  *chunk-number*: Number of chunks
  *current-chunk-length*: Length of current chunk
  *declared-chunk-length*: Declared size of the chunk
  *declared-file-size*: Declared size of the file
  *filename*: Name of the file being transferred
  *previous-state*: Previous state of session
  *state*: Current state of session
  *transferred-file-size*: Transferred size of the file

*flow*: Flow related fields:
  *tethered*: Tethering detected on flow. Enables/disables tethering detection result field in EDRs sent to MUR.

*ftp*: File Transfer Protocol (FTP) related fields:
  *client-ip-address*
  *client-port*
  *command name*: Command sent
  *connection-type*
  *filename*: File name being transferred in any of the FTP-related FTP command
  *pdu-length*: FTP PDU length
  *pdu-type*
  *previous-state*: Previous state of FTP session
  *reply code*
  *server-ip-address*
- server-port
- session-length: Total length of FTP session
- state: Current state of FTP session
- url: URL of file
- user: User identifier

**http:** Hypertext Transport Protocol (HTTP) related fields:
- attribute-in-data: dynamic header field in application payload
- attribute-in-url: dynamic header field in URL
- content disposition
- content length
- content type
- cookie: HTTP cookie header
- domain
- header-length: HTTP header length
- host
- payload-length: Payload length
- pdu-length
- previous-state: Previous state of session
- referer
- reply code: HTTP response
- request method: HTTP request method
- session-length: Total length of HTTP session
- state: Current state of session
- transaction-length: Total length of HTTP transaction
- transfer-encoding: Transfer encoding
- uri: Uniform Resource Identifier
- url: Uniform Resource Locator

**length size:** This optional filter allows the user to configure the HTTP URL length from 1 to 4095. The EDR rule-variable “HTTP URL” supports the maximum length of 4095. That is, any URL greater than the maximum length is truncated and then written to EDR.

In 17.0 and later releases: The length of HTTP URL is from 1 to 4095.
In 15.0 and 16.0 releases: The length of HTTP URL is from 1 to 255.
In releases prior to 15.0: The length of HTTP URL is from 1 to 127.

**user-agent**

**length size:** This optional filter allows the user to configure the HTTP User-Agent length from 1 to 255. In releases prior to 15.0, the EDR rule-variable “HTTP User-Agent” supports the maximum length of 127. That is, any user-agent greater than 127 is truncated and then written to EDR.
• **version**
• **x-header**: extension header
• **ad-delivered, ad-replaced, compression-bytes-in, compression-bytes-out, dns-resolution-locally, dns-resolution-remotely, tpo-enabled**

**Important**: The Traffic Performance Optimization (TPO) in-line service is not supported in this release.

• **icmp**: Internet Control Message Protocol (ICMP) related fields:
  • **code**: ICMP code
  • **type**: ICMP type

• **icmpv6**: Internet Control Message Protocol Version 6 (ICMPv6) related fields:
  • **code**: ICMPv6 code
  • **type**: ICMPv6 type

• **imap**: Internet Message Access Protocol (IMAP) related fields:
  • **cc**: IMAP e-mail CC field
  • **command**: IMAP command
  • **content**
  • **date**: IMAP e-mail Date field
  • **final-reply**: IMAP final reply
  • **from**: IMAP e-mail From field
  • **mail-size**: IMAP size of e-mail in RFC822 format
  • **mailbox-size**: IMAP number of e-mails in the mailbox
  • **message-type**: IMAP message type
  • **previous-state**: IMAP session previous state
  • **session-length**: IMAP session length
  • **session-previous-state**: IMAP session previous state
  • **session-state**: IMAP session state
  • **state**: IMAP state
  • **subject**: IMAP e-mail Subject field
  • **to**: IMAP e-mail To field

• **ip**: Internet Protocol (IP) related fields:
  • **dst-address**: destination IP address
  • **protocol**: Protocol being transported by IP packet
  • **server-ip-address**: IP address of server. This field in EDR contains either the IPv4 or IPv6 address of the server for a particular flow (flow level). The maximum length of this field is 48 characters. For an IPv6 address, the maximum length is 45 characters; for an IPv4 address, the maximum length is 15 characters.
  • **src-address**: Source IP address
**subscriber-ip-address**: IP address of subscriber. This field in EDR contains either the IPv4 or IPv6 address of the client/subscriber for a particular call (subscriber level). The value of this field does not change for a particular call. The maximum length of this field is 48 characters. For an IPv6 address, the maximum length is 45 characters. For an IPv4 address, the maximum length is 15 characters.

**total-length**: Total length of packet, including payload

**version**: IP version

**mms**: Multimedia Message Service (MMS) related fields:

- **bcc**
- **cc**
- **content location**
- **content type**
- **date** [ format { MM/DD/YYYY-HH:MM:SS | YYYY/MM/DD-HH:MM:SS } ]
- **from**
- **message-size**
- **previous-state**
- **response status**
- **state**
- **subject**
- **tid**
- **to**

**p2p**: Peer-to-peer protocol related fields:

- **duration**: Peer-to-peer protocol duration
- **protocol**: Peer-to-peer protocol
- **protocol-group**: Associated protocol group of the specific peer-to-peer protocol/application

**pop3**: Post Office Protocol version 3 (POP3) related fields:

- **command name**: Command of POP3 session
- **mail-size**: Mail size
- **pdu-length**: Length of POP3 PDU
- **pdu-type**: Type of packet
- **previous-state**: Previous state of POP3 session
- **reply status**: Reply for the POP3 command
- **session-length**: Total length of POP3 session
- **state**: Current state of POP3 session
- **user-name**: User of POP3 session

**rtcp**: RTP Control Protocol (RTCP) related fields:

- **control-session-flow-id**: Flow ID of the controlling RTSP/SIP session
- **jitter**: RTCP interarrival jitter
• **rtsp-id**: RTSP ID of the RTCP flow
• **uri**: URI of the control protocol related to the RTCP flow

• **rtp**: Real-time Transfer Protocol (RTP) related fields:
  • **control-session-flow-id**: Flow ID of the controlling RTSP/SIP session
  • **pdu-length**: Length of RTP PDU
  • **rtsp-id**: RTSP ID of the flow
  • **session-length**: Total length of RTP session
  • **uri**: URI of the control protocol related to the RTP flow

• **rtsp**: Real Time Streaming Protocol (RTSP) related fields:
  • **command-id**: RTSP command ID
  • **content-type**
  • **date**: RTSP Date field
  • **previous-state**: RTSP previous state
  • **reply-code**
  • **request-method 1**: play method
  • **request-method 2**: setup method
  • **request-method 3**: pause method
  • **request-method 4**: record method
  • **request-method 5**: options method
  • **request-method 6**: redirect method
  • **request-method 7**: describe method
  • **request-method 8**: announce method
  • **request-method 9**: teardown method
  • **request-method 10**: get-parameter method
  • **request-method 11**: set-parameter method
  • **request-packet**
  • **rtsp-uri**: RTSP RTP-Info stream-uri field
  • **session-id**: RTSP session-id field
  • **session-length**: Total number of bytes passed through the RTSP data session
  • **state**: RTSP state
  • **uri**: RTSP uri field
  • **uri-sub-part**
  • **user-agent**: RTSP user-agent field

• **sdp**: Session Description Protocol (SDP) related fields:
  • **connection-ip-address**: IP address in SDP connection field
  • **media-audio-port**: Port used for audio media
  • **media-video-port**: Port used for video media
- **secure-http**: HTTPS related field.
- **sip**: Session Initiation Protocol (SIP) related fields:
  - **call-id**: SIP call-id field
  - **content type**
  - **from**: SIP From field
  - **previous-state**: SIP previous state
  - **reply code**
  - **request method**
  - **request packet**
  - **state**: SIP state
  - **to**: SIP To field
  - **uri**: SIP URI field
  - **uri sub-part**
- **smtp**: Simple Mail Transfer Protocol (SMTP) related fields:
  - **command name**: Command of SMTP session
  - **mail-size**: Size of given mail
  - **pdu-length**: Length of SMTP PDU
  - **previous-state**: Previous state of SMTP session
  - **recipient**: SMTP e-mail Recipient field
  - **reply status**: Response for the SMTP command
  - **sender**: SMTP e-mail Sender field
  - **session-length**: Total length of SMTP session
  - **state**: Current state of SMTP session
- **tcp**: Transmission Control Protocol (TCP) related fields:
  - **dst-port**: TCP destination port
  - **duplicate**: TCP retransmitted/duplicate packet
  - **flag**: Current packet TCP flag
  - **os-signature**: OS signature string for TCP flow. Enables/disables OS Signature field in EDRs sent to MUR.
  - **out-of-order**: TCP out of order packet analyzed
  - **payload-length**: TCP payload length
  - **previous-state**: Previous state of MS
  - **src-port**: TCP source port
  - **state**: Current state of MS
  - **tpo-enabled**
EDR Format Configuration Mode Commands

**Important:** The Traffic Performance Optimization (TPO) in-line service is not supported in this release.

- **traffic-type:** Traffic type of flow (voice or non-voice depending upon flow type).
- **udp:** User Datagram Protocol (UDP) related fields:
  - **dst-port:** UDP destination port
  - **src-port:** UDP source port
- **voip-duration:** Duration of voice call, in seconds. For a flow in which voice call end is detected, output will be a non-zero value. For other flows it will be zero. This is no longer supported for P2P in 14.0 and later releases.
- **wsp:** Wireless Session Protocol (WSP) related fields:
  - **content type**
  - **domain:** WSP domain name
  - **host:** WSP host name
  - **pdu-length:** WSP PDU length
  - **pdu-type:** WSP PDU type
  - **reply code**
  - **session-length:** WSP total packet length
  - **tid:** WSP transaction identifier
  - **total-length:** WSP total packet length
  - **url:** WSP URL
  - **user-agent:** WSP user agent
- **wtp:** Wireless Transaction Protocol (WTP) related fields:
  - **gtr:** Group Transmission Flag
  - **pdu-length:** PDU length of the WTP packet
  - **pdu-type:** WTP protocol data unit information
  - **previous-state:** WTP previous state information
  - **state:** WTP current state information
  - **tid:** WTP transaction identifier
  - **transaction class:** WTP transaction class
  - **ttr:** WTP Trailer Transmission flag

**Important:** For more information on protocol-based rules, see the *ACS Ruledef Configuration Mode Commands* chapter.

```
priority priority
```

Specifies the CSV position of the field (protocol rule) in the EDR. `priority` must be an integer from 1 through 65535.
**in-quotes**

Specifies placing double quotes (" ") around the specified field in the EDR.

**Important:** In this release, this keyword is only valid for the MMS protocol to and subject fields. `rule-variable mms to priority priority [in-quotes] rule-variable mms subject priority priority [in-quotes]`

**Usage**

Use this command to specify what field appears in which order in the EDR. A particular field in an EDR format can be entered multiple times with different priorities. While removing the EDR field using the `no rule-variable` command you can remove all occurrences of a particular field by specifying the field name or a single occurrence by additionally specifying the optional `priority` keyword.

**Example**

The following is an example of this command:

```
rule-variable tcp dst-port priority 36
```
Chapter 119
EDR Module Configuration Mode Commands

The EDR Module Configuration Mode allows you to configure Event Data Record (EDR) file transfer parameters.

Mode

Exec > Global Configuration > Context Configuration > EDR Module Configuration
configure > context context_name > edr-module active-charging-service

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-edr)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
This command allows you to configure EDR/UDR file transfer parameters.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > EDR Module Configuration

```
configure > context context_name > edr-module active-charging-service
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-edr)#
```

**Syntax**

```
cdr { purge { storage-limit storage_limit | time-limit time_limit } [ max-files max_records_to_purge ] | push-interval push_interval | push-trigger space-usage-percent trigger_percentage | remove-file-after-transfer | transfer-mode { pull [ module-only ] | push primary { encrypted-url encrypted_url | url url } [ [ max-files max_records ] [ max-tasks task_num ] [ module-only ] [ secondary { encrypted-secondary-url encrypted_secondary_url | secondary-url secondary_url } ] [ via local-context ] + ] | use-harddisk }

default cdr [ purge | push-interval | push-trigger space-usage-percent | remove-file-after-transfer | transfer-mode [ module-only | push via ] | use-harddisk ] +

no cdr [ purge | remove-file-after-transfer | use-harddisk ] +
```

**Important:** The **use-harddisk** keyword is available only on the ASR 5000 and ASR 5500 chassis.

- **purge**: Disabled
- **push-interval**: 300 seconds
- **push-trigger**: 80 percent
- **remove-file-after-transfer**: Disabled
- **transfer mode**: Pull
- **push via**: LC is used for push
- **use-harddisk**: Disabled

If previously configured, disables the specified configuration:

- **purge**: Disables purging of records.
**remove-file-after-transfer**: Retains a copy of the file even after it has been pushed or pulled to another server.

**use-harddisk**: Disables data storage on the ASR 5000 SMC hard disk or ASR 5500 hard disk array.

---

**Important**: The **use-harddisk** keyword is available only on the ASR 5000 and ASR 5500 chassis.

```plaintext
purge { storage-limit storage_limit | time-limit time_limit } [ max-files max_records_to_purge ]
```

Specifies to purge/delete the EDR records based on "time" or "volume" limit. When the configured threshold limit is reached on the hard disk drive, the records that are created dynamically in the `/mnt/hd-raid/data/records/` directory are automatically deleted. Files that are manually created should be deleted manually.

- **storage-limit storage_limit**: Specifies to start deleting files when the specified megabytes of space is used for storage. `storage_limit` specifies the volume limit for the record files, in megabytes, and must be an integer from 10 through 143360.
- **time-limit time_limit**: Specifies to start deleting files older than the specified time limit. `time_limit` specifies the time limit for the record files, and must be an integer from 600 through 2592000.
- **max-files max_records_to_purge**: Specifies the maximum number of records to purge. `max_records_to_purge` can be 0, or an integer from 1000 through 10000. If the value is set to 0, during each cycle, the records will be deleted until the purge condition is satisfied. If the value is set between 1000 and 10000, during each cycle, the records will be deleted until either the purge condition is satisfied or the number of records deleted equals the configured `max-files` value.

Default: 0

```plaintext
push-interval push_interval
```

Specifies the transfer interval (in seconds) to push EDR and UDR files to an external file server. `push_interval` must be an integer from 60 through 3600.

Default: 300

```plaintext
push-trigger space-usage-percent trigger_percentage
```

Specifies the EDR/UDR disk space utilization percentage, upon reaching which an automatic push is triggered and files are transferred to the configured external server. `trigger_percentage` specifies the EDR/UDR disk utilization percentage for triggering push, and must be an integer from 10 through 80.

Default: 80

```plaintext
remove-file-after-transfer
```

Specifies that the system must delete EDR/UDR files after they are transferred to the external file server. Default: Disabled
transfer-mode { pull [ module-only ] | push primary { encrypted-url encrypted_url | url url } [ [ max-files max_records ] [ max-tasks task_num ] [ module-only ] [ secondary { encrypted-secondary-url encrypted_secondary_url | secondary-url secondary_url } ] [ via local-context ] + ] }

Specifies the EDR/UDR file transfer mode—how the EDR and UDR files are transferred to an external file server.

- **pull**: Specifies that the L-ESS (for ASR 5000) or external server (for ASR 5500) is to pull the EDR files.
- **push**: Specifies that the system is to push EDR files to the configured L-ESS (for ASR 5000) or external server (for ASR 5500).
- **max-files max_records**: Specifies the maximum number of files sent per iteration based on configured file size.
  Default: 4000
- **max-tasks task_num**: Specifies the maximum number of tasks (child processes) that will be spawned to push the files to the remote server. The `task_num` must be an integer from 4 through 8.
  Default: 4

**Important**: Note that increasing the number of child processes will improve the record transfer rate. However, spawning more child will consume additional resource. So, this option needs to be used with proper resource analysis.

- **module-only**: Specifies that the transfer-mode is only applicable to the EDR module; if not configured it is applicable to both EDR and UDR modules. This enables to support individual record transfer-mode configuration for each module.
- **primary encrypted-url encrypted_url**: Specifies the primary URL location in encrypted format to which the system pushes the EDR files.
  `encrypted_url` must be the location in an encrypted format, and must be an alphanumeric string of 1 through 1024 characters.
- **primary url url**: Specifies the primary URL location to which the system pushes the EDR files.
  `url` must be the location, and must be an alphanumeric string of 1 through 1024 characters in the “//user:password@host:[port]/directory” format.
- **secondary encrypted-secondary-url encrypted_secondary_url**: Specifies the secondary URL location in encrypted format to which the system pushes the EDR files when the primary location is unreachable or fails.
  `encrypted_secondary_url` must be the secondary location in an encrypted format, and must be an alphanumeric string of 1 through 1024 characters in the “//user:password@host:[port]/directory” format.
- **secondary secondary-url secondary_url**: Specifies the secondary location to which the system pushes the EDR files when the primary location is unreachable or fails.
  `secondary_url` must be the secondary location, and must be an alphanumeric string of 1 through 1024 characters in the “//user:password@host:[port]/directory” format.
- **via local-context**: Configuration to select LC/SPIO for transfer of EDRs. The system pushes the EDR files via SPIO in the local context.
use-harddisk

**Important:** The `use-harddisk` keyword is available only on the ASR 5000 and ASR 5500 chassis.

**ASR 5000:** Specifies that on the ASR 5000 chassis the hard disk on the SMC be used to store EDR/UDR files. On configuring to use the hard disk for EDR/UDR storage, EDR/UDR files are transferred from packet processing cards to the hard disk on the SMC. Default: Disabled

**ASR 5500:** Specifies that on the ASR 5500 chassis the hard disk the FSC hard disk array be used to store EDR/UDR files. On configuring to use the hard disk for EDR/UDR storage, EDR/UDR files are transferred from DPCs to the hard disk array. Default: Disabled

+ Indicates that more than one of the previous keywords can be entered within a single command.

**Usage**

Use this command to configure how the EDRs are moved and stored.

On the ASR 5000 or ASR 5500 chassis, you must run this command only from the local context. If you run this command in any other context it will fail and result in an error message.

If PUSH transfer mode is configured, the L-ESS (for ASR 5000) or external server (for ASR 5500) URL to which the EDR files need to be transferred to must be specified. The configuration allows a primary and a secondary server to be configured. Configuring the secondary server is optional. Whenever a file transfer to the primary server fails for four consecutive times, the files will be transferred to the secondary server. The transfer will switch back to the original primary server when:

- Four consecutive transfer failures to the secondary server occur.
- After switching from the primary server, 30 minutes elapses.

When changing the transfer-mode from pull to push, disable the PULL from the L-ESS (for ASR 5000) or external server (for ASR 5500) and then change the transfer mode to push. Make sure that the push server URL configured is accessible from the local context. Also, make sure that the base directory that is mentioned contains udr directory created within it.

When changing the transfer mode from push to pull, after changing, enable PULL on the L-ESS (for ASR 5000) or external server (for ASR 5500). Any of the ongoing PUSH activity will continue till all the scheduled file transfers are completed. If there is no PUSH activity going on at the time of this configuration change, all the PUSH related configuration is nullified immediately.

The `cdr use-harddisk` command is available only on the ASR 5000 and ASR 5500 chassis. This command can be run only in a context where CDRMOD is running. Configuring in any other context will result in failure with the message “Failure: Please Check if CDRMOD is running in this context or not.”

The `cdr use-harddisk` command can be configured either in the EDR or UDR module, but will be applicable to both record types. Configuring in one of the modules will prevent the configuration to be applied in the other module. Any change to this configuration must be done in the module in which it was configured, the change will be applied to both record types.

The VPNMgr can send a maximum of 4000 files to the remote server per iteration. However if the individual file size is big (say when compression is not enabled), then while transferring 4000 files SFTP operation takes a lot of time. To prevent this, the `cdr transfer-mode push` command can be configured with the keyword `max-files`, which allows operators to configure the maximum number of files sent per iteration based on configured file size.

**Example**

The following command retains a copy of the data file after it has been transferred to the storage location:
no cdr remove-file-after-transfer
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
end
```

**Usage**

Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Use this command to return to the parent configuration mode.
file

This command allows you to configure EDR file parameters.

Product  
All

Privilege  
Security Administrator, Administrator

Mode  
Exec > Global Configuration > Context Configuration > EDR Module Configuration

```
configure > context context_name > edr-module active-charging-service
```

Entering the above command sequence results in the following prompt:

```text
[context_name]host_name(config-edr)#
```

Syntax

```
file [ charging-service-name { include | omit } ] [ compression { gzip | none } ] [ current-prefix string ] [ delete-timeout seconds ] [ directory directory_name ] [ edr-format-name ] [ exclude-checksum-record ] [ field-separator { hyphen | omit | underscore } ] [ file-sequence-number rulebase-seq-num ] [ headers ] [ name file_name ] [ reset-indicator ] [ rotation [ num-records number | tariff-time minute minute_value hour hour_value | time seconds | volume bytes ] ] [ sequence-number { length length | omit | padded | padded-six-length | unpadded } ] [ storage-limit limit ] [ single-edr-format ] [ time-stamp { expanded-format | rotated-format | unix-format } ] [ trailing-text string ] [ trap-on-file-delete ] [ unique-seq-num ] [ xor-final-record ] +
```

default file [ charging-service-name ] [ compression ] [ current-prefix ] [ delete-timeout ] [ directory ] [ edr-format-name ] [ field-separator ] [ file-sequence-number ] [ headers ] [ name ] [ reset-indicator ] [ rotation [ num-records | tariff-time | time | volume ] ] [ sequence-number ] [ storage-limit ] [ time-stamp ] [ trailing-text ] [ unique-seq-num ] +

---

default

Configures the default setting for the specified keyword(s).

---

charging-service-name { include | omit }

Specifies to include/exclude name of the charging service in the file name.

- **include**: Include name of the charging service in the EDR file name.
- **omit**: Exclude name of the charging service in EDR file name.

---

compression { gzip | none }

Specifies compression of EDR files.

- **gzip**: Enables GNU zip compression of the EDR file at approximately 10:1 ratio.
- **none**: Disables Gzip compression.
**current-prefix** *string*

Specifies a string to add to the beginning of the EDR file that is currently being used to store EDR records.

*string* must be an alphanumeric string of 1 through 31 characters.

Default: **curr**

**delete-timeout** *seconds*

Specifies a timeout period (in seconds) when completed EDR files are deleted. By default, files are never deleted.

*seconds* must be an integer from 3600 through 31536000.

Default: Disabled

**directory** *directory_name*

Specifies a subdirectory in the default directory in which to store EDR files.

*directory_name* must be an alphanumeric string of 1 through 191 characters.

Default: */records/edr*

**edr-format-name**

Specifies creation of separate files for EDRs that have different formats. Name of the EDR format is included in the file name.

**exclude-checksum-record**

When entered, this keyword excludes the final record containing #CHECKSUM followed by the 32-bit Cyclic redundancy check (CRC) of all preceding records from the EDR file.

Default: Disabled (inserts checksum record into the EDR file header)

**field-separator** [ *hyphen|omit|underscore* ]

Specifies the field inclusion/exclusion type of separators between two fields of EDR file name:

- **hyphen**: Specifies to use “-” (hyphen) as the field separator.
- **omit**: Excludes the field separator.
- **underscore**: Specifies to use “_” (underscore) as the field separator.

**file-sequence-number** *rulebase-seq-num*

Specifies that the file name sequence numbers must be unique per rulebase and EDR format name combination.

**headers**

Includes a file header summarizing the record layout.

**name** *file_name*

Specifies a string to be used as the base file name for EDR files.

Default: **edr**

*file_name* must be an alphanumeric string of 1 through 31 characters. The file name format is as follows:

- **base**: Specifies the type of record in file or contains the operator-specified string.
  
  Default: edr
• **rulebase**: Specifies the name of the ACS rulebase. EDRs from different rulebases go into different EDR files.

• **format**: Specifies the name of the EDR format if `single-edr-format` is specified, else the format field (and the trailing underscore) is omitted from the file name.

• **sequencenum**: This is a 5-digit sequence number to detect the missing file sequence. It is unique among all EDR files on the system.

• **timestamp**: Contains a timestamp based on file creation time in UTC time in MMDDYYYYHHMMSS format.

EDR files that have not been closed have a string added to the beginning of their filenames.

Filename for an EDR file in CSV format that contains information for rulebase named `rulebase1` and an EDR schema named `edr_schema1` appears as follows:

```plaintext
edr_rulebase1_edr_schema1_00005_01302006143409
```

If the file name is not configured the system will create files for EDRs/UDRs/FDRs (xDRs) using the following template with limits to 256 characters:

```plaintext
basename_ChargSvcName_timestamp_SeqNumResetIndicator_FileSeqNumber
```

• **basename**: A global-based configurable text string that is unique per system that uniquely identifies the global location of the system running ACS.

• **ChargSvcName**: A system context-based configurable text string that uniquely identifies a specific context-based charging service

• **timestamp**: Date and time at the instance of file creation. Date and time in the form of “MMDDYYYYHHmmSS” where HH is a 24-hour value from 00-23

• **SeqNumResetIndicator**: A one-byte counter used to discern the potential for duplicated FileSeqNumber with a range of 0 to 255, which is incremented by a value of 1 for the following conditions:

  • Failure of an ACS software process on an individual PSC.

  • Failure of the system such that a second system takes over. For example, a backup or standby system put in place according to Interchassis Session Recovery.

  • File Sequence Number (FileSeqNumber) rollover from 999999999 to 0

• **FileSeqNumber**: Unique file sequence number for the file with 9 digit integer having range from 000000000 to 999999999. It is unique on each system.

File name for a closed xDR file in CSV format that contains information for ACS system `xyz_city1` and charging service name `prepaid2` with timestamp `12311969190000`, and file sequence number counter reset indicator to 002 for file sequence number `034939002` appears as follows:

```plaintext
xyz_city1_prepaid2_12311969190000_002_034939002
```

File name for a running xDR file, not closed, in CSV format that contains information for the same parameters for file sequence number `034939003` prefixed with `curr_` and appears as follows:

```plaintext
curr_xyz_city1_prepaid2_12311969190000_002_034939002
```

---

**Important**: When the "rulebase name" and "edr-format-name" options are enabled through this `file` command, if the "field-separator" value is "underscore" (default value) then, in the filename, the fields Rulebase name and EDR format name will be separated by "hyphen". If the "field-separator" value is "hyphen" then, in the filename, the fields Rulebase name and EDR format name will be separated by "underscore". This will ensure that the number of the fields in the filename is not increased and does not affect the backend billing system.
reset-indicator

Specifies inclusion of the reset indicator counter value, from 0 through 255, in the EDR file name, and is incremented (by one) whenever any of the following conditions occur:
- An ACSMgr/SessMgr process fails.
- A peer chassis has taken over in compliance with our Interchassis Session Recovery feature.
- The sequence number, see the sequence-number keyword, has rolled over to zero.

rotation { num-records number | tariff-time minute minute_value hour hour_value | time seconds | volume bytes }

Specifies when to close an EDR file and create a new one.
- **num-records number**: Specifies the number of records that should be added to the file. When the number of records in the file reaches the specified value, the file is complete.
  - *number* must be an integer from 100 through 10240.
  - Default: 1024
- **time seconds**: Specifies the period of time (in seconds) to wait before closing the EDR file and creating a new one.
  - *seconds* must be an integer from 30 through 86400.
  - Default: 3600
- **tariff-time minute minute_value hour hour_value**: Specifies the time of day (hour and minute) at which the files are rotated once per day.
  - *minute_value* is an integer value from “0” up to “59”.
  - *hour_value* is an integer value from “0” up to “23”.

**Important**: The options **time** and **tariff-time** are mutually exclusive and only any one of them can be configured. Other file rotation options can be used with either of them.

- **volume bytes**: Specifies the maximum size (in bytes) of the EDR file before closing it and creating a new one.
  - *bytes* must be an integer from 51200 through 62914560.
  - Note that a higher setting may improve the compression ratio when the compression keyword is set to gzip.

sequence-number { length length | omit | padded | padded-six-length | unpadded }

Specifies including/excluding sequence number in the file name.
- **length length**: Includes the sequence number with the specified length.
  - *length* must be the length of the file sequence number, with preceding zeroes, in the file name, and must be an integer from 1 through 9.

**Important**: The **length** keyword is applicable in both EDR and UDR modules. When applied in both modules without the **file udr-seq-num** configuration, the minimum among the two values will come into effect for both the modules. With the **file udr-seq-num** keyword, each module will use its own value of length.
• omit: Excludes the sequence number from the file name.

• padded: Includes the padded sequence number with preceding zeros in the file name. This is the default setting.

• padded-six-length: Includes the padded sequence number with six preceding zeros in the file name.

• unpadded: Includes the unpadded sequence number in the file name.

**single-edr-format**

Creates separate files for EDRs having different formats.
Default: Disabled

**storage-limit limit**

Specifies deleting files when the specified amount of space (in bytes) is used up for EDR/UDR file storage RAM on packet processing cards.

**Important:**

ASR 5000 and ASR 5500: limit must be an integer from 10485760 through 536870912. Default: 33554432

**Important:** The total storage limit is 536870912 bytes (512 MB). This limit is for both UDR and EDR files combined.

**time-stamp { expanded-format | rotated-format | unix-format }**

Specifies the timestamp of when the file was created be included in the file name.
- expanded-format: Specifies the UTC MMDDYYYYHHMMSS format.
- rotated-format: Specifies the time stamp format to YYYYMMDDHHMMSS format.
- unix-format: Specifies the UNIX format of x.y, where x is the number of seconds since 1/1/1970 and y is the fractional portion of the current second that has elapsed.

**trailing-text string**

Specifies the inclusion of an arbitrary text string in the file name.
string must be an alphanumeric string of 1 through 30 characters.

**trap-on-file-delete**

Instructs the system to send an SNMP notification (starCDRFileRemoved) when an EDR/UDR file is deleted due to lack of space.
Default: Disabled

**unique-seq-num**

Specifies that the file sequence numbers that are part of the EDR file names be independently generated. If disabled, a single set of sequence numbers are shared by both UDR and EDR files.
Default: Disabled
xor-final-record

Specifies inserting an XOR checksum (in place of the CRC checksum) into the EDR file header if the exclude-checksum-record is left at its default setting.

Default: Disabled

+

Indicates that more than one of the keywords can be entered in a single command.

Usage

Use this command to configure EDR file characteristics.

Example

The following command sets the prefix of the current active EDR file to Current:

```
file current-prefix Current
```

The following command sets the base file name to EDRfile:

```
file name EDRfile
```
The eGTP Service Configuration Mode is used to create and manage Evolved GPRS Tunneling Protocol (eGTP) interface types and associated parameters.

**Mode**

Exec > Global Configuration > Context Configuration > eGTP Service Configuration

`configure > context context_name > egtp-service service_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-egtp-service)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
associate

Configures an association with a GTP-U service where parameters are applied to the GTP-U data flow. For an SGSN being configured for S4 functionality, this command associates a configured GTP-U service that will enable communication with the SGW over the S4 interface.

**Product**
- ePDG
- P-GW
- SAEGW
- SGSN

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > eGTP Service Configuration

`configure > context context_name > egtp-service service_name`

Entering the above command sequence results in the following prompt:

`[context_name] host_name(config-egtp-service)#`

**Syntax**

```
associate gtpu-service name

no associate gtpu-service
```

**Usage**

Use this command to associate a GTP-U service with this eGTP service.

**Example**

The following command associates this eGTP service with a GTP-U service named `gtpu3`:

```
associate gtpu-service gtpu3
```
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Use this command to return to the parent configuration mode.
Configure the GPRS Tunneling Protocol Control (GTP-C) plane settings for this service.

**Product**
- ePDG
- MME
- P-GW
- SAEGW
- S-GW
- SGSN

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > eGTP Service Configuration

```
configure > context context_name > egtp-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-egtp-service)#
```

**Syntax**

```
gtpc { bind { ipv4-address ipv4_address [ ipv6-address ipv6_address ] | ipv6-address ipv6_address [ ipv4-address ipv4_address ] } | echo-interval seconds [ dynamic [ smooth-factor multiplier ] ] } | echo-retransmission-timeout seconds | error-response-handling | ip qos-dscp { forwarding_type } | max-retransmissions num | node-feature { pgw-restart-notification } } | path-failure detection-policy echo | retransmission-timeout seconds | retransmission-timeout-ms milliseconds }

no gtpc { bind { ipv4-address ipv4_address [ ipv6-address ipv6_address ] | ipv6-address ipv6_address [ ipv4-address ipv4_address ] } | echo-interval | node-feature { pgw-restart-notification } } | path-failure detection-policy }

default gtpc { echo-interval | echo-max-retransmissions | echo-retransmission-timeout | ip qos-dscp | max-retransmissions | node-feature { pgw-restart-notification } | path-failure detection-policy | retransmission-timeout | retransmission-timeout-ms }

```

# Disables or removes the configured GTP-C setting.

**default**

Resets the specified parameter to its default value.

```
bind { ipv4-address ipv4_address [ ipv6-address ipv6_address ] | ipv6-address ipv6_address [ ipv4-address ipv4_address ] }
```

Binds the service to an interface with an IPv4 address, IPv6 address or both.
ipv4-address ipv4_address [ ipv6-address ipv6_address ]: Binds this service to the IPv4 address of a configured interface. Optionally, bind the service to a configured interface with an IPv6 address. ipv4_address must be entered using IPv4 dotted-decimal notation. ipv6_address must be entered using IPv6 colon-separated-hexadecimal notation.

ipv6-address ipv6_address [ ipv4-address ipv4_address ]: Binds this service to the IPv6 address of a configured interface. Optionally, bind the service to a configured interface with an IPv4 address. ipv6_address must be entered using IPv6 colon-separated-hexadecimal notation. ipv4_address must be entered using IPv4 dotted-decimal notation.

**Important:** For binding GTP-C service on S2b interface; either IPv6 or IPv4 bind address shall be used; binding both v4 and v6 address is not supported on ePDG. The ipv6-address ipv6_address [ ipv4-address ipv4_address ] option is not currently supported on the SGSN.

echo-interval seconds [ dynamic [ smooth-factor multiplier ] ]

Configures the duration (in seconds) between the sending of echo request messages as an integer from 60 through 3600. Default: 60

dynamic: Enables the dynamic echo timer for the eGTP service. The dynamic echo timer uses a calculated round trip timer (RTT) to support variances in different paths to peer nodes.

smooth-factor multiplier: Introduces a multiplier into the dynamic echo timer as an integer from 1 through 5. Default: 2

echo-retransmission-timeout seconds

Default: 3

Configures the echo retransmission timeout, in seconds, for the eGTP service as an integer ranging from 1 to 20.

If dynamic echo is enabled (gtpc echo-interval dynamic) the value set in this command serves as the dynamic minimum (if the RTT multiplied by the smooth factor is less than the value set in this command, the service uses this value).

ip qos-dscp { forwarding_type }

Specifies the IP QoS DSCP per-hop behavior (PHB) to be marked on the outer header of signalling packets originating from the LTE component. This is a standards-based feature (RFC 2597 and RFC 2474).

Note that CS (class selector) mode options below are provided to support backward compatibility with the IP precedence field used by some network devices. CS maps one-to-one to IP precedence, where CS1 is IP precedence value 1. If a packet is received from a non-DSCP aware router that used IP precedence markings, then the DSCP router can still understand the encoding as a Class Selector code point.

The following forwarding types are supported:

- **af11**: Designates the use of Assured Forwarding 11 PHB.
  
  This is the default setting.

- **af12**: Designates the use of Assured Forwarding 12 PHB.

- **af13**: Designates the use of Assured Forwarding 13 PHB.

- **af21**: Designates the use of Assured Forwarding 21 PHB.

- **af22**: Designates the use of Assured Forwarding 22 PHB.

- **af23**: Designates the use of Assured Forwarding 23 PHB.

- **af31**: Designates the use of Assured Forwarding 31 PHB.
- `af32`: Designates the use of Assured Forwarding 32 PHB.
- `af33`: Designates the use of Assured Forwarding 33 PHB.
- `af41`: Designates the use of Assured Forwarding 41 PHB.
- `af42`: Designates the use of Assured Forwarding 42 PHB.
- `af43`: Designates the use of Assured Forwarding 43 PHB.
- `be`: Designates the use of Best Effort forwarding PHB.
- `cs1`: Designates the use of Class Selector code point “CS1”.
- `cs2`: Designates the use of Class Selector code point “CS2”.
- `cs3`: Designates the use of Class Selector code point “CS3”.
- `cs4`: Designates the use of Class Selector code point “CS4”.
- `cs5`: Designates the use of Class Selector code point “CS5”.
- `cs6`: Designates the use of Class Selector code point “CS6”.
- `cs7`: Designates the use of Class Selector code point “CS7”.
- `ef`: Designates the use of Expedited Forwarding PHB typically dedicated to low-loss, low-latency traffic.

The assured forwarding behavior groups are listed in the table below.

<table>
<thead>
<tr>
<th>Class</th>
<th>Class 1</th>
<th>Class 2</th>
<th>Class 3</th>
<th>Class 4</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Low Drop</strong></td>
<td>AF11</td>
<td>AF21</td>
<td>AF31</td>
<td>AF41</td>
</tr>
<tr>
<td><strong>Medium Drop</strong></td>
<td>AF12</td>
<td>AF22</td>
<td>AF32</td>
<td>AF42</td>
</tr>
<tr>
<td><strong>High Drop</strong></td>
<td>AF13</td>
<td>AF23</td>
<td>AF33</td>
<td>AF43</td>
</tr>
</tbody>
</table>

Traffic marked with a higher class is given priority during congestion periods. If congestion occurs to traffic with the same class, the packets with the higher AF value are dropped first.

```plaintext
max-retransmissions num
```

Configures the maximum number of retries for packets as an integer from 0 through 15. Default: 4
After max retransmissions is reached, the path is considered to be failed.

```plaintext
node-feature pgw-restart-notification
```

Enables P-GW Restart Notification functionality. Node will start announcement of new supported features to peer nodes in echo as soon as configuration is added.
Default: Disabled

```plaintext
path-failure detection-policy echo
```

Enables session cleanup upon path failure detected via ECHO timeout toward a peer.
Default: Enabled
If disabled, there is no session cleanup upon path failure detected via ECHO timeout toward a peer; however, SNMP trap/logs will continue to indicate path failure.
retransmission-timeout  seconds

**Important:** In 17.3 and later releases, this option has been deprecated. Use retransmission-timeout-ms.

Configures GTPv2 control packets (non-echo) retransmission timeout (in seconds) as an integer from 1 through 20. Default: 5

**Usage**

Use this command to configure GTP-C settings for the current service. This interface assumes the characteristics of an S11 reference point on the S-GW or MME. For communication between the S4-SGSN and the LTE S-GW, the interface assumes the characteristics of an S4 reference point on the S4-SGSN. Before using the `gtpc` command on the S4-SGSN, a new or existing service must be created or entered using the `egtp-service` command in Context Configuration Mode. Once the eGTP service is configured, the service must be associated with the configured 2G and/or 3G services on the S4-SGSN using the `associate` command in SGSN Service Configuration Mode and/or GPRS Service Configuration Mode.

**Important:** For ePDG, IPv6 bind address should be used as ePDG supports IPv6 as transport on S2b interface.

**Example**

The following command binds the service to a GTP-C interface with an IPv4 address of 112.104.215.177:

```
gtpc bind ipv4-address 112.104.215.177
```
**interface-type**

Configures the interface type used by this service.

**Product**
- ePDG
- MME
- P-GW
- SAEGW
- S-GW
- SaMOG
- SGSN

**Important:** Prior to release 16, the SGSN only supported this command on the ASR 5000 platform.

**Privilege**
- Administrator

**Mode**
- Exec > Global Configuration > Context Configuration > eGTP Service Configuration
- configure > context context_name > egtp-service service_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-egtp-service)#
```

**Syntax**

```
interface-type { interface-cgw-egress | interface-epdg-egress | interface-mme | interface-pgw-ingress | interface-sgsn | interface-sgw-egress | interface-sgw-ingress }
```

- **interface-cgw-egress**: Specifies the SaMOG Gateway's EGTP interface for egress.
- **interface-epdg-egress**: Specifies that the interface has the characteristics of an ePDG's egress EGTP interface.
- **interface-mme**: Specifies that the interface has the characteristics of an eGTP MME S11 reference point to/from an S-GW or an eGTP MME Sv reference point to/from a Mobile Switching Center (MSC).
- **interface-pgw-ingress**: Specifies that the interface has the characteristics of an eGTP P-GW S5/S8 reference point from an S-GW. The interface assumes the characteristics of either a GTP-C (control Plane) or GTP-U (user plane) reference point.
- **interface-sgsn**: Specifies that the interface has the characteristics of an eGTP S-GW S4 reference point to/from an SGSN. On an S4-SGSN, this option specifies that the eGTP service is used for an S4-SGSN and gives the service the characteristics required for messaging towards an SGW (S4) / MME (S3) / S4-SGSN (S16).
- **interface-sgw-egress**: Specifies that the interface has the characteristics of an eGTP S-GW S5/S8 reference point to an eGTP P-GW. The interface assumes the characteristics of either a GTP-C (control Plane) or GTP-U (user plane) reference point.
**interface-type**

**interface-sgw-ingress**: Specifies that the interface has the characteristics of:
- an eGTP-C S-GW S11 reference point from the MME.
- an eGTP-U S-GW S1-U reference point from the eNodeB.

**Usage**

Use this command to specify the type of interface this service uses. By configuring this command, the interface takes on the characteristics of the selected type.

Disable specific interface support for P-GW by entering the following command:

```
interface-type interface-pgw-ingress
```

**Example**

The following command configures the interface bound to this service to maintain the characteristics of an eGTP-C S-GW S11 reference point from an MME:

```
interface-type interface-sgw-ingress
```

The following command accepts or rejects Create Session Request (CSR) on GTP based S2a interface.

```
interface-type interface-pgw-ingress s2a
```
pool

This command enables the default S4-SGSN functionality for (flex) pooling and enables inclusion of the configured pool hop-counter count in new SGSN context/identity request messages. This command supports S4-SGSN pooling across the S16 interface. The S16 interface provides a GTPv2 path to a peer S4-SGSN. Support for this interface is provided as part of the S4 interface license. This command sets the S4-SGSN as the default SGSN within a pool. If the default S4-SGSN receives an inbound SGSN context request, it forwards it to the right SGSN in the pool based on the NRI bits of the P-TMSI.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > eGTP Service Configuration

configure > context context_name > egtp-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-egtp-service)#

Syntax

pool { default-sgsn | hop-counter count }

no pool default-sgsn

no

Disables the default SGSN pooling functionality or removes the SGSN pool hop-counter IE from the GTP Identity/context requests.

default-sgsn

Enables default SGSN pooling functionality.

hop-counter count

Enables and configures the SGSN pool hop-counter to set the number of hops and to include the configured count in the new SGSN Context Requests or the new SGSN Identity Requests. If default-sgsn is enabled, then any messages relayed will have the default value of 4 for the counter if the message does not include this hop-counter ID.

count: Enter an integer from 1 to 255.

Default: 4

Usage

Use this command to enable the default flex functionality without exposing the pool (flex) structure. This functionality provides a means for SGSNs outside of the pool to reach a pooled SGSN on the basis of its NRI. Once the pooling has been enabled, Repeat the command using the hop-counter keyword to enable inclusion of the hop-counter IE in SGSN context/identity request messages and to configure the count for the
pooling hop-counter. If the SGSN is behaving as the ‘default SGSN’, this SGSN will forward (relay) requests with the hop-count included to the target SGSN.

**Example**

Enable the default pooling functionality which allows an outside SGSN to reach a pooled SGSN:

```
pool default-sgsn
```

Set the hop-count to be included in messages to 25:

```
pool hop-count
```
**validation-mode**

Configures the type of validation to be performed on messages received by this service.

**Product**
ePDG
P-GW
SAEGW
SGSN

**Important:** The ePDG and SGSN are not currently supported on the ASR 5500 platform.

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > eGTP Service Configuration

```
configure > context context_name > egtp-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-egtp-service)#
```

**Syntax**

```
validation-mode { custom1 | standard }

default validation-mode
```

<table>
<thead>
<tr>
<th><strong>default</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Returns the command to the default setting of <strong>standard</strong>.</td>
</tr>
</tbody>
</table>

{ **custom1** | **standard** }

**custom1:** Specifies that the message should be validated based on a vendor-specific set of mandatory elements.

**standard:** Specifies that the message should be validated based on the set of mandatory elements as defined in 3GPP 29.274. This is the default option on an S4-SGSN.

**Usage**

Use this command to specify the type of validation performed on messages received by this service. The information elements contained in messages have mandatory elements and conditional elements. The standard set of elements, as defined by 3GPP 29.274 is checked if this command is set to “standard”. The **custom1** setting is for a vendor-specific set of mandatory elements.

**Example**

The following command sets the validation mode for incoming messages to **standard**:

```
validation-mode standard
```
validation-mode
Chapter 121
EPDG Service Configuration Mode Commands

Creates Evolved Packet Data Gateway service and enters EPDG service configuration mode.

Mode

Exec > Global Configuration > Context > EPDG Service Configuration

configure > context context_name > epdg service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-epdg-service)#
aaa

This command configures aaa parameters for ePDG service.

**Product**
ePDG

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
aaa send framed-mtu value
aaa send framed-mtu
```

- `no`
  Disables aaa parameters for ePDG service.

- `send`
  Configures AVP to be send to AAA server.

  ```plaintext
  framed-mtu value
  ```
  This is the framed-MTU AVP value to be sent in DER, which is an integer between 64 through 1500.

**Usage**

Use this command to configure aaa parameters for ePDG service.

**Example**

The following command is used to configures aaa parameters framed-MTU AVP value 100 to be send to AAA for ePDG service.

```plaintext
aaa send framed-mtu 100
```
allow

This command allows duplicate precedence in a TFT for a S2b ePDG session.

**Product**
ePDG

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context > EPDG Service Configuration

`configure > context context_name > epdg service service_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-epdg-service)#
```

**Syntax**

```
[ no ] allow { | duplicate-prec-in-tft }
```

- **no**
  Disables allowing exception.

- **custom-swm-swu-error-mapping**
  Customises mapping of SWm errors with SWu Notify Error Type.

- **duplicate-prec-in-tft**
  The duplicate precedence is allowed in a tft for a S2b ePDG session.

**Usage**

Use this command to allow exception with Spec or RFC.

**Example**

The following command is used to allow duplicate precedence in a tft for a S2b ePDG session.

```
allow duplicate-prec-in-tft
```
associate

This command associates configuration of ePDG service to qos mapping and EGTP service.

Product

ePDG

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > Context > EPDG Service Configuration

configure > context context_name > epdg service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-epdg-service)#

Syntax

associate {egtp-service egtp_service_name | qci-qos-mapping qci-qos_mapping | subscriber-map subscriber_map_name }:

no associate {egtp-service | qci-qos-mapping | subscriber-map }

no

Disables association.

egtp-service egtp_service_name

The eGTP service should be configured before associating the same with ePDG service.

egtp_service_name is a string and the value must be between 1 and 63.

qci-qos-mapping qci-qos_mapping

The associated qci-qos mapping table should be configured prior to associating the same with ePDG service.

qci-qos_mappingis a string and the value must be between 1 and 63.

subscriber-map subscriber_map_name

Configures subscriber map association to get PGW address locally.

subscriber_map_name is a string and the size must be between 1 and 64.

Usage

Use this command to associate the ePDG service to egtp service or QCI to QoS mapping.

Example

The following command removes the association of epdg service to egtp service.

    no associate egtp-service
bind

This command binds the services.

Product
ePDG

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context > EPDG Service Configuration

configure > context context_name > epdg service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-epdg-service)#

Syntax

bind address bind_address crypto-template crypto_template_service_name

no bind address

no
Disables binding.

address bind_address
Specifies the address of the EPDG service. This must be followed by an IPv4 address, using dotted-decimal notation or an IPv6 address, using xx::yy::zz format.

crypto-template crypto_template_service_name
Specifies the crypto template to use, this is a string of size between 0 and 127.

Usage
Use this command to bind the ePDG service.

Example
The following command binds the ePDG Service to the IPv4 adress 12.32.44.56.

    bind address 12.32.44.56
**dns-pgw**

Configures context of dns-client.

**Product**
ePDG

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context > EPDG Service Configuration

`configure > context context_name > epdg service service_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-epdg-service)#
```

**Syntax**

```
dns-pgw { context dns_client_context_name | selection { topology [ weight ] | weight } }

[ no | default ] dns-pgw { context | selection { topology [ weight ] | weight } }
```

**default**

Configures context of dns-client to its default value.

**no**

Disables dns-client's context.

**context dns_client_context_name**

Specifies the dns-client's context name, which is a string and should be between 1 and 79.

**selection { topology [ weight ] | weight }**

Specifies the pgw dns selection criteria.

- **topology**: Enables topology selection.
- **topology weight**: Enables topology with weight.
- **weight**: Enables selection with weight-only, disables topology selection.

**Usage**

Enable/disable PGW Selection based on topology and load-balancing of PGWs on weight's from DNS. Use this command to configure the source in which dns-client is configured, dns-pgw selection topology/weight will be used to enable/disable PGW Selection based on topology and load-balancing of PGWs.

**Example**

Use the following command to configure dns-client context.

```
dns-pgw context 21
```
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Use this command to return to the parent configuration mode.
fqdn

Designates ePDG fully qualified domain name.

**Product**
ePDG

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context > EPDG Service Configuration

```
configure > context context_name > epdg service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-epdg-service)#
```

**Syntax**

```
fqdn epdg_fqdn

[no | default ] fqdn
```

---

**default**
Resets the ePDG fully qualified domain name to its default setting.

---

**no**
Disables ePDG fqdn.

---

**fqdn epdg_fqdn**
Designates EPDG with fully qualified domain name, name is a string between 1 and 256 alphanumeric characters.

**Usage**

Use this command to configure ePDG FQDN under ePDG service which will we used for longest suffix match during dynamic allocation.

**Example**

Use the following command to disable ePDG a FQDN:

```
no fqdn
```
ip

This command configures Internet Protocol (IP) parameters.

Product
ePDG

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context > ePDG Service Configuration
configure > context context_name > epdg service service_name

Entering the above command sequence results in the following prompt:

/context_name/host_name(config-epdg-service)#

Syntax

ip fragment-chain { max-ooo-fragment fragments | timeout secs }
default ip fragment-chain { max-ooo-fragment | timeout }

default
Resets the ePDG Internet Protocol(IP) parameters to default values.

fragment-chain
This option configures ip fragment chain settings during TFT handling.

max-ooo-fragment fragments
This is the number of fragments to buffer per fragment chain for out-of-order reception before receiving first fragment(for L4 packet filtering).

fragments is an integer value between 0 through 300.
The default value is 45.
0 represents no buffering is done for out-of-order fragments, correct bearer will be selected with first fragment.

timeout secs
This is the time to hold an ip fragment chain.
secs is an integer value between 1 through 10.
The default value is 5.

Usage
Use this command to configure ePDG Internet Protocol (IP) parameters.

Example
Use the following command to configure ePDG IP parametr timeout to 6 seconds:

  ip fragment-chain timeout 6
**mobile-access-gateway**

Configures MAG context within epdg service.

**Product**
ePDG

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context > EPDG Service Configuration

```
configure > context context_name > epdg service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-epdg-service)#
```

**Syntax**

```
mobile-access-gateway context context-name [ mag-service mag-service-name ]
```

```
no mobile-access-gateway context
```

**Usage**

Use this command to specify where MIPv6 sessions are routed through this service.

**Example**

Use the following command to configure MAG context with context name fg.

```
mobile-access-gateway context fg
```
pgw-selection

Configures pgw-selection related parameters for the EPDG service.

Product

ePDG

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > Context > EPDG Service Configuration

configure > context context_name > epdg service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-epdg-service)#

Syntax

[ no ] pgw-selection { agent-info error-terminate }

no

Disables pgw-selection related parameters for the EPDG service.

pgw-selection agent-info error-terminate

agent-info specifies the action to be taken when MIP6-agent-info is expected but not received from AAA/HSS.
error-terminate terminates the pgw-selection and rejects the call.

Usage

Use this command to terminate the pgw-selection and reject the call MIP6-agent-info is expected but not received from AAA/HSS.

Example

Use the following command to terminate pgw-selection and reject the call.

    pgw-selection agent-info error-terminate
plmn

Configures PLMN related parameters for the EPDG service.

**Product**  
ePDG

**Privilege**  
Security Administrator, Administrator

**Mode**  
Exec > Global Configuration > Context > EPDG Service Configuration

```
configure > context context_name > epdg service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-epdg-service)#
```

**Syntax**

```
plmn id mcc mcc_plmn_id mnc mnc_plmn_id

no plmn id
```

**no**

Disables PLMN related parameters for the EPDG service.

```
plmn id mcc mcc_plmn_id mnc mnc_plmn_id
```

**plmn id mcc mcc_plmn_id**  
configures MCC part of PLMN ID for the EPDG service and prompts as “Enter a number, ranging from 200...999 - string of size 3 to 3”.
mcc_plmn_id is a string of three characters, entered as number between 200 and 999.

**mnc mnc_plmn_id**  
configures MNC part of PLMN ID for the EPDG service and prompts as “Enter a number, ranging from 00...999 - string of size 2 to 3”.
mnc_plmn_id is a string of two to three characters, entered as number between 00 and 999.

**Usage**

Use this command to configure PLMN identifier (MCC and MNC Values) for ePDG Service.

**Example**

Use the following command to configure PLMN identifier MCC 456 and MNC 64 for ePDG service.

```
plmn id mcc 456 mnc 64
```
setup-timeout

Maximum time allowed for session setup in seconds.

**Product**
ePDG

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context > EPDG Service Configuration

```
configure > context context_name > epdg service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-epdg-service)#
```

**Syntax**

```
setup-timeout time

default setup-timeout
```

**Example**

Use this command to configure maximum time allowed for session setup in seconds.

Use the following command to configure maximum session time as 120 seconds:

```
setup-timeout 120
```
**subscriber**

Configures a subscriber with a given name.

**Product**
ePDG

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context > EPDG Service Configuration

```console
configure > context context_name > epdg service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-epdg-service)#
```

**Syntax**

```
subscriber name

default subscriber name

no subscriber
```

---

**default**

Configures a subscriber with a given default name.

```
default
```

**no**

Cancels the subscriber configuration.

```
no
```

**subscriber name**

`name` is a string of size between 1 and 127.

**Usage**

Use this command to configure the subscriber with a given name.

**Example**

Use the following command to configure the subscriber as sss.

```
subscriber sss
```
**username**

Sets the options related to username received from mobile.

**Product**
ePDG

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context > EPDG Service Configuration

```
configure > context context_name > epdg service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-epdg-service)#
```

**Syntax**

```
username { check-mac-address [ failure-handling { continue | terminate } ] | mac-address-delimiter { NAI-label | colon | colon-or-NAI-label } | mac-address-stripping }
no username { check-mac-address | mac-address-stripping }
```

**Usage**

Use this command to set the options (Validate Mac address / mac-address-delimiter / mac-address-stripping) related to username received from mobile.

**Example**

Use the following command to set the options related to username received from mobile.
username check-mac-address failure-handling terminate
**vendor-specific-attr**

Configures the vendor-specific-attributes values on PMIP based S2b interface.

**Product**
ePDG

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context > EPDG Service Configuration

```
configure > context context_name > epdg service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-epdg-service)#
```

**Syntax**

```
vendor-specific-attr { dns-server-req { apco | pco } | pcscf-server-req { apco | private-extn } }

default vendor-specific-attr { dns-server-req | pcscf-server-req }
```

---

**default**

Configures vendor-specific-attributes to default the value. Default setting is to use APCO IE for DNS Server Address and PrivateExtension IE for PCSCF Server Address.

**dns-server-req**

Configures the DNS Server Address to be present in PCO/APCO IE.

**apco**

Configures to use APCO IE to carry information over PMIP based S2b.

**pco**

Configures to use PCO IE to carry information over PMIP based S2b.

**pcscf-server-req**

Configures the PCSCF Server Address to be present in APCO/PrivateExtn IE.

**apco**

Configures to use APCO IE to carry information over GTP based S2b.

**private-extn**

Configures to use PrivateExtension IE to carry information over GTP based S2b.
Usage
Use this command to configure the vendor-specific-attributes values on PMIP based S2b interface.

Example
Use the following command to configure the vendor-specific-attributes values on PMIP based S2b interface to pco.

```
vendor-specific-attr dns-server-req pco
```
Chapter 122
Ethernet Interface Configuration Mode Commands

The Ethernet Interface Configuration Mode is used to create and manage the IP interface parameters within a specified context.

Mode

Exec > Global Configuration > Context Configuration > Ethernet Interface Configuration

configure > context context_name > interface interface_name broadcast

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-if-eth)#

**Important:** Available commands or keywords/variables vary based on platform type, product version, and installed license(s).
bfd

Configures Bidirectional Forwarding Detection (BFD) interface parameters.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Ethernet Interface Configuration

```bash
cfgure > context context_name > interface interface_name broadcast
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-eth)#
```

**Syntax**

```
[no] bfd { echo | interval interval_num } min_rx milliseconds multiplier value
```

- **no**
  Disables the specified option on this interface.

- **echo**
  Enables BFD echo mode.
  BFD echo mode works with asynchronous BFD. Echo packets are sent by the forwarding engine and forwarded back along the same path in order to perform detection—the BFD session at the other end does not participate in the actual forwarding of the echo packets. The echo function and the forwarding engine are responsible for the detection process, therefore the number of BFD control packets that are sent out between two BFD neighbors is reduced.
  Since the forwarding engine is testing the forwarding path on the remote (neighbor) system without involving the remote system, there is an opportunity to improve the interpacket delay variance, thereby achieving quicker failure detection times than when using BFD Version 0 with BFD control packets for the BFD session.

- **interval interval_num**
  Specifies the transmit interval (in milliseconds) between BFD packets.
  - *For releases prior to 17.0, interval_num is an integer from 50 through 999. (Default 50)*
  - *For release 17.0 onwards, interval_num is an integer from 50 through 10000. (Default 50)*

- **min_rx milliseconds**
  Specifies the receive interval in milliseconds for control packets.
  - *For releases prior to 17.0, milliseconds is an integer from 50 through 999. (Default 50)*
  - *For release 17.0 onwards, milliseconds is an integer from 50 through 10000. (Default 50)*
**multiplier value**

Specifies the value used to compute the hold-down time as a number from 3 to 50.

**Usage**

Specify BFD parameters including echo mode and the transmit interval between BFD packets.

To apply enable echo mode on this interface, use the following command:

```
bfd echo
```

The following command sets BFD interval parameters:

```
bfd interval 3000 min_rx 300 multiplier 3
```
crypto-map

Applies the specified IPSec crypto-map to this interface.

Product

PDSN
HA

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > Context Configuration > Ethernet Interface Configuration

configure > context context_name > interface interface_name broadcast

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-if-eth)#

Syntax

```
crypto-map map_name [ secondary-address sec_ip_addr ]
```

no

Deletes the application of the crypto map on this interface.

```
map_name
```

Specifies the name of the crypto map being applied as an alphanumeric string of 1 through 127 characters that is case sensitive.

```
secondary-address sec_ip_addr
```

Applies the crypto map to the secondary address for this interface. `sec_ip_addr` must be specified using the IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

Usage

In order for ISAKMP and/or manual crypto maps to work, they must be applied to a specific interface using this command. Dynamic crypto maps should not be applied to interfaces. The crypto map must be configured in the same context as the interface.

Example

To apply the IPSec crypto map named cmap1 to this interface, use the following command:

```
crypto-map cmap1
```
description

Sets the descriptive text for the current interface.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Ethernet Interface Configuration

```
configure > context context_name > interface interface_name broadcast
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-eth)#
```

**Syntax**

```
description text

no description
```

**Usage**

Clears the description for the interface.

```
text
```

Specifies the descriptive text as an alphanumeric string of 0 through 79 characters.

**Example**

```
description sampleInterfaceDescriptiveText
```
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**
Use this command to return to the Exec mode.
**exit**

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Use this command to return to the parent configuration mode.
ip access-group

Specifies the name of the Access Control List (ACL) group to assign to the interface.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Ethernet Interface Configuration
configuration > context context_name > interface interface_name broadcast

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-if-eth)>

Syntax

[ no ] ip access-group group_name { in | out } priority

- no
  Removes the ACL group from this interface.

- group_name
  Specifies the name of an existing ACL group as an alphanumeric string of 1 through 47 characters.

Important: Up to eight ACLs can be applied to a group provided that the number of rules configured within the ACL(s) does not exceed the 128-rule limit for the interface.

- { in | out }
  Specifies whether the ACL group will apply to inbound or outbound traffic.

- priority
  If more than one ACL group is applied, priority-value specifies the priority in which they will be compared against the packet. If not specified, the priority is set to 0. priority-value must be an integer from 0 through 4294967295. If access groups in the list have the same priority, the last one entered is used first.

Usage

Specify the name of the Access Control List (ACL) group to assign to the interface along with its directionality and priority.

Example

ip access-group acl-101 in 56
**ip address**

Specifies the primary and optional secondary IPv4 addresses and subnets for this interface.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Ethernet Interface Configuration

```
configure > context context_name > interface interface_name broadcast
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-eth)#
```

**Syntax**

```
[ no ] ip address ip_address/mask [ secondary ip_address/mask ] [ srp-activate ]
```

- **no**
  Removes the ACL group from this interface.

- **ip_address/mask**
  Configures the IPv4 address for the interface specifying the networking mask as well. `ip_address` and `mask` must be entered using IPv4 dotted-decimal notation. CIDR notation is also accepted for the mask.

**Important:** For IPv4 addresses, 31-bit subnet masks are supported per RFC 3021.

- **secondary ip_address/mask**
  Configures a secondary IPv4 address on the interface.

**Important:** You must configure the primary IPv4 address before you will be allowed to configure a secondary address.

- **srp-activate**
  Activates the IP address for Interchassis Session Recovery (ICSR). Enable this IPv4 address when the Service Redundancy Protocol (SRP) determines that this chassis is ACTIVE.

**Usage**

Specify the primary and optional secondary IP addresses and subnets for this interface, as well as the SRP parameter for ICSR.

**Example**

```
ip address 192.154.3.5/24 srp-activate
```
**ip igmp profile**

Associates an Internet Group Management Protocol (IGMP) profile with this interface.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Ethernet Interface Configuration

```
configure > context context_name > interface interface_name broadcast
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-eth)#
```

**Syntax**

```
[ no ] ip igmp profile profile_name
```

- **no**
  Removes the IGMP profile from this interface.

- **profile_name**
  Specifies the name of an existing IGMP profile as an alphanumeric string of 1 through 63 characters. If the name is not for an existing profile, you are prompted to create a new profile. You are then moved to the IGMP Profile Configuration mode.

**Usage**
Associates an Internet Group Management Protocol (IGMP) profile with this interface.

**Example**

```
ip igmp profile default
```
**ip mtu**

Configures the Maximum Transmission Unit (MTU) for this IP interface.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Ethernet Interface Configuration

```
configure > context context_name > interface interface_name broadcast
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-eth)#
```

**Syntax**

```
[ no ] ip mtu mtu-size
```

- **no**
  - Removes the MTU value.

- **mtu-size**
  - Specifies the MTU in bytes as an integer from 576 though 2048.

**Usage**

IP MTU is supported for a normal interface and point-to-point interface (OLC ports).
The maximum MTU size allowed with an OLC port is 1600.
The maximum MTU size allowed with an Ethernet port is 2048. The default MTU size is 1500.
The maximum sizes for ethernet MTUs are:

- **Untagged traffic** (non-VLAN) – ip MPU mtu-size + ethernet header (20 bytes)
- **VLAN traffic** – ip MPU mtu-size + ethernet header (20 bytes) + vlan header (4 bytes)

**Example**

The following command sets the MTU value to **2048**.

```
ip mtu 2048
```
ip ospf authentication-key

Configures the password for authentication with neighboring Open Shortest Path First (OSPF) routers.

**Product**
- PDSN
- HA
- GGSN

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration > Context Configuration > Ethernet Interface Configuration
- `configure > context context_name > interface interface_name broadcast`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-eth)#
```

**Syntax**

```
ip ospf authentication-key [ encrypted ] password auth_key
no ip ospf authentication-key
```

- `no` Deletes the authentication key.
- `encrypted` Use this keyword if you are pasting a previously encrypted authentication key into the CLI command.
- `password auth_key` Specifies the password to use for authentication as an alphanumeric string of 1 through 16 characters entered in clear text format.

**Usage**

Use this command to set the authentication key used when authenticating with neighboring routers.

**Example**

To set the authentication key to 123abc, use the following command;

```
ip ospf authentication-key password 123abc
```

Use the following command to delete the authentication key;

```
no ip ospf authentication-key
```
**ip ospf authentication-type**

Configures the OSPF authentication method to be used with OSPF neighbors over the logical interface.

**Product**
- PDSN
- HA
- GGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Ethernet Interface Configuration

```bash
configure > context context_name > interface interface_name broadcast
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-eth)#
```

**Syntax**

```bash
ip ospf authentication-type { message-digest | null | text }
no ip ospf authentication-type { message-digest | null | text }
```

**Usage**

Disables this function.

- `message-digest`
  Uses the message digest (MD) authentication method.

- `null`
  Uses no authentication, thus disabling either MD or clear text methods.

- `text`
  Uses the clear text authentication method.

**Example**

Use this command to set the type of authentication to use when authenticating with neighboring routers.

To set the authentication type to use clear text, enter the following command;

```bash
ip ospf authentication-type text
```
**ip ospf bfd**

Enables or disables OSPF Bidirectional Forwarding Detection (BFD) on this interface.

**Product**

PDSN
HA
GGSN

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > Ethernet Interface Configuration

```bash
configure > context context_name > interface interface_name broadcast
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-eth)#
```

**Syntax**

```
ip ospf bfd [ disable ]
```

```bash
no ip ospf cost
```

- **no**
  - Disable this function.

- **disable**
  - Disables OSPF BFD on this interface.

**Usage**

Enable or disable OSPF Bidirectional Forwarding Detection (BFD) on this interface.

**Example**

Use the following command to enable OSPF BFD;

```bash
ip ospf bfd
```
### ip ospf cost

Configures the cost associated with sending a packet over the OSPF logical interface.

**Product**
- PDSN
- HA
- GGSN

**Privilege**
- Security Administrator, Administrator

**Mode**
```
Exec > Global Configuration > Context Configuration > Ethernet Interface Configuration
```
```
configure > context context_name > interface interface_name broadcast
```

Entering the above command sequence results in the following prompt:
```
[context_name]host_name(config-if-eth)#
```

**Syntax**
```
ip ospf cost value

no ip ospf cost
```

<table>
<thead>
<tr>
<th>no</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable this function.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the cost to assign to OSPF packets as an integer from 1 through 65535. Default: 10</td>
</tr>
</tbody>
</table>

**Usage**

Use this command to set the cost associated with routes from the interface.

**Example**

Use the following command to set the cost to 20;
```
ip ospf cost 20
```

Use the following command to disable the cost setting;
```
no ip ospf cost
```
ip ospf dead-interval

Configures the interval that the router should wait, during which time no packets are received and after which the router considers a neighboring router to be off-line.

Product
PDSN
HA
GGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Ethernet Interface Configuration

configure > context context_name > interface interface_name broadcast

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-if-eth)#

Syntax

[ no ] ip ospf dead-interval seconds

no

Returns the value to its default of 40 seconds.

seconds

Specifies the interval (in seconds) as an integer from 1 through 65535. This number is typical four times the hello-interval. Default: 40

Usage
Use this command to set the dead intervals for OSPF communications.

Example
To set the dead-interval to 100, use the following command;

   ip ospf dead-interval 100
ip ospf hello-interval

Configures the interval (in seconds) between sending OSPF hello packets.

**Product**
- PDSN
- HA
- GGSN

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration > Context Configuration > Ethernet Interface Configuration

```
configure > context context_name > interface interface_name broadcast
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-eth)#
```

**Syntax**

```
ip ospf hello-interval seconds

no ip ospf hello-interval
```

- **no**
  - Returns the value to its default of 10 seconds.

- **seconds**
  - Specifies the number of seconds between sending hello packets as an integer from 1 through 65535. Default: 10

**Usage**

Specify the interval (in seconds) between sending OSPF hello packets.

**Example**

To set the hello-interval to 25, use the following command;

```
ip ospf hello-interval 25
```
ip ospf message-digest-key

Enables or disables the use of MD5-based OSPF authentication.

**Product**
- PDSN
- HA
- GGSN

**Privilege**
- Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Ethernet Interface Configuration

```plaintext
configure > context context_name > interface interface_name broadcast
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-eth)#
```

**Syntax**

```plaintext
ip ospf message-digest-key key_id md5 [ encrypted ] password authentication_key
```

no ip ospf message-digest-key key_id

- **no**
  - Deletes the key.

- **message-digest-key key_id**
  - Specifies the key identifier number as an integer from 1 through 255.

- **encrypted**
  - Use this if you are pasting a previously encrypted authentication key into the CLI command.

- **password authentication_key**
  - Specifies the password to use for authentication as an alphanumeric string of 1 through 16 characters entered in clear text format.

**Usage**

Use this command to create an authentication key that uses MD5-based OSPF authentication.

**Example**

To create a key with the ID of 25 and a password of 123abc, use the following command:

```plaintext
ip ospf message-digest-key 25 md5 password 123abc
```

To delete the same key, enter the following command:

```plaintext
no ip ospf message-digest-key 25
```
ip ospf network

Configures the Open Shortest path First (OSPF) network type.

**Product**
- PDSN
- HA
- GGSN

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration > Context Configuration > Ethernet Interface Configuration
- `configure > context context_name > interface interface_name broadcast`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-eth)#
```

**Syntax**

```
ip ospf network { broadcast | non-broadcast | point-to-multipoint | point-to-point }
no ip ospf network
```

**Usage**

Use this command to specify the OSPF network type.

**Example**

To set the OSPF network type to `broadcast`, enter the following command;

```
    ip ospf network broadcast
```
To disable the OSPF network type, enter the following command:

```
no ip ospf network
```
ip ospf priority

Designates the OSPF router priority.

**Product**
- PDSN
- HA
- GGSN

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration > Context Configuration > Ethernet Interface Configuration
- `configure > context context_name > interface interface_name broadcast`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-eth)#
```

**Syntax**

- `ip ospf priority value`
- `no ip ospf priority value`

  - **no**
    - Disable this function.
  
  - **value**
    - Sets the priority value as an integer from 0 through 255.

**Usage**

Use this command to set the OSPF router priority.

**Example**

To set the priority to 25, enter the following command:

```
 ip ospf priority 25
```

To disable the priority, enter the following command:

```
 no ip ospf priority
```
# ip ospf retransmit-interval

Configures the interval in (seconds) between LSA (Link State Advertisement) retransmissions.

**Product**
- PDSN
- HA
- GGSN

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration > Context Configuration > Ethernet Interface Configuration
- `configure > context context_name > interface interface_name broadcast`

Entering the above command sequence results in the following prompt:
```
[context_name]host_name(config-if-eth)#
```

**Syntax**

```
ip ospf retransmit-interval seconds

no ip ospf retransmit-interval
```

**Usage**
Configure the interval in (seconds) between LSA (Link State Advertisement) retransmissions.

**Example**

To set the retransmit-interval to 10, use the following command:

```
ip ospf retransmit-interval 10
```
**ip ospf transmit-delay**

Configures the interval (in seconds) that the router should wait before transmitting an OSPF packet.

**Product**
- PDSN
- HA
- GGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Ethernet Interface Configuration

```
configure > context context_name > interface interface_name broadcast
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-eth)#
```

**Syntax**

```
ip ospf transmit-delay seconds
no ip ospf transmit-delay
```

- **no**
  Returns the value to its default of 1 second.

- **seconds**
  Specifies the number of seconds that the router should wait before transmitting a packet as an integer from 1 through 65535. Default: 1

**Usage**

Configure the interval (in seconds) that the router should wait before transmitting an OSPF packet.

**Example**

To set the transmit-delay to 5, use the following command;

```
ip ospf transmit-delay 5
```
**ipv6 access-group**

Specifies the name of the access control list (ACL) group to assign to this interface. You can filter for either inbound or outbound traffic.

**Product**

PDSN

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > Ethernet Interface Configuration

`configure > context context_name > interface interface_name broadcast`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-eth)#
```

**Syntax**

```
[ no ] ipv6 access-group group name { in | out } { priority-value priority_value }
```

- **no**
  
  Removes a previously configured access group association.

- **group_name**
  
  Specifies the name of the access group as an alphanumeric string of 1 to 79 characters.

- **in**
  
  Applies the filter to the inbound traffic.

- **out**
  
  Applies the filter to the outbound traffic.

- **priority-value**
  
  Specifies the priority of the access group as an integer from 0 to 4294967295. 0 is the highest priority. If priority-value is not specified, the priority is set to 0. If access groups in the list have the same priority, the last one entered is used first.

**Usage**

Use this command to specify the ACL group to assign the interface to. Specify an ACL group name with this command.

**Important:** Up to eight ACLs can be applied to a group provided that the number of rules configured within the ACL(s) does not exceed the 128-rule limit for the interface.
Example

Use the following command to associate the `group_1` access group with the current IPv6 profile for inbound access:

```
ipv6 access-group group_1 in 1
```
**ipv6 address**

Specifies an IPv6 address and subnet mask.

**Product**
PDSN
HA

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Ethernet Interface Configuration

```
configure > context context_name > interface interface_name broadcast
```

Entering the above command sequence results in the following prompt:

```
/context_name]host_name(config-if-eth)#
```

**Syntax**

```
ipv6 address ip_address/mask
```

**ip_address/mask**

Specifies an individual host IP address to add to this host pool in IPv6 CIDR colon-separated-hexadecimal notation.

---

**Important:** On the ASR 5000, routes with IPv6 prefix lengths less than /12 and between the range of /64 and /128 are not supported.

---

**Usage**

Configures the IPv6 address and subnet mask for a specific interface.
ipv6 ospf

Enables Open Shortest Path First Version 3 (OSPFv3) functionality on this IPv6 a interface.

Product
- PDSN
- HA
- GGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Ethernet Interface Configuration

Syntax

[ no ] ipv6 ospf [ area { integer | ipv4-address } | cost cost-value | dead-interval dead-intrv | hello-interval hello-intrvl | priority p-value | retransmit-interval retx-interval | transmit-delay td-interval ]

no
Removes a previously configured access group association.

area { integer | ipv4-address }
Specifies an OSPFV3 area.
decimal_value: Specifies the identification number of the area as an integer from 0 through 4294967295.
ipv4address: Specifies the IP address of the area in IPv4 dotted-decimal notation.

cost cost-value
Specifies a link cost as an integer from 1 through 65535. The link cost is carried in the LSA updates for each link. The cost is an arbitrary number.

dead-interval dead-intrv
Specifies the interval (in seconds) after which a neighbor is declared dead when no hello packets as an integer from 1 through 65535.

hello-interval hello-intrvl
Specifies the interval (in seconds) between hello packets that OSPFV3 sends on an interface as an integer from 1 through 65535.

priority p-value
Specifies the of the interface as an integer from 0 through 255.
retransmit-interval  retx-interval
Specifies the time (in seconds) between link-state advertisement (LSA) retransmissions for adjacencies belonging to the OSPFv3 interface as an integer from 1 through 65535.

transmit-delay  td-interval
Specifies the estimated time (in seconds) required to send a link-state update packet on the interface as an integer from 1 through 65535.

Usage
Configure an OSPFv3 interface in this context.

Example
ipv6 ospf area 334 cost 555 dead-interval 40 hello-interval 10 priority 10 retransmit-interval 5 transmit-delay 10
**ipv6 router advertisement**

Enables or disables the system to send IPv6 router advertisements.

**Product**
- PDSN
- HA

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration > Context Configuration > Ethernet Interface Configuration
  - `configure > context context_name > interface interface_name broadcast`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-eth)#!
```

**Syntax**

```
[ no ] ipv6 router advertisement
```

**Usage**

Enables sending of router advertisements on the interface. All of the pool prefixes in the context (belonging to the interface) will be advertised in the router advertisement. The router-lifetime in the advertisement is sent as 0 to indicate to the receiver that the sender cannot be a default-router. For all the prefixes (pools), the valid and preferred lifetime are sent as default. The router-advertisement is sent every 600 seconds. If the pool-prefix is deleted, then an router-advertisement is sent for that particular prefix with the valid and preferred time set to 0.
**logical-port-statistics**

Enables or disables the collection of logical port (VLAN and NPU) bulk statistics for the first 32 configured Ethernet or PVC interface types.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Ethernet Interface Configuration

```
configure > context context_name > interface interface_name broadcast
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-eth)#
```

**Syntax**

```
[ no ] logical-port-statistics
```

```
no
```

Stops the collection of logical port statistics on this interface.

**Usage**

Starts or stops the collection of logical port bulkstats. Default: This feature is not enabled.

**Example**

To start collection of logical port statistics on this interface, enter the following command:

```
logical-port-statistics
```
**mpls ip**

Enables or disables dynamic Multiprotocol Label Switching (MPLS) distribution and forwarding of IP packets on this interface.

**Product**
- GGSN
- HA
- P-GW
- SAEGW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Ethernet Interface Configuration

configure > context context_name > interface interface_name broadcast

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-eth)#
```

**Syntax**

```
[ no ] mpls ip
```

- **no**
  Stops dynamic label distribution and forwarding on this interface.

**Usage**

Starts label distribution and forwarding over an interface for a context that has MPLS enabled. For additional information, refer to the *Context Configuration Mode Commands* chapter. Default: This feature is not enabled.

**Example**

To start dynamic MPLS distribution and forwarding on this interface, enter the following command:

```
mpls ip
```
policy-forward

This command supports downlink IPv4 data packets received from the SGi that are forwarded/redirected to a configured next-hop address if the subscriber session does not exist in the P-GW.

**Product**
PDSN
P-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Ethernet Interface Configuration

```
configure > context context_name > interface interface_name broadcast
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-eth)#
```

**Syntax**

```
policy-forward { icmp unreachable next-hop ip address | unconnected-address next-system ip_address }
```

```
no policy-forward unconnected-address
```

- `no` Deletes the policy forwarding configuration for unconnected address for the current interface.

```
icmp unreachable next-hop ip address
```

Specifies routing of Internet Control Message Protocol (ICMP) unreachable is required in overlapping pool configuration. `ip_address` must be expressed in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

```
unconnected-address next-system ip address
```

Specifies the IP address of the next system P-GW to handle processing during P-GW upgrade. `ip_address` must be an IP address expressed in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

**Important:** The `unconnected-address next-system ip address` keyword enables IPv4 downlink data packet forwarding/redirection.

**Usage**

Use this command to set the redirecting policy for IP packets from an existing P-GW to a new P-GW during upgrade. To configure this command both keywords will be in separate interface.

**Important:** This is a customer specific command.
Example

To configure existing P-GW system for redirecting the P-GW packets to new P-GW during existing P-GW upgrade enter the following commands:

```
policy-forward unconnected-address next-system ip_address

policy-forward icmp unreachable next-hop ip_address
```
pool-share-protocol

Configures the primary or secondary system for the IP pool sharing protocol and enter IPSP configuration mode.

**Product**

PDSN

HA

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > Ethernet Interface Configuration

`configure > context context_name > interface interface_name broadcast`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-eth)#
```

**Syntax**

```
pool-share-protocol { primary ip_address | secondary ip_address } [ mode { active | inactive | check-config } ]
```

no pool-share-protocol

no

Deletes the IP pool sharing protocol information from the current interface.

**primary address**

On the secondary system, defines the IP address of an interface on the primary system that has identical IP pools configured for use with the IP pool sharing protocol. `ip_address` must be expressed in IP v4 dotted-decimal notation.

**secondary ip_address**

On the primary system, define the IP address of an interface on the secondary system that has identical IP pools configured for use with the IP pool sharing protocol. `ip_address` must be expressed in IP v4 dotted-decimal notation.

**mode {active | inactive | check-config}**

This is an optional command to manage the mode for IP pool sharing protocol for primary or secondary HA.

**active**: Activates the IP pool sharing protocol mode.

**inactive**: Inactivates the IP pool sharing protocol mode.

**check-config**: Verifies the IP pool sharing protocol configuration.

**Usage**

Use this command to set the IP address of the primary or secondary system for use with the IP pool sharing protocol and enter ipsp configuration mode. This command must be configured for an interface in each
context that has IP pools configured. Refer to the System Administration and Configuration Guide for information on configuring and using the IP pool sharing protocol.

**Important:** Both the primary and secondary systems must be in the same subnet.

**Important:** For information on configuring and using IP Pool Sharing Protocol (IPSP), refer to the *Packet Data Serving Node Administration Guide*.

**Important:** Reserve free addresses on the primary HA for this command via the `reserved-free-percentage` command as described in the *IPSP Configuration Mode Commands* chapter of this guide.

### Example

To configure a secondary system with an IP address of 192.168.100.10 for use with the IP pool sharing protocol, enter the following command:

```
pool-share-protocol secondary 192.168.100.10
```

To inactivate a secondary system with an IP address of 192.168.100.10 for use with the IP pool sharing protocol, enter the following command:

```
pool-share-protocol secondary 192.168.100.10 mode inactive
```
port-switch-on-L3-fail

Causes the ASR 5000 line card port or the ASR 5500 MIO port to which the current interface is bound to switch over to the port on the redundant line card or MIO when connectivity to the specified IP address is lost.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Ethernet Interface Configuration
configure > context context_name > interface interface_name broadcast

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-if-eth)#

Syntax

port-switch-on-L3-fail address { ip_address | ipv6_address } [ minimum-switchover-period switch_time ] [ interval int_time ] [ timeout time_out ] [ num-retry number ]

no port-switch-on-L3-fail

no

Disable port switchover on failure.

ip_address

The IP address to monitor for connectivity, entered in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

minimum-switchover-period switch_time

After a switchover occurs, another switchover cannot occur until the specified amount of time (in seconds) has elapsed. switch_time must be an integer from 1 through 3600. Default: 120

interval int_time

Specifies how often (in seconds) monitoring packets are sent to the IP address being monitored. int_time must be an integer from 1 through 3600. Default: 60

timeout time_out

Specifies how long to wait (in seconds) without a reply before resending monitoring packets to the IP address being monitored. time_out must be an integer from 1 through 10. Default: 3

num-retry number

Specifies how many times to retry sending monitor packets to the IP address being monitored before performing the switchover. number must be an integer from 1 through 100. Default: 5
Usage

Use this command to monitor a destination in your network to test for L3 connectivity. The destination being monitored should be reachable from both the active and standby line cards.

Example

The following command enables port switchover on connectivity failure to the IP address 192.168.10.100 using default values:

```
port-switch-on-L3-fail address 192.168.10.100
```

The following command disables port switchover on connectivity failure:

```
no port-switch-on-L3-fail
```
**vlan-map**

Sets a single next-hop IP address so that multiple VLANs can use a single next-hop gateway. The vlan-map is associated with a specific interface.

**Product**
- PDSN
- HA
- SGSN

**Privilege**
- Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Ethernet Interface Configuration
configure > context context_name > interface interface_name broadcast

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-eth)#
```

**Syntax**

```
vlan-map next-hop ip_address
```

```
next-hop ip_address
```

Specifies the IP address for the next-hop gateway in IPv4 dotted-decimal notation.

**Usage**

Use this command to combine multiple VLAN links to go through a single IP address. This feature is used in conjunction with nexthop forwarding and overlapping IP pools.

After configuring the vlan-map, move to the Ethernet Port Configuration mode to attach the vlan-map to a specific VLAN.

**Example**

The following command sets an IPv4 address for a next-hop gateway.

```
vlan-map next-hop 123.123.123.1
```
Chapter 123
Ethernet Port Configuration Mode Commands

The Ethernet Port Configuration Mode is used to create and manage Ethernet ports and their bindings between contexts.

Mode

Exec > Global Configuration > Ethernet Port Configuration

```
configure > port ethernet slot_number/port_number
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-port-slot_number/port_number)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
**bind interface**

Configures an association (binds) between a virtual IP interface, an SS7 or Frame Relay link to a specific context.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Ethernet Port Configuration
configure > port ethernet slot_number/port_number

Entering the above command sequence results in the following prompt:

[local]host_name(config-port-slot_number/port_number)#

**Syntax**

```
[ no ] bind interface interface_name context_name
```

- **no**
  Indicates the virtual interface specified is to be unbound from the context.

- **interface_name**
  Specifies the name of the virtual interface to be bound to the context as an alphanumeric string of 1 through 79 characters.

- **context_name**
  Specifies the name of the context to be bound to the virtual port. context_name must refer to a previously configured context.

**Usage**

Bind an interface to a context to allow the context to provide service.

**Example**

```
bind interface sampleVirtual sampleContext

no bind interface sampleVirtual sampleContext
```
boxertap

Binds a physical port to a named interface for debugging purposes.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Ethernet Port Configuration
configure > port ethernet slot_number/port_number

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-port-slot_number/port_number)#
```

**Syntax**

```
[ no ] boxertap interface_name
```

- `no`
  Unbinds the physical port to the interface.

- `interface_name`
  Specifies the name of the virtual interface to be bound to the physical port as an alphanumeric string of 1 through 79 characters.

**Usage**

Bind a physical port to a named interface for debugging purposes.

**Example**

```
boxertap ggsn01

no boxertap ggsn01
```
default

Restores the speed and communication mode of the default interface for the specified context.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Ethernet Port Configuration

configure > port ethernet slot_number/port_number

Entering the above command sequence results in the following prompt:

[local]host_name(config-port-slot_number/port_number)#

Syntax

default { flow-control | link-aggregation { lacp | redundancy } | medium | preferred slot | threshold { high-activity | monitoring | rx-utilization | tx-utilization } }

---

flow-control

ASR 5000: Restores the default behavior to advertise symmetric flow control.
ASR 5500: Restores the MIO card default to no flow control.

link-aggregation { lacp | redundancy }

Restores the default values for link-aggregation as follows:
- *lacp*: Active – sends out LACP packets periodically.
- *redundancy*: Standard – treats all cards in the group as one group.

medium

ASR 5000: Restores the default values for the medium options as follows:
- SPIO and fast ethernet line cards: auto
- Gigabit ethernet line card: auto
ASR 5500: Restores the MIO card default medium value to auto.

preferred slot

Sets the port for non-revertive operation for port redundancy auto-recovery; requiring an administrative user to manually issue a port switch to command to return service to the original port.

threshold { high-activity | monitoring | rx-utilization | tx-utilization }

Restores the specified port-level threshold parameters to its default value(s). The possible values are:
- *high-activity*: High port activity threshold settings. Default: 50 percent
- *monitoring*: Threshold monitoring configuration settings. Default: Disabled
- *tx-utilization*: Transmit port utilization threshold settings. Default: 80 percent
Usage

Restores port-level parameters to their default values.

Example

```
default medium
```
description

Sets the port descriptive text.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Ethernet Port Configuration

configure > port ethernet slot_number/port_number

Entering the above command sequence results in the following prompt:

[local]host_name(config-port-slot_number/port_number)#

Syntax

description text

no description

no

Clears the description for the port.

text

Specifies the descriptive text as an alphanumeric string of 1 to 79 characters. If you include spaces between words in the description, you must enclose the text with double quotation marks (" "),

Usage

The description should provide useful information on the port’s primary function, services, end users, etc.

Example

description samplePortDescriptiveText
description “This is a sample description”
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Use this command to return to the parent configuration mode.
fault-unidirect-mode

Configures the unidirectional mode that generates fault messages for the connection's peer when local faults are detected and remote faults are received.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Ethernet Port Configuration

```
configure > port ethernet slot_number/port_number
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-port-slot_number/port_number)#
```

**Syntax**

```
[ no ] fault-unidirect-mode ( clause-46 | clause-66 )
```

- `no fault-unidirect-mode`
  Disables fault message generation.

- `{ clause-46 | clause-66 }

  **clause-46:** On local fault reception, continuous remote faults are sent. On remote fault reception, continuous idles are sent. [IEEE 802.3, Clause 46, Reconciliation Sublayer (RS) and 10 Gigabit Media Independent Interface (XGMII)]

  **clause-66:** On local fault reception, frame transmit is continued, remote fault indication is sent during Inter-Frame Gap (IFG). On remote fault reception, frame transmit is continued. [IEEE 802.3, Clause 66, Extensions of the 10 Gb/s Reconciliation Sublayer (RS), 100BASE-X PHY, and 1000BASE-X PHY for unidirectional transport]

**Usage**

Configure the unidirectional mode that generates fault messages for the connection's peer when local faults are detected and remote faults are received.

**Example**

After flow control has been disabled, use the following command to enable flow control:

```
fault-unidirect-mode clause-46
```
flow-control

Enables and disables flow control on the ASR 5000 Quad Gig-E line card (QGLC) and the ASR 5500 MIO card.

**Product**
- PDSN
- SGSN
- GGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Ethernet Port Configuration

```
configure > port ethernet slot_number/port_number
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-port-slot_number/port_number)#
```

**Syntax**

```
[ no ] flow-control

no
```

Disables flow control on the specified port.

**Usage**
Flow control is enabled by default on the QGLC and can be disabled using the `no` command on a per-port basis. This command does not work on the Fast Ethernet Line Card (FELC), Gigabit Ethernet Line Card (GELC/GLC2) or 10 GigE Line Card (XGLC) which do not support flow control.

Flow control is not supported on the MIO card.

**Example**

After flow control has been disabled, use the following command to enable flow control:

```
flow-control
```
ingress-mode

Labels this port as an ingress port (incoming traffic).

Product
IPSG

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Ethernet Port Configuration

configure > port ethernet slot_number/port_number

Entering the above command sequence results in the following prompt:

[local]host_name(config-port-slot_number/port_number)#

Syntax

[ no ] ingress-mode

no

Disables ingress port tag.

Usage

Use this command to label this port in order for the session manager to recognize the interface from which IP data packets are being received. This command should be used in single context configurations. In single context configurations, the ingress port can only be identified if labeled.
link-aggregation

Aggregates ports on an ASR 5000 Quad Gig-E line card (QGLC), or 10 Gig-E line cards (XGLCs), or an ASR 5500 Management Input/Output (MIO) card and sets related parameters in accordance with IEEE 802.3ad.

Product
- WiMAX
- PDSN
- HA
- FA
- GGSN
- SGSN

Privilege
- Security Administrator, Administrator

Mode
- Exec > Global Configuration > Ethernet Port Configuration
- configure > port ethernet slot_number/port_number

Entering the above command sequence results in the following prompt:

[local]host_name(config-port-slot_number/port_number)#

Syntax

link-aggregation { distribution { block | random | rotate | simple } | lacp { active | passive } [ rate { auto | fast | slow } ] [ timeout { long | short } ] | master { global group group_number | group group_number | local group group_number } | member { global group group_number | group group_number | local group group_number } | redundancy { standard | switched } [ hold-time sec ] [ preferred slot { card_number | none } ] | toggle-link }

no link-aggregation [ toggle-link ]

default link-aggregation { distribution | lacp | redundancy | toggle-link }

distribution { block | random | rotate | simple }

**Important:** The distribution keyword is not supported on the ASR 5500.

Configures link aggregation distribution and controls how a Link Aggregation Group (LAG) hash map is generated. This method is required for Equal Cost Multi-Path (ECMP) routing over LAG. Set this option on the master port for use with the whole group. The following list defines the distribution options (assuming port index 0,1,2,3 were selected.

- **block:** Blocks of the same port index (Example: 0000111122223333)
- **random:** Based on pseudo random number
- **rotate:** Repetition of rotated port index (Example: 0123123023013012…)
- **simple:** Repetition of all selected port indexes (Example: 0123012301230123…)
lACP { active | passive }

Configures the Link Aggregation Control Protocol (LACP). Set this option on the master port for use with the whole group.
active mode sends out LACP packets periodically. (Default)
passive mode only responds to LACP packets received.

rate { auto | fast | slow }

Configures the rate at which the LACP sends packets.
auto: rate is controlled by the peer
fast: 1 seconds
slow: 30 seconds (Default) [ASR 5000 only]

timeout { long | short }

Configures LACP timeout events. Set this option on the master port for use with the whole group.
long: Set LACP to long timeout
short: Set LACP to short timeout

master { global group group_number | group group_number | local group group_number }

This command creates the Master port for the aggregated group.
global: Set group global across slots.
group group_number: Set link aggregation group number. group_number must be an integer between 1 and 1023.
local: Set group local within same slot.

member { global group group_number | group group_number | local group group_number }

This command makes the port a member of the aggregated group.
global: Set group global across slots.
group group_number: Set link aggregation group number. group_number must be an integer from 1 through 1023.
local: Set group local within same slot.

redundancy { standard | switched } [ hold-time sec ] [ preferred slot { card_number | none } ]

Connects top and bottom QGLCs, side-by-side XGLCs, or MIO cards, to different Ethernet switches. The master port must be set to make this effective for the group.
standard: Treats all cards in the group as one group. (Default)
switched: Assumes cards are connected to different switches. [ASR 5000 only]
hold-time sec: Sets the amount of time to hold (in seconds) before switching between cards. Applies to standard and switched modes. sec must be an integer from 0 through 3600. Default: 10
preferred slot { card_number | none }: Specifies the preferred behavior for a LAG using two Ethernet switches. Applies to standard and switched modes. card_number is an integer between 1 and 48 on an ASR 5000, or 5 or 6 on an ASR 5500.

When a card number is specified, system behavior varies based on the card type.

*QGLC (ASR 5000) – the preferred slot is selected only when both the top and bottom slots have the same number of active LACP ports.
**XGLC** (ASR 5000) – the preferred slot is selected for the initial timeout period to make the selection of an Ethernet switch less random.

**MIO** (ASR 5500) – the preferred slot is selected for the initial timeout period to make the selection of an Ethernet switch less random.

**none**: Specifies no preferred slot.

---

**toggle-link**

---

**Important**: The **toggle-link** keyword is **not** supported on the ASR 5500.

Set to toggle link on port switch.

---

**default**

Restores the default values.

---

**no**

This command deletes the Ethernet port from any group it might be in. If the port was the Master of a group, the whole group would be deleted.

---

**Usage**

Configure from one to four ports on a QGLC (vertical aggregation) or the single port on XGLCs (horizontal aggregation), or traffic ports on an MIO card to be in an aggregation group that links to an aggregation group on a remote Ethernet switch. Very large files can be downloaded across all ports in a group, which makes for a faster download when compared to serial downloads over a single link.

Related **link-aggregation** commands are described in the *Card Configuration Mode Commands* and *Global Configuration Mode Commands* chapters of this guide. For additional information, also refer to the *System Administration Guide*.

---

**Example**

The following example configures the port to be the Master for Group 2:

```
link aggregation master group 2
```
media

Configures the port interface type. (ASR 5000 only)

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Ethernet Port Configuration

configure > port ethernet slot_number/port_number

Entering the above command sequence results in the following prompt:

[local]host_name(config-port-slot_number/port_number)#

Syntax

media { rj45 | sfp }

{ rj45 | sfp }

rj45: Sets the physical interface to copper RJ-45 connectors.
sfp: Sets the physical interface connection to optical Small Form Factor (SFP) gigabit via an SFP transceiver.

Usage
Set the media option when the physical cabling interface is changed.

Example
The following commands are entered one-at-a-time to set the physical interface to RJ-45 and SFP:

  media rj45

  media sfp
medium

Configures the port speed and communication mode. (ASR 5000 only)

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Ethernet Port Configuration

configure > port ethernet slot_number/port_number

Entering the above command sequence results in the following prompt:

[local]host_name(config-port-slot_number/port_number)#

Syntax

medium { auto | speed { 10 | 100 | 1000 | 10000 } duplex { full | half } }

| { auto | speed { 10 | 100 | 1000 | 10000 } duplex { full | half } } |
|---------------------------------------------------------------|
| Default: auto                                                |
| Optionally sets the speed of the interface and the communication mode. |
| auto: configures the interface to auto negotiate the interface speed. |
| speed { 10 | 100 | 1000 | 10000 }: specifies the speed to use at all times. |
| duplex { full | half }: sets the communication mode of the interface to either full or half duplex. |

Important: Ethernet networking rules dictate that if a device whose interface is configured to auto-negotiate is communicating with a device that is manually configured to support full duplex, the first device will negotiate to the manually configured speed of the second device but will only communicate in half duplex mode.

Usage
Set the medium options when the physical interface changes.

Important: The speed keyword for the medium command is not supported on the ASR 5500.

Example
The following configures the port’s speed and communication mode to be auto negotiated.

medium auto

The following command configures the port’s interface speed to gigabit with full duplex communication.

medium speed 1000 duplex full
preferred slot

Assigns revertive or non-revertive control to port redundancy auto-recovery. (ASR 5x00 only)

Default: non-revertive operation

Product

PDSN
FA
HA
SGSN
GGSN

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > Ethernet Port Configuration

configure > port ethernet slot_number/port_number

Entering the above command sequence results in the following prompt:

[local]host_name(config-port-slot_number/port_number)#

Syntax

[ no ] preferred slot slot#

no

Disables revertive or auto-recovery operation for the selected port.

preferred slot slot#

Identifies the physical chassis slot where the ASR 5000 line card or SPIO card, or the ASR 5500 MIO card is installed.

Usage

This command enables or disables revertive port redundancy, wherein after a port failover, when the original port is restored to service (such as link up) the system will return service to that port automatically.

Disabled, which is the default setting, causes non-revertive operation; requiring an administrative user to manually issue an Exec mode `link-aggregation port switch to` command to return service to the original port.

This command must be issued on a per port basis, allowing you to configure specific ports to be used on individual line card, SPIO, or an MIO card.

Important: This command is not supported on all platforms.

Example

For ASR 5000:
preferred slot 17

For ASR 5500:

preferred slot 5
**shutdown**

Terminates all processes supporting the port or blocks the shutting down of the port. Conversely, the port is enabled with the use of the `no` keyword.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Ethernet Port Configuration

```
configure > port ethernet slot_number/port_number
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-port-slot_number/port_number)#
```

**Syntax**

```
[ no ] shutdown
```

```
no
```

Enables the port and places it in service.

**Usage**

Shut down a port prior to re-cabling and/or other maintenance activities. For Release 15.0 and higher, this command powers down the port on FELC, GELC and QGLC line cards (ASR 5000). This command already powers down the ports on MIO/UMIO cards (ASR 5500).

To enable a port (bring it into service) use the `no` keyword.

**Example**

Use the following command to disable the port:

```
shutdown
```

Use the following command to enable the port for service:

```
no shutdown
```
**snmp trap link-status**

Enables or disables the generation of an SNMP trap for link status changes.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Ethernet Port Configuration

```configure > port ethernet slot_number/port_number```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-port-slot_number/port_number)#
```

**Syntax**

```
[ no ] snmp trap link-status
```

- **no**
  - Disables the sending of traps for link status changes.

**Usage**
Enable link status change traps when a monitoring facility can use the information or if there are troubleshooting activities in progress.

**Example**
Use the following command to disable sending of traps:

```
no snmp trap link-status
```
**srp virtual-mac-address**

Configures the Standby Router Protocol (SRP) virtual MAC address for the port.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Ethernet Port Configuration

```
configure > port ethernet slot_number/port_number
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-port-slot_number/port_number)#
```

**Syntax**

```
srp virtual-mac-address MAC_Address
```

```
no srp virtual-mac-address
```

- **no**
  Disables the SRP virtual MAC addressing for Ethernet ports. The block of virtual MAC addresses is not saved.

- **MAC_Address**
  Enables SRP virtual addressing for the specified MAC address.

**Usage**

The SRP virtual MAC address is applied to the port when the chassis is in SRP ACTIVE state. The default is `no srp virtual-mac-address`.

**Important:** This command is not supported on all platforms.

**Example**

Use the following command to enable the SRP’s virtual MAC addressing:

```
srp virtual-mac-address MAC_Address
```
**threshold high-activity**

Configures thresholds for high port activity for the port.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Ethernet Port Configuration
`configure > port ethernet slot_number/port_number`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-port-slot_number/port_number)#
```

**Syntax**

```
threshold high-activity high_thres [ clear low_thres ]
```

- **high_thres**
  Specifies the high threshold high port activity percentage that must be met or exceeded within the polling interval to generate an alert or alarm. The percentage is expressed as an integer from 0 through 100. Default: 50

- **clear**
  Allows the configuration of the low threshold.

- **low_thres**
  Specifies the low threshold high port activity percentage that maintains a previously generated alarm condition. If the activity percentage falls below the low threshold within the polling interval, a clear alarm will be generated. The percentage is expressed as an integer from 0 through 100. Default: 50

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**

High port activity thresholds generate alerts or alarms based on the utilization percentage of each configured port during the specified polling interval. This threshold is configured on a per-port basis. Alerts or alarms are triggered for high port activity based on the following rules:

- **Enter condition**: Actual percent utilization of a port is greater than High Threshold.
- **Clear condition**: Actual percent utilization of a port is less than Low Threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the `threshold poll` command in the *Global Configuration Mode Commands* chapter to configure the polling interval and the `threshold monitoring` command in this chapter to enable thresholding for this value.

**Example**

The following command configures a high port utilization threshold percent of 70 and a low threshold percent of 50 for a system using the Alarm thresholding model:

```
threshold high-activity 70 clear 50
```
threshold monitoring

Enables or disables thresholding for port-level values.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Ethernet Port Configuration
configure > port ethernet slot_number/port_number

Entering the above command sequence results in the following prompt:

[local] host_name(config-port-slot_number/port_number)#

Syntax

[ no ] threshold monitoring

no

Disables threshold monitoring for port-level values. This is the default setting.

Usage

Thresholding on the system is used to monitor the system for conditions that could potentially cause errors or outage. Typically, these conditions are temporary (such as high-activity) and are quickly resolved. However, continuous or large numbers of these error conditions within a specific time interval may be indicative of larger, more severe issues. Thresholding helps identify potentially severe conditions so that immediate action can be taken to minimize and/or avoid system downtime.

Thresholding reports conditions using one of the following mechanisms:

• **SNMP traps**: SNMP traps have been created that indicate the condition (high threshold crossing and/or clear) of each of the monitored values. Complete descriptions and other information pertaining to these traps is located in the starentMIB(8164).starentTraps(2) section of the SNMP MIB Reference. The generation of specific SNMP traps can be enabled or disabled on the system allowing you to view only those traps that are most important to you.

• **Logs**: The system provides a facility called threshold for which active and event logs can be generated. As with other system facilities, logs are generated Log messages pertaining to the condition of a monitored value are generated with a severity level of WARNING.

• **Alarm System**: High threshold alarms generated within the specified polling interval are considered “outstanding” until a the condition no longer exists and/or a condition clear alarm is generated. “Outstanding” alarms are reported to through the system’s alarm subsystem and are viewable through the system’s CLI.

The following table indicates the reporting mechanisms supported by each of the above models.

Table 25. Thresholding Reporting Mechanisms by Model

<table>
<thead>
<tr>
<th>Model</th>
<th>SNMP Traps</th>
<th>Logs</th>
<th>Alarm System</th>
</tr>
</thead>
</table>

Cisco ASR 5x00 Command Line Interface Reference
This command enables thresholding for port-level values. Refer to the `threshold high-activity`, `threshold rx-utilization`, and `threshold tx-utilization` commands in this chapter for information on configuring these values. In addition, refer to the `threshold poll` command in the *Global Configuration Mode Commands* chapter for information on configuring the polling interval over which these values are monitored.
threshold rx-utilization

Configures thresholds for receive port utilization.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Ethernet Port Configuration

```
configure > port ethernet slot_number/port_number
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-port-slot_number/port_number)#
```

**Syntax**

```
threshold rx-utilization high_thresh [ clear low_thresh ]
```

- `high_thresh`
  Specifies the high threshold receive port utilization percentage that must be met or exceeded within the polling interval to generate an alert or alarm. The percentage is expressed as an integer from 0 through 100. Default: 80

- `clear`
  Allows the configuration of the low threshold.

- `low_thresh`
  Specifies the low threshold receive port utilization percentage that maintains a previously generated alarm condition. If the utilization percentage falls below the low threshold within the polling interval, a Clear Alarm will be generated. The percentage is expressed as an integer from 0 through 100. Default: 80

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**

Receive port utilization thresholds generate alerts or alarms based on the utilization percentage of each configured port in relation to data received during the specified polling interval. This threshold is configured on a per-port basis.

**Important:** Ports configured for half-duplex do not differentiate between data received and data transmitted. Therefore, to avoid redundant alarms, it is recommended that only the receive or transmit utilization threshold be configured.
Alerts or alarms are triggered for receive port utilization based on the following rules:

- **Enter condition**: Actual percent utilization of a port for received data is greater than High Threshold
- **Clear condition**: Actual percent utilization of a port for received data is less than Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the `threshold poll` command in the *Global Configuration Mode Commands* chapter to configure the polling interval and the `threshold monitoring` command in this chapter to enable thresholding for this value.

**Example**

The following command configures a receive port high utilization threshold percent of 70 and a low threshold percent of 50 for a system using the Alarm thresholding model:

```
threshold rx-utilization 70 clear 50```

threshold tx-utilization

Configures thresholds for transmit port utilization.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Ethernet Port Configuration
configure > port ethernet slot_number/port_number

Entering the above command sequence results in the following prompt:

[local]host_name(config-port-slot_number/port_number)#

Syntax

threshold tx-utilization  high_thresh [ clear low_thresh ]

high_thresh
The high threshold transmit port utilization percentage that must be met or exceeded within the polling interval to generate an alert or alarm. The percentage is expressed as an integer from 0 through 100. Default: 80

clear
Allows the configuration of the low threshold.

low_thresh
The low threshold transmit port utilization percentage that maintains a previously generated alarm condition. If the utilization percentage falls below the low threshold within the polling interval, a clear alarm will be generated. The percentage is expressed as an integer from 0 through 100. Default: 80

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage
Transmit port utilization thresholds generate alerts or alarms based on the utilization percentage of each configured port in relation to data transmitted during the specified polling interval. This threshold is configured on a per-port basis.

Important: Ports configured for half-duplex do not differentiate between data received and data transmitted. Therefore, to avoid redundant alarms, it is recommended that only the receive or transmit utilization threshold be configured.

Alerts or alarms are triggered for transmit port utilization based on the following rules:
- **Enter condition**: Actual percent utilization of a port for transmit data is greater than High Threshold
- **Clear condition**: Actual percent utilization of a port for transmit data is less than Low Threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the `threshold poll` command in the *Global Configuration Mode Commands* chapter to configure the polling interval and the `threshold monitoring` command in this chapter to enable thresholding for this value.

**Example**

The following command configures a transmit port high utilization threshold percent of `70` and a low threshold of `50` for a system using the Alarm thresholding model:

```
threshold tx-utilization 70 clear 50
```
vlan

Enters VLAN Configuration mode. Creates VLAN if necessary.

Product
HA
HSGW
PDSN
P-GW
SAEGW
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Ethernet Port Configuration
configure > port ethernet slot_number/port_number

Entering the above command sequence results in the following prompt:
[local]host_name(config-port-slot_number/port_number)#

Syntax

vlan_vlan_id [ inline-process | subscriber-vlan ] [ -noconfirm ]

<table>
<thead>
<tr>
<th>vlan_id</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies a VLAN identifier as an integer from 1 through 4094. If this identifier does not already exist you are prompted to confirm the identifier an a new one is created.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>inline-process</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies that this VLAN will be used for inline processing.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>subscriber-vlan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies that this VLAN will be used for subscriber-based processing.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>-noconfirm</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies that the command must execute without any prompts and confirmation from the user.</td>
</tr>
</tbody>
</table>

Usage
Use this command to specify an existing VLAN ID or create a new VLAN ID and enter the VLAN Configuration mode.
For additional information, refer to the VLAN Configuration Mode Commands chapter.

Example
The following command creates the VLAN ID 234.
Vlan 234

Are you sure? [Yes|No]: y
Chapter 124
Exec Mode Commands (A-C)

This section includes the commands `aaa test` through `crypto-group`.
The Exec Mode is the initial entry point into the command line interface system. Exec mode commands are useful in troubleshooting and basic system monitoring.

Mode

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
aaa test

Tests Authentication, Authorization and Accounting (AAA) functionality between this system and a remote server.

**Product**
- PDSN
- HA
- GGSN
- SGSN
- ASN-GW

**Privilege**
- Security Administrator, Administrator, Operator

**Mode**
- Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
aaa test { accounting username user_name | authenticate user_name password | session user_name password }
```

- **accounting username user_name**
  Tests RADIUS or GTPP accounting functionality for the specified user.
  *user_name* must be the name of a user configured on the RADIUS or CFG server.

**Important:** GTPP is used only in conjunction with the GGSN or SGSN product.

- **authenticate user_name password**
  Tests RADIUS authentication functionality for the specified user.
  *user_name* is the name of a user configured on the RADIUS server. *password* is the user's password.

- **session user_name password**
  Tests both RADIUS authentication and RADIUS or GTPP accounting functionality for the specified user.
  *user_name* is the name of a user configured on the RADIUS server. *password* is the user's password.

**Important:** GTPP is used only in conjunction with the GGSN or SGSN product.

**Usage**

This command is used to test RADIUS-based authentication and RADIUS or GTPP accounting. This command may be useful for diagnosing problems with subscribers and access to the system and/or billing data.
Example

The following command verifies accounting for a user named *user1*:

```
  aaa test accounting username user1
```

The following command tests authentication for a user named *user1* with the password *abc123*:

```
  aaa test authentication user1 abc123
```

The following command tests both accounting and authentication for the user named *user1* with the password *abc123*:

```
  aaa test session user1 abc123
```
**abort**

Stops software patch or upgrade process.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec
The following prompt is displayed in the Exec mode:

```
[local]host_name# 
```

**Syntax**

```
abort { patch | upgrade } [ -noconfirm ]
```

- **patch**
  Stops a running software patch process.

- **upgrade**
  Stops a running software upgrade process.

**Important:** The `abort upgrade` command can only be used during Stage 1 (busy-out) of an on-line software upgrade.

- **-noconfirm**
  Executes the command without any additional prompt and confirmation from the user.

**Usage**

Use this command to stop a running StarOS patch or upgrade process. For additional information on software patches and upgrades, refer to the *System Administration Guide*.

**Example**

The following command stops an in-progress StarOS upgrade:

```
abort upgrade
```
active-charging service

Creates an active charging service (ACS).

Product  
ACS

Privilege  
Security Administrator, Administrator, Operator

Mode  
Exec

The following prompt is displayed in the Exec mode:

[local] host_name#

Syntax

```
active-charging service ecs_service_name [ -noconfirm ]
```

- `ecs_service_name`
  Specifies name of the active charging service.
  `ecs_service_name` must be an alphanumeric string of 1 through 15 characters.
  If the named service does not exist, it is created and the CLI mode changes to the ACS Configuration Mode wherein the service can be configured.
  If the named service already exists, the CLI mode changes to the ACS Configuration mode wherein the specified active charging service can be configured.

- `-noconfirm`
  Executes the command without any additional prompt and confirmation from the user.

Usage

Use this command to create an active charging service in the system. This command can be used directly in Exec Mode after issuing the `require active-charging` command in the Global Configuration Mode. This command allows an operator (rather than security administrators and administrators) to configure the ACS functionality only.

On entering this command, the CLI prompt changes to:

```
[context_name] hostname(config-acs)#
```

**Important:** Operators need special CLI privilege for ACS functionality to be able to use this CLI command.

Example

The following command creates an active charging service named `test`:

```
active-charging service test
```
alarm

Disables the internal audible alarm on the system management card.

**Product**

All

**Privilege**

Security Administrator, Administrator, Operator

**Mode**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
alarm cutoff
```

**Usage**

Alarm cutoff disables the audible alarm. The alarm may be enabled following this command if an event within the system results in the audible alarm being enabled.

**Example**

```
alarm cutoff
```
**aps**

Allows the operator to perform SONET Automatic Protection Switching (APS) administrative operations.

> **Important:** Use of this command is limited to the OLC2 and the CLC2 line cards.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator, Operator

**Mode**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
aps { clear slot#/port# | exercise slot#/port# | lockout slot#/port# | switch { force | manual } slot#/port# }
```

---

**clear slot#/port#**

Clears the last switch command on the specified channelized port.

- `slot#/port#` is the CLC2/OLC2 slot number (valid range is 17 - 48) and appropriate port number (CLC2 valid range is 1 - 4; OLC2 valid value is 1).

---

**exercise slot#/port#**

Tests the APS protocol on line connected to port.

- `slot#/port#` is the CLC2/OLC2 slot number (valid range is 17 - 48) and appropriate port number (CLC2 valid range is 1 - 4; OLC2 valid value is 1)

---

**lockout slot#/port#**

Prevents the working port from switching to the protection port.

- `slot#/port#` is the CLC2/OLC2 slot number (valid range is 17 - 48) and appropriate port number (CLC2 valid range is 1 - 4; OLC2 valid value is 1)

---

**switch { force | manual } slot#/port#**

Switch to either the working port or the protection port:

  - **force:** Forces a switch of ports, even if there is an active alarm state.
  - **manual:** Implements a switch of ports if there are no active alarms.

- `slot#/port#` is the CLC2/OLC2 slot number (valid range is 17 - 48) and appropriate port number (CLC2 valid range is 1 - 4; OLC2 valid value is 1)
Usage

This command allows an operator to perform administrative/maintenance APS tasks such as testing the APS protocol, switching the working port to the protection port, and locking out the switching function.

Example

The following command starts an APS protocol test on port 2 of card 27:

```
aps exercise 27/2
```
autoconfirm

Enables or disables confirmation for certain commands. This command affects the current CLI session only.

**Important:** Use the `autoconfirm` command in the Global Configuration Mode to change the behavior for all future CLI sessions.

**Product**
All

**Privilege**
Security Administrator, Administrator, Operator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
autoconfirm

no autoconfirm
```

**Usage**

When `autoconfirm` is enabled, certain commands ask you to answer yes or no to confirm that you want to execute the command. When `autoconfirm` is disabled, the confirmation questions never appear. Disabling `autoconfirm` is active for the current session only.

By default `autoconfirm` is enabled.

**Example**

The following command enables command confirmation:

```
autoconfirm
```

The following command disables command confirmation for the duration of the current CLI session:

```
no autoconfirm
```
bulkstats force

Manages the collection and delivery of system statistics (bulkstats) to the configured server.

Product
All

Privilege
Security Administrator, Administrator, Operator

Mode
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax
bulkstats force { gather | transfer }

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>gather</td>
<td>Immediately collects the system statistics.</td>
</tr>
<tr>
<td>transfer</td>
<td>Immediately sends the currently collected statistics to the configured server.</td>
</tr>
</tbody>
</table>

Usage
When the current system statistics are desired immediately as opposed to the normal scheduled collection and delivery intervals issue this command. Troubleshooting the system may require the review of statistics at times when the scheduled delivery is not timely.

Example
The following causes the chassis to immediately collect system statistics. This would be in anticipation of a transfer command.

    bulkstats force gather

The following command causes the chassis to immediately send all collected statistics to the configured server.

    bulkstats force transfer
call-home send

Manages how Cisco Smart Call Home messages are sent to alert groups.

Product
All

Privilege
Security Administrator, Administrator, Operator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

**call-home send alert-group** { configuration profile profile name | inventory profile profile name }

<table>
<thead>
<tr>
<th>configuration profile profile name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sends configuration messages to the previously defined profile, expressed as an alphanumeric string of 1 through 31 characters.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>inventory profile profile name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sends inventory messages to the previously defined profile, expressed as an alphanumeric string of 1 through 31 characters.</td>
</tr>
</tbody>
</table>

Usage

Use this command to send specified alert-group call-home message from the CLI to all profiles subscribed to the specified alert group, or to a specified profile which does not need to be subscribed to the specified alert-group. For additional information, refer to the Call-Home Configuration Mode Commands and Call-Home Profile Configuration Mode Commands chapters.

Example

The following command sets the system to send configuration related call-home messages to the profile named Profile1.

```
call-home send alert-group configuration profile Profile1
```
call-home test

Sends a test Smart Call Home event message to a specified profile.

Product
All

Privilege
Security Administrator, Administrator, Operator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

call-home test message { test_message_content | profile profile name }

call-home test message message test_message_content

Defines the message to send to the defined profile as an alphanumeric string of 1 through 128 characters.

profile profile_name

Specifies the previously defined profile to which the message will be sent, expressed as an alphanumeric string of 1 through 31 characters.

Usage
Use this command to send test call-home messages from the CLI to a specified profile. If a message is not specified, the system sends out a default message.

Example
The following command sets the system to send a test call-home message Test_Message_1 to the profile named Profile1.

call-home test message Test_Message_1 profile Profile1
card busy-out

Moves processes from the source packet processing card to the destination packet processing card, or disables the packet processing card from accepting any new calls. When busy-out is enabled, the packet processing card stops receiving new calls but continues to process calls until they are completed. The command prompt is returned once the command is initiated. The busy-out procedure is completed in background. (ASR 5x00 only)

Product
All

Privilege
Security Administrator, Administrator, Operator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

card busy-out { migrate from src_slot to dst_slot } [ -noconfirm ]

no card busy-out

---

no

Disables busy-out. The packet processing card is re-enabled to accept new calls.

---

migrate from src_slot to dst_slot

Moves processes from the specified source packet processing card to the specified destination packet processing card. The command prompt is returned once the command is initiated. The card migration is completed in background.

src_slot indicates the source slot number of the card from which processes will be migrated. dst_slot indicates the destination slot number of the card to which processes will be migrated.

---

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

---

Usage

Migrating a packet processing card changes the active/standby status of a packet processing card. This results in the active sessions/processes being moved to the newly active card. This is useful when there is a maintenance activity on the active card which requires removing the card from service.

The destination slot specified must contain a packet processing card which is in the standby state for the command to complete successfully.

⚠️ Caution: Be cautious when executing this command. Depending on the number of active sessions being migrated, some subscribers may experience service interruptions.
Using busy-out to refuse new calls on a packet processing card allows you to take a card out of service without any interruptions to the end user. An individual system can be taken completely out of service gracefully by enabling busy-out on all packet processing cards and waiting for current calls to complete. The `show card info` command shows if busy-out is enabled.

**Important:** When a packet processing card fails, is migrated, or is restarted for any reason, busy-out is reset to disabled, the default behavior.

**Important:** This command is not supported on all platforms.

**Example**

The following command migrates the active processes from the packet processing card in slot 12 to the card in slot 14. This command executes after you provide confirmation of the request.

```
card migrate from 12 to 14
```

The following command migrates the active processes from the packet processing card in slot 1 to the card in slot 8. This command executes after you provide confirmation of the request.

```
card migrate from 1 to 8
```

The following command sets the packet processing card in slot 1 to stop accepting new calls:

```
card busy-out 1
```
card halt

Halts all StarOS processes on a card. A **card reboot** command must be issued to bring the card back into service after it is halted. (ASR 5x00 only)

**Product**
All

**Privilege**
Security Administrator, Administrator, Operator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
card halt slot_num [ -force ] [ -noconfirm ]
```

- **slot_num**
  Indicates the slot number of the card of interest.

- **-force**
  Over-rides any warnings to force the card to be halted.

- **-noconfirm**
  Executes the command without any additional prompt and confirmation from the user.

**Usage**

Halt a card to stop the card for maintenance or emergency situations.

⚠️ **Caution:** Caution should be taken in using this command. Halting a card which has no redundant card available may cause a service interruption and loss of active sessions.

⚠️ **Important:** On the ASR 5500, do not initiate a **card halt** for an active FSC if there are less than **two** active FSCs in the system. The system returns an error message if there are less than four active FSCs.

⚠️ **Caution:** The **-force** and **-noconfirm** options should only be used concurrently by experienced users as this will cause an immediate halt regardless of warnings and no confirmation from the user.

⚠️ **Important:** This command is not supported on all platforms.

**Example**

The following command temporarily stops the card in slot 1.
card halt 1

The following commands force the card to halt and indicate no confirmation is to take place, respectively.

    card halt 1 -force -noconfirm

    card halt 1 -noconfirm
card migrate

Migrates StarOS processes from an active packet processing card to a standby packet processing card. (ASR 5x00 only)

Product
All

Privilege
Security Administrator, Administrator, Operator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local] host_name#

Syntax

card migrate from src_slot to dst_slot [ -noconfirm ]

src_slot
Indicates the slot number of the packet processing card from which processes will be migrated. The packet processing card in this slot must be in Active mode.

dst_slot
Indicates the slot number of the packet processing card to which processes will be migrated.

-noconfirm
Executes the command without any additional prompt and confirmation from the user.

Usage
This command allows an operator to move processes from an active to a standby packet processing card.

Example
The following will cause processes currently running on the card in slot 8 to migrate to the standby card in slot 9. The migration will not occur if any warnings are generated.

    card migrate from 8 to 9
card reboot

Resets of the target card. For ASR 5000, rebooting a packet processing or line card will result in the card downloading the image from the active system management card. For ASR 5500, rebooting a card will result in the card downloading the image from the active MIO card.

Product
All

Privilege
Security Administrator, Administrator, Operator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

card reboot target_slot [ -force ] [ -noconfirm ]

target_slot
Initiates a reboot of the card in the specified the slot number.

-force
Indicates that the reboot is to take place ignoring any state or usage warnings that might be generated.

-noconfirm
Executes the command without any additional prompt and confirmation from the user.

Usage
A reboot is used to reset the card and receive a new download. This may be useful when a card is not responding or when it is necessary to cause the card to reload its image and restart.

⚠️ Caution: Caution should be taken in using this command. Rebooting a card which has no redundant card available may cause a service interruption and loss of active sessions.

⚠️ Important: On the ASR 5500, do not initiate a card reboot for an active FSC if there are less than four active FSCs in the system. The system returns an error message if there are less than four active FSCs.

⚠️ Caution: The -force and -noconfirm options should only be used concurrently by experienced users as this will cause an immediate reboot regardless of warnings and no confirmation from the user.

⚠️ Important: This command is not supported on all platforms.
Example

The following will cause the card in slot 8 to reboot without any confirmation from the user. The card will not reboot if there are any warnings generated.

    card reboot 8 -noconfirm

The following command will cause the card in slot 8 to reboot regardless of any warnings. The user must provide confirmation prior to this command executing.

    card reboot 8 -force

The following command will cause the card in slot 8 to reboot regardless of any warnings with no additional user confirmation.

    card reboot 8 -force -noconfirm
card restart

Performs a soft-reset of the target card causing all application processes to restart. (ASR 5x00 only)

Product
All

Privilege
Security Administrator, Administrator, Operator

Mode
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

card restart target_slot [ -force ] [ -noconfirm ]

- **target_slot**
  Initiates a restart of the card in the specified slot number.

- **-force**
  Indicates the restart is to take place ignoring any state or usage warnings that might be generated.

- **-noconfirm**
  Executes the command without any additional prompt and confirmation from the user.

Usage
Restarting a card may be useful when a card is not performing as expected (performance drop, increased response delays, etc.). A restart may be preferred to a reboot as the card becomes available in less time than a reboot.

When this command is issued for an active card, the user is prompted for confirmation unless the -force and/or -noconfirm keywords are used. Because the reboot of standby or redundant cards is non-service impacting, the reboot proceeds immediately after the command execution without user confirmation.

⚠️ **Caution:** Caution should be taken in using this command. Restarting a card which has no redundant card available may cause a service interruption and loss of active sessions.

🔍 **Important:** This command is not supported on all platforms.

⚠️ **Caution:** The -force and -noconfirm options should only be used concurrently by experienced users as this will cause an immediate restart regardless of warnings and no confirmation from the user.

Example
The following will cause the card in slot 8 to restart without any confirmation from the user. The card will not reboot if there are any warnings generated.

```
card restart 8 -noconfirm
```

The following command will cause the card in slot 8 to restart regardless of any warnings. The user must provide confirmation prior to this command executing.

```
card restart 8 -force
```

The following command will cause the card in slot 8 to restart regardless of any warnings with no additional user confirmation.

```
card restart 8 -force -noconfirm
```
**card switch**

Manages card pairs and their active/standby status. (ASR 5x00 only)

**Product**
All

**Privilege**
Security Administrator, Administrator, Operator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
card switch { from target_slot | to target_slot } [ -noconfirm ]
```

- `from target_slot`
  Specifies the slot number of a currently active card that is to be switched. The slot number must be valid and contain a card in active mode.

- `to target_slot`
  Specifies the slot number of a standby card which is to become the active card. The slot number must be valid and contain a card in standby.

- `-noconfirm`
  Executes the command without any additional prompt and confirmation from the user.

**Usage**

Card switch-overs change the active/standby status of a card. This is useful when there is a maintenance activity on the active card which requires removing the card from service.

⚠️ **Caution:** Caution should be taken in using this command. Depending on the amount of bandwidth/traffic being switched, some subscribers may experience service interruptions.

ℹ️ **Important:** This command is not supported on all platforms.

**Example**

The following command switches the active/standby status of the line cards in slots 17 and 18. This command only executes after you provide confirmation of the request.

```bash
card switch from 17 to 18
```

The following command switches the active/standby status of the cards in slots 1 and 2. This command executes immediately with no additional user confirmation.
card switch from 1 to 2 -noconfirm
card upgrade

Upgrades the programmable memory on a card. (ASR 5x00 only)

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
card upgrade slot_number[ -noconfirm ]
```

*slot_number*

The slot number of the card to be upgraded, for ASR 5000: from 1 through 16, and for ASR 5500: from 1 through 10.

* -noconfirm

Executes the command without any additional prompt and confirmation from the user.

⚠️ **Caution:** Use this command only if instructed by or working with Technical Assistance Center personnel.

ℹ️ **Important:** On the ASR 5500, do not initiate a `card upgrade` for an active FSC if there are less than four active FSCs in the system. The system returns an error message if there are less than four active FSCs.

**Usage**

You can only initiate an upgrade if:
- there is no migration occurring,
- the card is active or standby,
- there is no online upgrade in progress.

ℹ️ **Important:** The following operations are not allowed while a card is upgrading: change edc requirement (config), change card [no] shutdown (config), change card active (config), change card redundancy (config), card halt (exec), card reboot (exec), start an online upgrade.

ℹ️ **Important:** Level unlock operations are ignored while a card is upgrading.
Important: This command is not supported on all platforms.

Example

The following command initiates a packet processing card upgrade on slot number 10:

```
card upgrade 10
```
cdr-push

Initiates a manual push of CDR files to a configured URL or Local - External Storage System (L-ESS).

**Product**
All

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
cdr-push { all | local-filename file_name }
```

- **all**
  Pushes all CDR files to the configured URL.

- **local-filename file_name**
  Pushes only the specified file to the configured URL.
  
  *file_name* must be the absolute path of the local file to push, and must be an alphanumeric string of 1 through 1023 characters.

**Usage**

Use this command to manually push CDR files to the configured URL or L-ESS. For information on configuring the L-ESS, see the `cdr` command in the **EDR Module Configuration Mode Commands** and the **UDR Module Configuration Mode Commands** chapters.

**ASR 5000**: Run this command only from the local context. If you are in any other context, you will see this failure message: “Failure: Manual PUSH of CDRs supported only in the local context”

**ASR 5500**: Run this command only from the local context. If you are in any other context, you will see this failure message: “Failure: Manual PUSH of CDRs supported only in the local context”

**Example**

The following command pushes all CDR files to the URL:

```
cdr-push all
```
chassis

Identifies the chassis that can encrypt and decrypt encrypted passwords in the configuration file. If two or more chassis are configured with the same chassis key value, the encrypted passwords can be decrypted by any of the chassis sharing the same chassis key value. As a corollary to this, a chassis key value will not be able to decrypt the passwords that were encrypted using a different chassis key value.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

[ no ] chassis { key value key_string | keycheck key_string }

no

Resets the chassis key to the factory default value. The factory default value is unique to the chassis. Once this command is executed, the chassis key value command can be used to change the default chassis key.

key value key_string

Specifies the chassis key value as an alphanumeric string of 1 through 16 characters.

The chassis key value is stored as a one-way encrypted value, much like a password. It is never displayed in its plain-text form.

keycheck key_string

Generates a one-way encrypted key value based on the entered alphanumeric string of 1 through 16 characters.

The generated encrypted key value is compared against the encrypted key value of the previously entered chassis key value. If the encrypted values match, then the command succeeds and key check passes. If the comparison fails, a message is displayed indicating that the key check has failed. Note that if the default chassis key (no chassis key) is currently being used, this key check will always fail since there will be no chassis key value to compare against.

Usage
Establish multiple, unique chassis keys to encrypt and decrypt passwords in configuration files.

Example

The following command generates a one-way encrypted key based on the string tewks367.

chassis key value tewks367
clear aaa

Clears all Authentication, Authorization, and Accounting (AAA) statistics for the current context.

**Product**
- PDSN
- GGSN
- ASN-GW
- P-GW
- SAEGW

**Privilege**
- Security Administrator, Administrator, Operator

**Mode**
- Exec

The following prompt is displayed in the Exec mode:

```
[local] host_name#
```

**Syntax**

```
clear aaa local counters
```

**Usage**
Clearing the AAA statistics may be useful when monitoring the statistics manually. Clearing resets the counters to zero. The keyword `local` is not intended to imply the local context defined for all systems. Rather, it indicates the statistics within the current context are to be cleared.

**Example**

The following command zeroes out all the AAA statistics in the current context.

```
clear aaa local counters
```
clear active-charging analyzer statistics

Clears protocol analyzer statistics.

Product

ACS

Privilege

Security Administrator, Administrator, Operator

Mode

Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

```
clear active-charging analyzer statistics [ name protocol_name ] [ | { grep grep_options | more } ]
```

- **name protocol_name**
  
  Clears statistics for the specified protocol analyzer. If this keyword is not specified all statistics are cleared. `protocol_name` must be one of the following:
  
  - `dns`
  - `file-transfer`
  - `ftp`
  - `http`
  - `icmp`
  - `icmpv6`
  - `imap`
  - `ip`
  - `ipv6`
  - `mms`
  - `p2p` [ `application p2p_list` | `protocol-group group_list` ]: Peer-to-peer analyzer.
    
    - `p2p application p2p_list`: The supported applications are:
      
      - `actionvoip`
      - `actsync`
      - `adobeconnect`
      - `aimini`
      - `amazoncloud`
      - `antsp2p`
      - `apple-push`
clear active-charging analyzer statistics

• apple-store
• applejuice
• applemaps
• ares
• armagetron
• avi
• badoo
• baidumovie
• battlefld
• bbm
• beatport
• bitcasa
• bittorrent
• bittorrent-sync
• blackberry-store
• blackberry
• blackdialer
• box
• callofduty
• chikka
• cisco-jabber
• citrix
• clubbox
• clubpenguin
• crossfire
• cyberghost
• ddlink
• didi
• directconnect
• dofus
• dropbox
• edonkey
• facebook
• facetime

⚠️ Important: The facetime protocol is available only in releases 9.0 and 11.0. This protocol is not available in release 10.0.
*fasttrack
*feidian
*fiesta
*filetopia
*flash
*flickr
*florensia
*foursquare
*freenet
*friendster
*fring
*funshion
*gadu_gadu
*gamekit

**Important:** The gamekit protocol is available only in releases 9.0 and 11.0. This protocol is not available in release 10.0.

*gmail
*gnutella
*goober
*google-music
*google-push
*google
*googleplay
*googleplus
*gotomeeting
*gtalk
*guildwars
*halflife2
*hamachivpn
*hbogo
*heytell
*hike-messenger
*hls
*hotspotvpn
*hulu
*hyves
clear active-charging analyzer statistics

• iax
• icall
• icecast
• icloud
• idrive
• igo
• iheartradio
• imesh
• imessage
• imgur
• imo
• instagram
• iplayer
• iptv
• irc
• isakmp
• iskoot
• itunes
• jabber
• jap
• jumblo
• kakaotalk
• kik-messenger
• kontiki
• kugoo
• kuro
• linkedin
• lync
• magicjack
• manolito
• mapfactor
• mapi
• maplestory
• meebo
• mgcp
• mojo
• monkey3
- mozy
- msn
- msrp
- mute
- mypeople
- myspace
- nateontalk
- naverline
- navigon
- netmotion
- nimbuzz
- nokia-store
- octoshape
- off
- ogg
- oist
- oovoo
- opendrive
- openft
- openvpn
- orb
- oscar
- outlook
- paltalk
- pando
- pandora
- path
- pcanywhere
- pinterest
- plingm
- poco
- popo
- pplive
- ppstream
- ps3
- qq
- qqqgame
clear active-charging analyzer statistics

• qqlive
• quake
• quicktime
• radio-paradise
• radius
• rdp
• rdt
• regram
• rfactor
• rhapsody
• rmstream
• rodi
• rynga
• samsung-store
• scydo
• secondlife
• shoutcast
• silverlight
• siri
• skinny
• skydrive
• skype
• slacker-radio
• slingbox
• smartvoip
• snapchat
• softether
• sopcast
• soribada
• soulseek
• soundcloud
• spdy
• speedtest
• splashfighter
• spotify
• ssdp
• stealthnet
• steam
• stun
• sudaphone
• svtplay
• tagged
• talkatone
• tango
• teamspeak
• teamviewer
• telegram
• thunder
• tor
• truecaller
• truphone
• tumblr
• tunnelvoice
• tvants
• tvuplayer
• twitter
• twitch
• ultrabac
• ultrasurf
• upc-phone
• usenet
• ustream
• uusee
• vchat
• veehtv
• viber
• vine
• voipdiscount
• vopium
• vpnx
• voxer
• vtok
• vtun
• warcft3
clear active-charging analyzer statistics

• waze
• webex
• wechat
• weibo
• whatsapp
• wii
• windows-azure
• windows-store
• winmx
• winny
• wmstream
• wofkungfu
• wofwarcraft
• wuala
• xbox
• xdcc
• xing
• yahoo
• yahoomail
• youku
• yourfreetunnel
• youtube
• zattoo

p2p protocol-group group_list: The supported P2P protocol groups are:

• generic
• anonymous-access
• business
• communicator
• cloud
• e-store
• e-mail
• e-news
• internet-privacy
• filesharing
• gaming
• p2p-filesharing
clear active-charging analyzer statistics

- `p2p`: p2p
- `anon`: anon
- `filesharing`: filesharing
- `remote-control`: remote-control
- `social-nw-gaming`: social-nw-gaming
- `social-nw-generic`: social-nw-generic
- `social-nw-videoconf`: social-nw-videoconf
- `standard`: standard
- `streaming`: streaming
- `pop3`: pop3
- `pptp`: pptp
- `rtcp`: rtcp
- `rtp`: rtp
- `rtsp`: rtsp
- `sdp`: sdp
- `secure-http`: secure-http
- `sip`: sip
- `smtp`: smtp
- `tcp`: tcp
- `tftp`: tftp
- `udp`: udp
- `wsp`: wsp
- `wtp`: wtp

**grep grep_options | more**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of `grep` and `more`, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter.

**Usage**

Use this command to clear ACS analyzer statistics.

**Example**

The following command clears active charging service analyzer information for TCP analyzer:

```
    clear active-charging analyzer statistics name tcp
```
clear active-charging charging-action statistics

Clears ACS charging action statistics.

Product
ACS

Privilege
Security Administrator, Administrator, Operator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

```
clear active-charging charging-action statistics [ name charging_acion_name ] [ | { grep grep_options | more } ]
```

- **name charging_acion_name**
  Clears statistics for the specified charging action. `charging_acion_name` must be the name of a charging action, and must be an alphanumeric string of 1 through 63 characters.

- **grep grep_options | more**
  Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent. For details on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage

Use this command to clear active charging action statistics.

Example

The following command clears active charging action statistics information for charging action named `pre-paid`:

```
clear active-charging charging-action statistics name pre-paid
```
clear active-charging content-filtering server-group statistics

Clears statistics for all/a specific CF server group.

**Product**
CF

**Privilege**
Security Administrator, Administrator, Operator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
clear active-charging content-filtering server-group statistics [ name cf_server_group_name ] [ | { grep grep_options | more } ]
```

- **name cf_server_group_name**
  Clears statistics for the specified CF server group.
  *cf_server_group_name* must be the name of a CF server group, and must be an alphanumeric string of 1 through 15 characters.

- **grep grep_options | more**
  Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
  For details on the usage of *grep* and *more*, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter.

**Usage**

Use this command to clear content filtering statistics for CF server groups.

**Example**

The following command clears category-based content filtering statistics information for Rulebase named *cf_rule1*:

```
clear active-charging content-filtering category statistics rulebase name cf_rule1
```
clear active-charging credit-control statistics

Clears credit control statistics.

Product
ACS

Privilege
Security Administrator, Administrator, Operator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

```
clear active-charging credit-control statistics [ group cc_group_name | server { ip-address ip_address | name cc_group_name } ]
```

clear active-charging credit-control statistics
Clears statistics for all credit control groups.

```group cc_group_name```

Clears statistics for the specified credit control group.

*cc_group_name* must be an alphanumeric string of 1 through 63 characters.

```server { ip-address ip_address | name cc_group_name }```

Clears statistics for the credit control server specified as:

- **ip-address**: an IP address for the credit control group entered in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation

- **cc_group_name**: name of the credit control group server entered as an alphanumeric string of 1 through 127 characters.

Usage

Use this command to clear credit control statistics.

Example

The following command clears statistics information for credit control:

```
clear active-charging credit-control statistics
```
clear active-charging dns-learnt-ip-addresses

Clears DNS learnt IP address statistics for the DNS Snooping feature.

Product
ACS

Privilege
Security Administrator, Administrator, Operator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

```
clear active-charging dns-learnt-ip-addresses statistics sessmgr { all | instance sessmgr_instance } [ | { grep grep_options | more } ]
```

```
sessmgr { all | instance sessmgr_instance }

*all*: Clears statistics for all SessMgr instances.

*instance sessmgr_instance*: Clears statistics for the specified SessMgr instance.

`sessmgr_instance` must be an integer from 1 through 65535.

```
grep grep_options | more
```

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage

Use this command to clear DNS learnt IP address statistics for the DNS Snooping feature.

On clearing the statistics using this command, only the entries-flushed, entries-replaced, and IP-Overflows statistics are cleared as these are cumulative statistics. Total-entries will not be cleared as it is an instantaneous statistic of the current total entries in that rule line.

Example

The following command clears all DNS learnt IP address statistics:

```
clear active-charging dns-learnt-ip-addresses statistics sessmgr all
```
clear active-charging edr-format statistics

Clears ACS statistics for all or a specific Event Data Record (EDR) format.

Product
ACS

Privilege
Security Administrator, Administrator, Operator

Mode
Exec
The following prompt is displayed in theExec mode:
[local]host_name#

Syntax

clear active-charging edr-format statistics [ name edr_format_name ]

name edr_format_name
Clears statistics for the specified EDR format.

edr_format_name must be the name of an EDR format, and must be an alphanumeric string of 1 through 63 characters.

Important: If an EDR format name is not specified, statistics for all EDR formats are cleared.

Usage
Use this command to clear the accumulated statistics for the specified EDR format.

Example
The following command clears the statistics for all EDR formats:

clear active-charging edr-format statistics
**clear active-charging edr-udr-file statistics**

Clears Event Data Record (EDR) and Usage Data Record (UDR) file related statistics.

**Product**  
ACS

**Privilege**  
Security Administrator, Administrator, Operator

**Mode**  
Exec  
The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
clear active-charging edr-udr-file statistics
```

**Usage**

Use this command to clear EDR and UDR file statistics.

**Example**

The following command clears statistical information for EDR and UDR files:

```
  clear active-charging edr-udr-file statistics
```
clear active-charging firewall statistics

Clears Stateful Firewall statistics.

Product
PSF

Privilege
Security Administrator, Administrator, Operator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

clear active-charging firewall statistics [ callid call_id | domain-name domain_name | nat-realm nat_realm_name | protocol { icmp | icmpv6 | ip | ipv6 | other | tcp | udp } | username user_name ] [ acsmgr instance instance_id ] [ | { grep grep_options | more } ]

acsmgr instance instance_id

Specifies an ACS Manager instance ID as an integer from 1 through 65535.

callid call_id

Specifies a call identification number as an eight-byte hexadecimal number.

domain-name domain_name

Specifies the domain name.

domain_name must be an alphanumeric string of 1 through 127 characters.

nat-realm nat_realm_name

Specifies the NAT realm.

nat_realm_name must be an alphanumeric string of 1 through 31 characters.

protocol { icmp | ip | other | tcp | udp }

Specifies a protocol for the statistics.

• icmp: ICMPv4
  • icmpv6
  • ip: IPv4
  • ipv6
  • other: Protocols other than TCP, UDP, and ICMPv4/ICMPv6
  • tcp
  • udp
username  user_name

Specifies the user name.
user_name must be an alphanumeric string of 1 through 127 characters.

grep  grep_options | more

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage

Use this command to clear Stateful Firewall statistics.

Example

The following command clears all Stateful Firewall statistics:

   clear active-charging firewall statistics
**clear active-charging firewall track-list**

Clears the list of servers being tracked for involvement in any Denial-of-Service (DOS) attacks.

**Product**
PSF

**Privilege**
Security Administrator, Administrator, Operator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
clear active-charging firewall track-list attacking-servers
```

**Usage**
Use this command to clear the list of servers being tracked for involvement in any DOS attacks.

**Example**

The following command clears the list of servers being tracked for involvement in any DOS attacks:

```
clear active-charging firewall track-list attacking-servers
```
clear active-charging fw-and-nat policy statistics

Clears statistics for all or a specific Firewall-and-NAT policy.

**Product**
PSF
NAT

**Privilege**
Security Administrator, Administrator, Operator

**Mode**
Exec
The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
clear active-charging fw-and-nat policy statistics { all | name policy_name } [ | { grep grep_options | more } ]
```

---

**all**
Clears information for all Firewall-and-NAT policies.

**name policy_name**
Clears information for the specified Firewall-and-NAT policy.
`policy_name` must be the name of a Firewall-and-NAT policy, and must be an alphanumeric string of 1 through 63 characters.

**grep grep_options | more**
Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

---

**Usage**
Use this command to clear statistics for all or a specific firewall-and-NAT policy.

**Example**
The following command clears statistics for the firewall-and-NAT policy named `test123`:

```
clear active-charging fw-and-nat policy statistics name test123
```
clear active-charging group-of-ruledefs statistics

Clears ACS group of ruledefs statistics.

**Product**
ACS

**Privilege**
Security Administrator, Administrator, Operator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local] host_name#
```

**Syntax**

```
clear active-charging group-of-ruledefs statistics [ name group_of_ruledefs ] [ | { grep grep_options | more } ]
```

<table>
<thead>
<tr>
<th><strong>name group_of_ruledefs</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Clears statistics for the specified group of ruledefs.</td>
</tr>
<tr>
<td><code>group_of_ruledefs</code> must be the name of a group of ruledefs, and must be an alphanumeric string of 1 through 63 characters.</td>
</tr>
</tbody>
</table>

| **grep grep_options | more** |
|---------------------|
| Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent. |
| For details on the usage of `grep` and `more`, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter. |

**Usage**

Use this command to clear statistical information related to all or specified Active Charging Service group of ruledefs.

**Example**

The following command clears statistical information related to the group of ruledefs named `ruledef_group12`:

```
clear active-charging group-of-ruledefs statistics name ruledef_group12
```
clear active-charging nat statistics

Clears NAT realm statistics.

**Product**
NAT

**Privilege**
Security Administrator, Administrator, Operator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

**Syntax**

```
clear active-charging nat statistics [ nat-realm nat_realm_name ] [ | { grep grep_options | more } ]
```

- **clear active-charging nat statistics**
  
  This command when issued in the local context clears statistics for all NAT realms in all contexts. When issued within a specific context, this command clears statistics for all NAT realms in that context.

- **nat-realm nat_realm_name**
  
  This command when issued in the local context clears statistics for the specified NAT realm in all contexts. When issued in a specific context, this command clears statistics for the specified NAT realm in that context.

  *nat_realm_name*: Specifies name of the NAT realm as an alphanumeric string of 1 through 31 characters.

- **grep grep_options | more**
  
  Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent. For details on the usage of `grep` and `more`, refer to the `Regulating a Command’s Output` section of the `Command Line Interface Overview` chapter.

**Usage**

Use this command to clear NAT realm statistics.

**Example**

The following command when issued in the local context, clears NAT realm statistics for NAT realms named `test135` in all contexts:

```
clear active-charging nat statistics nat-realm test135
```
clear active-charging regex statistics

Clears regular expression (regex) related statistics.

Product
ACS

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

```
clear active-charging regex statistics ruledef { all | instance instance_number }
```

- **all**
  Clears all regex-related statistics.

- **instance instance_number**
  Clears regex-related statistics for specified Session Manager instance.
  *instance_number* must be an integer from 1 through 65535.

Usage

Use this command to clear regular expression (regex) related statistics.

Example

The following command clears all regex-related statistics:

```
clear active-charging regex statistics ruledef all
```
clear active-charging rulebase statistics

Clears ACS rulebase statistics.

**Product**
ACS

**Privilege**
Security Administrator, Administrator, Operator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
clear active-charging rulebase statistics [ name rulebase_name ] [ | { grep grep_options | more } ]
```

- **rulebase_name**
  Clears statistics for the specified ACS rulebase.
  *rulebase_name* must be the name of a rulebase, and must be an alphanumeric string of 1 through 15 characters.

- **grep grep_options | more**
  Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent. For details on the usage of **grep** and **more**, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter.

**Usage**

Use this command to clear ACS rulebase statistics.

**Example**

The following command clears statistics for the ACS rulebase named *postpaid*:

```
clear active-charging rulebase statistics name postpaid
```
clear active-charging ruledef statistics

Clears statistics for rule definitions configured in the Active Charging Service (ACS).

Product
ACS

Privilege
Security Administrator, Administrator, Operator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

clear active-charging ruledef statistics [ charging | firewall | name ruledef_name | tpo ] [ | { grep grep_options | more } ]

charging
Clears statistics for all charging ruledefs.

firewall
Clears statistics for all Stateful Firewall ruledefs.

name ruledef_name
Clears statistics for the specified ruledef.

ruledef_name must be the name of a ruledef, and must be an alphanumeric string of 1 through 63 characters.

tpo

Important: The Traffic Performance Optimization (TPO) in-line service is not supported in this release.

grep grep_options | more
Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage
Use this command to clear ACS ruledef statistics.

Example
The following command clears all ruledef statistics:

clear active-charging ruledef statistics
clear active-charging subsystem

Clears all ACS subsystem information.

**Product**
ACS

**Privilege**
Security Administrator, Administrator, Operator

**Mode**
Exec
The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
clear active-charging subsystem
```

**Usage**
Use this command to clear all ACS subsystem information.

**Example**
The following command clears all ACS subsystem information:

```
clear active-charging subsystem
```
clear active-charging tcp-proxy statistics

Clears ACS TCP Proxy statistics.

Product
ACS

Privilege
Security Administrator, Administrator, Operator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

clear active-charging tcp-proxy statistics [ all | ip-layer | proxy-fac | rulebase rulebase_name | socket-migration | tcp-layer ]

all
Clears all TCP Proxy statistics.

ip-layer
Clears TCP Proxy statistics for IP layer.

proxy-fac
Clears TCP Proxy Flow Admission Control statistics.

rulebase rulebase_name
Clears TCP Proxy statistics for the specified rulebase. 
rulebase_name must be the name of a rulebase, and must be an alphanumeric string of 1 through 63 characters.

socket-migration
Clears TCP Proxy Socket Migration related statistics.

tcp-layer
Clears TCP Proxy statistics for TCP layer.

Usage

Use this command to clear TCP Proxy statistics.

Example

The following command clears TCP Proxy statistics for the rulebase named test14:

clear active-charging tcp-proxy statistics rulebase test14
clear active-charging tethering-detection statistics

Clears statistics pertaining to the Tethering Detection feature.

**Product**
ACS

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local] host_name#
```

**Syntax**

```
clear active-charging tethering-detection statistics
```

**Usage**

Use this command to clear statistics pertaining to the Tethering Detection feature.
clear active-charging tpo policy statistics

The Traffic Performance Optimization (TPO) in-line service is not supported in this release.
clear active-charging tpo profile statistics

The Traffic Performance Optimization (TPO) in-line service is not supported in this release.
clear active-charging url-blacklisting statistics

Clears URL Blacklisting feature related statistics.

Product
CF

Privilege
Security Administrator, Administrator, Operator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

clear active-charging url-blacklisting statistics [ rulebase name rulebase_name ] [ | { grep grep_options | more } ]

rulebase name rulebase_name

Clears URL Blacklisting information for the specified rulebase.

rulebase_name must be the name of a rulebase, and must be an alphanumeric string of 1 through 63 characters.

grep grep_options | more

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage

Use this command to clear URL Blacklisting feature related statistics, optionally for a specific rulebase.

Example

The following command clears URL Blacklisting feature related statistics for rulebase12:

clear active-charging url-blacklisting statistics rulebase name rulebase12
clear active-charging video detailed-statistics

Resets the detailed statistics for TCP video flows.

**Product**
MVG

**Privilege**
Security Administrator, Administrator, Operator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
clear active-charging video detailed-statistics
```

**Usage**
Use this command to reset the detailed statistics for TCP video flows.

**Example**

The following command resets the detailed statistics for TCP video flows:

```
clear active-charging video detailed-statistics
```
clear administrator

Ends the session of an administrative user specified by either user name or session ID.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

```
clear administrator { name user_name | session id id_num }
```

- **name user_name**
  Identifies the user name of the administrative user.

- **session id id_num**
  Identifies the ID number of the administrative user session as displayed in the output of the `show administrators session id` command.

Usage
This command is used to terminate command line interface sessions for other administrative users.

Example
The following command ends the session of the administrative user identified as `user1`:

```
clear administrator name user1
```

The following command ends the session of the administrative user with the session ID of 3:

```
clear administrator session id 3
```
clear alarm

Clears outstanding alarm conditions

**Product**
All

**Privilege**
Security Administrator, Administrator, Operator

**Mode**
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

**Syntax**

```plaintext
clear alarm { all | chassis | id num | port slot/port | slot slot }
```

- **all**
  Clear all outstanding alarms

- **chassis**
  Clears chassis-wide and fan tray alarms

- **id num**
  Clears a specific alarm by its internal alarm ID. `num` is the internal alarm identification number.

- **port slot/port**
  Clears alarms for the specified port. `slot/port` is the card slot and port on the card for which to clear alarms.

- **slot slot**
  Clears alarms for the specified slot. `slot` is the card slot for which to clear alarms.

**Usage**
Use this command to clear outstanding alarm conditions.

**Example**
To clear all outstanding alarms, use the following command:

```plaintext
clear alarm all
```

To clear all alarms for slot 7, enter the following command:

```plaintext
clear alarm slot 7
```
Clears the Access Link Control Application Part (ALCAP) session statistics of an ALCAP service associated with a Home-NodeB Gateway (HNB-GW) service instance configured and running on a system.

**Product**
HNB-GW

**Privilege**
Operator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
clear alcap statistics [ alcap-service alcap_svc_name [ aal2-node aal2_node_name [ aal2-path aal2_path_id ] ] ]
```

- **alcap-service alcap_svc_name**
  Specifies the name of the ALCAP service for which statistics are to be cleared.

- **aal2-node aal2-node**
  Specifies the name of the ATM Adaptation Layer 2 (AAL2) node for which ALCAP service statistics will be cleared.

- **aal2-path aal2_path_id**
  Specifies the identity number of the AAL2 path on a specific ATM Adaptation Layer 2 (AAL2) node for which ALCAP service statistics will be cleared.

**Usage**

This command is used to clear the sessions statistics and counters for ALCAP service.

**Example**

The following command clears the service session statistics of ALCAP service named as `alcap_hnb_svc1`:

```
clear alcap statistics alcap-service alcap_svc1
```
clear asngw-service

Clears the service session statistics for an Access Service Network Gateway (ASN-GW) service specified by either service name or trusted peer address.

Product
ANS-GW

Privilege
Security Administrator, Administrator

Mode
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

```
clear asngw-service statistics [ name svc_name | peer-address ip_address ]
```

<table>
<thead>
<tr>
<th>name svc_name</th>
</tr>
</thead>
</table>
| Identifies the name of the ASN-GW service for which statistics will be cleared. svc_name must be an alphanumeric string of 1 through 63 characters.

<table>
<thead>
<tr>
<th>peer-address ip_address</th>
</tr>
</thead>
</table>
| Identifies the IP address of the ASN-GW peer for which service statistics will be cleared. ip_address must be entered in IPv4 dotted-decimal notation.

Usage
This command is used to terminate command line interface sessions for ASN GW services.

Example
The following command clears the service session statistics of the ASN-GW service named aasn_svc1:

```
clear asngw-service statistics name aasn_svc1
```
clear asnpc-service

Clears the service session statistics of an ASN paging controller service specified by either ASN PC service name or trusted paging controller peer address.

**Product**
ANS-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
clear asnpc-service statistics [ name svc_name | peer-address ip_address ]
```

- **name svc_name**
  Identifies the name of the ASN PC service for which session statistics will be cleared. *svc_name* must be an alphanumeric string of 1 through 63 characters.

- **peer-address ip_address**
  Identifies the IP address of the ASN PC peer for which all service statistics will be cleared. *ip_address* must be entered in IPv4 dotted-decimal notation.

**Usage**

This command is used to terminate command line interface sessions for ASN PC services.

**Example**

The following command clears the service session statistics of ASN PC service named as *asnpc_svc1*:

```
clear asnpc-service statistics name asnpc_svc1
```
clear apn statistics

Deletes all previously gathered statistics for either a specific Access Point Name (APN) or all APNs configured with the given context.

Product

GGSN
P-GW
SAEGW

Privilege

Security Administrator, Administrator, Operator

Mode

Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

clear apn statistics [ name apn_name | smgr-instance instance ] [ | { grep grep_options | more } ]

<table>
<thead>
<tr>
<th>name apn_name</th>
</tr>
</thead>
</table>
| Specifies the name of a specific APN configured in the context for which to clear statistics. `apn_name` is the name of the APN expressed as an alphanumeric string of 1 through 63 characters that is case sensitive.

<table>
<thead>
<tr>
<th>smgr-instance instance</th>
</tr>
</thead>
</table>
| Specifies a particular Sessmgr instance in the context for which to clear APN statistics. `instance` must be an integer from 1 to 4294967295.

<table>
<thead>
<tr>
<th>grep grep_options</th>
<th>more</th>
</tr>
</thead>
</table>
| Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent. For details on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage

Statistics for a single APN can be cleared using the `name` keyword. Statistics for all APNs in the context can be deleted by entering the command with no keywords.

If this command is executed from within the local context with no keywords, statistics will be cleared for every APN configured on the system regardless of context. In addition, if the `name` keyword is used when executing from within the local context, statistics for all APNs configured with the specified name will be cleared regardless of context.

Example

The following command clears statistics for an APN called `isp1`:

```
clear apn statistics name isp1
```
clear bcmcs statistics

Clears Broadcast Multicast Service (BCMCS) statistics.

Product
PDSN

Privilege
Security Administrator, Administrator, Operator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

```
clear bcmcs statistics [ psdn-service service_name ]
```

```
psdn-service service_name
```

Specifies a specific PDSN service for which to clear BCMCS-specific statistics. This value must be an alphanumeric string of 1 through 63 characters.

Usage

Use this command to clear accumulated BCMCS statistics. You may specify an individual PDSN or peer to selectively clear statistics.

Example

```
clear bcmcs statistics

clear bcmcs statistics psdn-service service_name
```
clear blacklisted-gtpu-bind-address

Clears the GTP-U loopback address blacklisted by a specific radio network controller (RNC) as defined for a specific IuPS Service configuration.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator, Operator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

**Syntax**

```
clear blacklisted-gtpu-bind-address ip_address rnc-id rnc_id mcc mcc_num mnc mnc_num
iups-service name
```

* ip_address
  Specifies the IP loopback address that has been blacklisted in IPv4 dotted-decimal notation. This loopback address was originally defined with the `associate-gtpu-bind-address` command in the Radio-Network-Controller Configuration mode of the IuPS Service.

**Usage**

This command enables this loopback address to be used for future RAB-assignment requests.

**Example**

```
clear blacklisted-gtpu-bind-address 1.1.1.1 rnc-id 2 mcc 123 mnc 321
iups-service iups1
```
clear bssap+ statistics

Clears the BSSAP+ protocol (base station subsystem GPRS protocol) statistics collected for the Gs interface between the SGSN and the MSC/VLR.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator, Operator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
clear bssap+ statistics [ gs-service gs_svc_name ] [ vlr { isdn-number ISDN_Num| name vlr_name } ] [ | { grep grep_options | more } ]
```

---

**gs-service gs_svc_name**
Specifies the name of a preconfigured Gs service handling BSSAP+ information as an alphanumeric string of 1 through 63 characters that is case sensitive.

**vlr { isdn-number ISDN_Num| name vlr_name**
Specifies a VLR (by ISDN number or name) handling BSSAP+ information.

- **isdn-number ISDN_Num** is the configured E.164-type ISDN number for the VLR. Enter a numerical string of 1 to 15 digits.
- **name vlr_name** is the configured name of the VLR entered as an alphanumeric string of 1 through 63 characters.

---

**Usage**

Use this command to delete or clear collected BSSAP+ protocol statistics for the entire SGSN or for a specified Gs interface. Using the keywords of this command, the interface can be identified by defining a specific VLR connected to the SGSN or by identifying the Gs service to which the interface has been configured.

**Example**

The following command clears the BSSAP+ statistics collected for the Gs interface configured for the Gs service named gssvc1.

```
clear bssap+ statistics gs-service gssvc1
```
clear bssgp statistics

Clears collected BSSGP protocol (base station subsystem GPRS protocol) statistics for traffic between the base station subsystem (BSS) and the SGSN.

Product
SGSN

Privilege
Security Administrator, Administrator, Operator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

clear bssgp statistics [ gprs-service gprs_svc_name | nse nse_id [ bvc bvc_id ] ] [ | { grep grep_options | more } ]

**gprs-service gprs_svc_name**

Specifies the name of a preconfigured GPRS service for which the BSSGP statistics have been collected as an alphanumeric string of 1 through 63 characters that is case sensitive.

**nse nse_ID**

Clears the BSSGP statistics collected for the network service entity (NSE) specified as an integer from 0 through 65535.

**bvc bvc_ID**

Enter this keyword to clear the BSSGP statistics collected for the identified BSSGP virtual connection (BVC) specified as an integer from 0 through 65000.

| { grep grep_options | more }

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter.

Usage
Use this command to clear the BBSGP statistics for a particular GPRS service or NSEI.

Example
The following command deletes the collected BSSGP statistics for the GPRS service named *gprsl*.

```
clear bssgp statistics gprs-service gprsl
```
clear bulkstats

Clears counters and accumulated bulk statistics related information.

Product
All

Privilege
Security Administrator, Administrator, Operator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

clear bulkstats { counters | data }

counters
Clears the counters maintained by the system’s “bulkstats” facility.

data
Clears any accumulated data that has not been transferred. This includes any “completed” files that have not been successfully transferred.

Usage
Once bulk statistics collection is enabled, the system stores the information until the specified transfer criteria is met or until a manual transfer is initiated. The system maintains counters for the “bulkstats” software facility. (Refer to the data keyword for the show bulkstats command for information on viewing the counters.)

This command can be used to delete bulk statistics information that has been collected but not transferred and/or to clear the counters that have been maintained.

Example

The following command clears bulk statistics-related counters:

    clear bulkstats counters
clear cae-group statistics server

This command resets the discardable statistics, which are the Hit Count, Timeout Consecutive (Cumulative), and Last Failure statistics, for all CAEs or for a specific CAE. The CAE (Content Adaptation Engine) is an optional component of the Mobile Videoscape.

Product
MVG

Privilege
Security Administrator, Administrator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

clear cae-group statistics server { all | name cae_name }

Usage

Use this command to reset the discardable statistics for all CAEs or for a specific CAE. This command must be issued in the same context in which the associated CAE group is defined.

Example

The following command clears the discardable statistics for the CAE named server_1:

    clear cae-group statistics server name server_1
clear call-home statistics

Clears Cisco Call Home feature statistics.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local] host_name#
```

**Syntax**

clear call-home statistics

**Usage**

Use this command to reset the statistics for all Call Home events.

**Example**

The following command clears the discardable statistics for the Call Home feature:

```
clear call-home statistics
```
clear cdr statistics

Clears statistics related to charging data records (CDRMOD).

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

clear cdr statistics

Usage
Use this command to reset the statistics for charging data records.

Example
The following command clears the discardable statistics related to CDRs:

  clear cdr statistics
clear cli history

Clears the tracking history of command line interface (CLI) command usage.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

clear cli history

**Usage**
Use this command to clear the tracking history of CLI command usage.

**Example**

The following command clears the CLI history:

```
clear cli history
```
clear cmp cert-name

Clears information stored for the specified IPSec Certificate Management Protocol v2 (CMPv2) certificate.

Product
All products supporting IPSec CMPv2 features

Important: This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

Privilege
Security Administrator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

clear cmp cert-name cert_name

cert-name cert_name

Specifies the CMP certificate name as an alphanumeric string of 1 through 129 characters.

Usage
Use this command to clear the information for the specified CMP certificate.

Example
The following command clears information for the specified CMP certificate:

clear cmp cert-name certificate01
clear cmp statistics


**Product**
All products supporting IPSec CMPv2 features

**Important:** This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

**Privilege**
Security Administrator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
clear cmp statistics
```

**Usage**
Use this command to clear statistics for IPSec CMPv2 certificates.

**Example**

The following command clears CMPv2 certificates:

```
clear cmp statistics
```
clear config

Replaces the active configuration source file with an empty configuration where possible.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

clear config [ -noconfirm ]

    -noconfirm
    Executes the command without any additional prompt and confirmation from the user.

Usage
This command clears the current configuration when a complete overwrite is desired or if it is necessary to start from an empty configuration.

Important: Clearing the configuration will cause the active configuration source file to be empty and of no use in configuring the system to an active state providing service.

Important: This command should only be performed on configurations that have been previously backed up for easy restoration.

Example
The following command clears the active configuration after the user provides confirmation of the request.

clear config

The following command clears the active configuration source file immediately with no user confirmation.

clear config -noconfirm
clear congestion-control statistics

Cleans the congestion control statistics for all instances of the specified manager type.

**Product**
All

**Privilege**
Security Administrator, Administrator, Operator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local] host_name#
```

**Syntax**

```
clear congestion-control statistics { allmgr | asngwmgr | asnpcmgr | bindmux | gtpcmgr | hamgr | hnbmgr | imsimgr | ipsecmgr | ipsmgm | imsimgr | l2tpmgr }
```

- **allmgr**
  Clears the statistics for all A11 Manager instances.

- **asngwmgr**
  Clears the statistics for all ASN GW Manager instances

- **asnpcmgr**
  Clears the statistics for all ASN PC-LR Manager instances

- **bindmux**
  Clears the statistics for all IPCF BindMux-Demux Manager instances.

- **gtpcmgr**
  Clears the statistics for all GTPC Manager instances.

- **hamgr**
  Cleans the statistics for all HA Manager instances.

- **hnbmgr**
  Clears the statistics for all HNB Manager instances.

- **imsimgr**
  Clears the statistics for all IMSI Manager instances.

- **ipsecmgr**
  Clears the statistics for all IPSEC Manager instances.
**Usage**

Use this command to clear statistics for all instances of the specified manager.

**Important:** When this command is issued in any context other than the local context, only instances of the specified manager for the current context have the statistics cleared. When the current context is the local context, all instances of the specified manager type in all contexts have the statistics cleared.

**Example**

Clear the statistics for all instances of the A11 manager, by entering the following command:

```
clear congestion-control statistics allmgr
```
clear content-filtering category statistics

Clears the Category-based Content Filtering application statistics.

**Product**
CF

**Privilege**
Security Administrator, Administrator, Operator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

**Syntax**

```
clear content-filtering category statistics [ facility srdbmgr instance instance_value ]
```

**Usage**

Use this command to clear all Category-based Content Filtering application statistics, or statistics for a specific SRDB Manager instance.

**Example**

The following command clears all Category-based Content Filtering application statistics:

```
clear content-filtering category statistics
```
clear crash

Removes a specific crash file or all crash files.

Product
All

Privilege
Security Administrator, Administrator, Operator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

clear crash [ list | number crash_num ]

list | number crash_num
list: removes all crash files.
number crash_num: removes only the crash file specified as an integer from 1 through 30.

Usage
Clear crashes for general maintenance activities in cleaning out old, unused, or files which are of no importance.

Example
The following will remove all crash files.

    clear crash list

The following command will remove only crash file 27.

    clear crash number 27
clear credit-control statistics

Clears credit control statistics.

Product
All

Privilege
Security Administrator, Administrator, Operator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

```
clear credit-control statistics cc-service cc_service_name
```

**cc-service cc_service_name**

Specifies an existing Credit Control service name as an alphanumeric string of 1 through 63 characters.

Usage

Use this command to clear active credit control statistics.

Example

The following command clears the configured credit control statistics for a service named service1:

```
clear credit-control statistics cc-service service1
```
clear crypto

Clears crypto associations or crypto statistics.

Product
- ePDG
- PDSN
- HA
- GGSN
- PDG/TTG
- PDIF
- SCM

Privilege
Security Administrator, Administrator, Operator

Mode
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

```
clear crypto { isakmp [ tag map_name | peer peer_ip ] | security-association { counters tag map_name [ tx | rx ] | tag map_name | peer peer_ip[ sa-index numbr ] } | statistics { ikev2 | ipsec-3gpp-cscf | srtp } [service-ip-address ip-address | service-name name ] }
```

- **isakmp [ tag map_name | peer peer_ip ]**
  - When no keywords are specified, this command clears all of the ISAKMP security associations for the current context.
  - **tag map_name**: Clears the ISAKMP SAs for the specified crypto map. **map_name** is the name of an existing crypto map.
  - **peer peer_ip**: Deletes the ISAKMP SAs for the specified peer. **peer_ip** must be entered in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

- **security-association { counters tag map_name [ tx | rx ] | tag map_name | peer peer_ip[ sa-index numbr ] }**
  - **counters tag map_name [ tx | rx ]**: Resets the counters for the specified crypto map. **map_name** is the name of an existing crypto map. **tx** specifies that only the transmit SA counters are reset. **rx** specifies that only the receive SA counters are reset. If neither **tx** or **rx** are specified, both transmit and receive SA counters are reset.
  - **tag map_name**: Tears down a Security Association (SA) for the specified crypto map. **map_name** is the name of an existing crypto map.
  - **peer peer_ip**: Clears the SAs for all tunnels who have the peer at the specified IP address. **peer_ip** must be entered in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.
  - **[ sa-index numbr ]**: Clears a specified security association. **numbr** is an integer from 1 to 4 for releases prior to 15.0, or 1 to 5 for release 15.0 and higher.
Caution: Modification(s) to an existing crypto map and/or ISAKMP policy configuration will not take effect until the related security association has been cleared.

```
statistics { ikev2 | ipsec-3gpp-cscf | srtp } [ service-ip-address ip-address | service-name name ]
```

ikev2: Clears global IKEv2 statistics for the current context.
ipsec-3gpp-cscf: Clears global CSCF IPSec statistics for the current context.
srtp: Clears global CSCF SRTP (Secure Real-time Transport Protocol) statistics for the current context.
service-ip-address ip-address: Clears statistics for the specified service-ip address.
service-name name: Clears statistics for the specified service name.

Usage

Clear SAs and apply changes to the crypto map or clear the crypto statistics for this context.

Example

The following clears all IKEv2 crypto statistics for the current context:

```
clear crypto statistics ikev2
```
clear cs-network statistics

Clears the HNB-Circuit Switched (CS) network service associated for an HNB-GW service instance.

**Product**
HNB-GW

**Privilege**
Operator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
clear cs-network statistics [ name cs_svc_name | ranap-only | rtp-only | sccp-only ]
```

- **name cs_svc_name**
  
  Clears the session statistics for an HNB-CS Network service name configured and running on this system. `cs_svc_name` must be an alphanumeric string of 1 through 63 characters.

- **ranap-only**

  Clears the session statistics limited to Radio Access Network Application Protocol (RANAP) traffic only for the specified HNB-CS Network service.

- **rtp-only**

  Clears the session statistics limited to Real Time Protocol (RTP) traffic only for the specified HNB-CS Network service.

- **sccp-only**

  Clears the session statistics limited to Signaling Connection Control Part (SCCP) traffic only for the specified HNB-CS Network service.

**Usage**

Use this command to clear the session statistics for overall session or in selected part of user session for HNB-CS Network services configured and running on a system.

**Example**

The following command clears the session statistics for RANAP part of session for the HNB-CS Network service `hnb_CS_1`:

```
clear cs-network statistics name hnb_CS_1 ranap-only
```
clear cscf service

Resets statistics counters for a specific Call/Session Control Function (CSCF) service, all CSCF services, or for all services within a specified context (VPN).

**Product**

SCM

**Privilege**

Security Administrator, Administrator, Operator

**Mode**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name# 
```

**Syntax**

```
clear cscf service { diameter { location-info | policy-control } statistics [ service-name service_name service_name | vpn-name name ] | li-packet-cable statistics [service-name service_name] | performance-counters name service_name | statistics name service_name { all | atcf | calls | eatf | ip-security | message | npdb | package-name { message-summary | presence | reg | winfo } | registrations | sigcomp | tcp { msrp | sip } | vpn-name name { all | calls | ip-security | message | package-name { message-summary | presence | reg | winfo } | registrations | sigcomp | tcp { msrp | sip } } } } 
```

**diameter { location-info | policy-control } statistics [ service-name service_name ]**

Clears Diameter (DPECA) statistics on the CSCF Rx interface with the configuration information.

**service-name service_name**: Specifies the name of an existing CSCF service for which the statistics will be reset as an alphanumeric string of 1 through 63 characters.

**vpn-name name**: Specifies the name of an existing context in which all statistics for all services will be reset as an alphanumeric string of 1 through 79 characters.

**li-packet-cable statistics [service-name service_name]**

Refer to the *Lawful Intercept Configuration Guide* for a description of this command.

**performance-counters name service_name**

Clears all CSCF performance counters for an existing CSCF service specified as an alphanumeric string of 1 through 63 characters.

**statistics name service_name { all | atcf | calls | eatf | ip-security | message | npdb | package-name { message-summary | presence | reg | winfo } | registrations | sigcomp | tcp { msrp | sip } | vpn-name name { all | calls | ip-security | message | package-name { message-summary | presence | reg | winfo } | registrations | sigcomp | tcp tcp { msrp | sip } } }**

Clears service statistics for an existing CSCF service specified as an alphanumeric string of 1 through 63 characters.

**all**: Clears all CSCF service statistics.
**clear cscf service**

- **atcf**: Clears statistics related to ATCF access transfers.
- **calls**: Clears statistics related to CSCF calls.
- **eatf**: Clears statistics related to emergency access transfers.
- **ip-security**: Clears statistics related to CSCF IPSec.
- **message**: Clears statistics for the SIP method MESSAGE.
- **npdb**: Clears statistics related to NPDB.
- **package-name**: Clears statistics for the associated event package.
  - **message-summary**: Clears statistics for the “message-summary” event package.
  - **presence**: Clears statistics for the “presence” event package.
  - **reg**: Clears statistics for the “reg” event package.
  - **winfo**: Clears statistics for the “watcher-info” event package.
- **registrations**: Clears statistics related to CSCF registrations, reRegistrations, and de-registrations.
- **sigcomp**: Clears statistics related to CSCF sigcomp.
- **tcp**: Displays session statistics related to CSCF TCP.
  - **msrp**: Clears statistics related to CSCF MSRP TCP.
  - **sip**: Clears statistics related to CSCF SIP TCP.
- **vpn-name name**: Clears statistics for a specific CSCF service configured in a specific context on this system. `name` must be an existing context expressed as an alphanumeric string of 1 through 79 characters.

---

**Important**: This keyword must be followed by another statistics-related keyword.

---

**Usage**

Use this command to reset statistics counters for CSCF services. This command will reset the counters in the output of the `show cscf service statistics` command.

---

**Important**: This command will not clear current registered users and current CSCF sessions.

---

**Example**

The following command resets all statistics for a service named `cscf1`:

```
clear cscf service statistics name cscf1 all
```
clear cscf sessions

Clears statistics for Call/Session Control Function (CSCF) sessions on this system.

**Product**
SCM

**Privilege**
Security Administrator, Administrator, Operator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
clear cscf sessions { counters { calls | subscription } service service_name | service service_name { all | aor aor | session-id id } }
```

```
counters { calls | subscription } service service_name
```
Clears counters for all CSCF sessions matching the filter criteria.
- **calls**: Counters associated with calls in CSCF service.
- **subscription**: Counters associated with subscriptions in CSCF service.
- **service service_name**: Counters on specific CSCF service. *service_name* must be an existing CSCF service expressed as an alphanumeric string of 1 through 63 alphanumeric characters.

```
service service_name { all | aor aor | session-id id }
```
Clears session information for all CSCF sessions matching the filter criteria.
- **service service_name**: Session statistics on specific CSCF service. *service_name* must be an existing CSCF service expressed as an alphanumeric string of 1 through 63 alphanumeric characters.
  - • **all**: Specifies that session statistics are to be cleared for all sessions on this service.
  - • **aor aor**: Specifies that session statistics are to be cleared for sessions at this specific AoR. *aor* must be an existing AoR expressed as an alphanumeric string of 1 through 79 characters.
  - • **session-id id**: Specifies that session statistics are to be cleared for sessions with this ID. *id* must be an existing session ID expressed as an alphanumeric string of 1 through 63 characters.

**Usage**
Use this command to clear session information for CSCF sessions.

**Example**
The following command resets all session statistics for a service named cscf1:

```
clear cscf sessions service cscf1 all
```
clear cscf sip

Resets SIP statistics counters for a specific CSCF service, all CSCF services, or for all services within a specified context (VPN) or interface.

Product
SCM

Privilege
Security Administrator, Administrator, Operator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

```
clear cscf sip statistics [ name service_name [ interface { domain name domain_name | ip address ip_address } | vpn-name name ]
```

**name service_name**
Specifies the name of an existing CSCF service for which the SIP statistics will be reset as an alphanumeric string of 1 through 63 characters.

**interface { domain name domain_name | ip address ip_address }**
SIP statistics will be reset in this interface.
domain name domain_name: Specifies an existing domain associated with the CSCF service as an alphanumeric string of 1 through 64 characters.
ip address ip_address: Specifies the destination or source ip address associated with the CSCF service.

**vpn-name name**
Specifies the name of an existing context in which all SIP statistics for all services will be reset as an alphanumeric string of 1 through 79 characters.

Usage
Use this command to reset SIP counters found in the output of the `show cscf sip` command.

Example
The following command resets the SIP statistics for a service named `cscf1`:

```
clear cscf sip statistics name cscf1
```
clear cscf subscription

Clears all subscriptions for a named service or for individual subscribers within the service.

**Product**
SCM

**Privilege**
Security Administrator, Administrator, Operator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local] host_name#
```

**Syntax**

```
clear cscf subscription service service_name { all | from-aor subscriber_aor to-aor resource_aor }
```

- `service service_name`
  Specifies the name of an existing CSCF service for which the subscription(s) will be cleared as an alphanumeric string of 1 through 63 characters.

- `all | from-aor subscriber_aor to-aor resource_aor`
  - `all`: Removes all CSCF subscriptions for the specified service.
  - `from-aor subscriber_aor`: Removes all CSCF subscriptions for a specified subscriber in a specified service.
  - `subscribed-to resource_aor`: Removes all CSCF subscriptions for a specified subscriber in a specified service with a specified subscribed-to resource AoR.

**Usage**

Use this command to clear subscriptions to enforce policies. This command initiates a SUBSCRIBE request with Expires as 0 in the corresponding subscription dialog.

**Example**

The following command clear all subscriptions for a CSCF service named `cscf1`:

```
clear cscf subscription service cscf1 all
```
clear dhcp statistics

Deletes all previously gathered statistics for either a specific or all DHCP IPv4 servers configured within the given context.

Product
GGSN
ASN-GW
P-GW
SAEGW

Privilege
Security Administrator, Administrator, Operator

Mode
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

```
clear dhcp statistics [ dhcp-service svc_name | server ip_address ]
```

**dhcp-service svc_name**
Specifies the name of a specific DHCP service for which to clear statistics as an alphanumeric string of 1 through 63 characters that is case sensitive.

**server ip_address**
Specifies the IP address of a DHCP server in IPv4 dotted-decimal notation as configured in the context for which to clear statistics.

Usage
Statistics for a single server can be cleared using the server keyword. Statistics for all DHCP servers in the context can be deleted by entering the command with no keywords.
This command can be executed from any context configured on the system.
If this command is executed from within the local context with no keywords, statistics will be cleared for every DHCP server configured on the system regardless of context. In addition, if the server keyword is used when executing from within the local context, statistics for all DHCP servers configured with the specified name will be cleared regardless of context.

Example
The following command clears statistics for all configured DHCP servers within the context:

```
clear dhcp statistics
```
clear dhcpv6 statistics

Deletes all previously gathered statistics for either a specific or all DHCP IPv6 (DHCPv6) servers configured within the given context.

**Product**
- GGSN
- ASN-GW
- P-GW
- SAEGW

**Privilege**
- Security Administrator, Administrator, Operator

**Mode**
- Exec

The following prompt is displayed in the Exec mode:

```
[local] host_name#
```

**Syntax**

```
clear dhcpv6 statistics [ server ipv6_address | service svc_name ]
```

**server ipv6_address**

Specifies the IP address of a DHCP server in IPv6 colon-separated-hexadecimal notation as configured in the context for which to clear statistics.

**service svc_name**

Specifies the name of a specific DHCPv6 service for which to clear statistics as an alphanumeric string of 1 through 63 characters that is case sensitive.

**Usage**

Statistics for a single server can be cleared using the `server` keyword. Statistics for all DHCPv6 servers in the context can be deleted by entering the command with no keywords. This command can be executed from any context configured on the system. If this command is executed from within the local context with no keywords, statistics will be cleared for every DHCPv6 server configured on the system regardless of context. In addition, if the server keyword is used when executing from within the local context, statistics for all DHCPv6 servers configured with the specified name will be cleared regardless of context.

**Example**

The following command clears statistics for all configured DHCPv6 servers within the context:

```
clear dhcpv6 statistics
```
clear diameter aaa-statistics

Clears Diameter AAA statistics.

**Product**
All

**Privilege**
Security Administrator, Administrator, Operator

**Mode**
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

**Syntax**

`clear diameter aaa-statistics [ all | [ group aaa_group ] server diameter_server ] [ | { grep grep_options | more } ]`

- **all**
  Clears all Diameter server statistics.

- **group aaa_group**
  Clears Diameter server statistics for the specified AAA group.
  `aaa_group` must be the name of a AAA server group, and must be an alphanumeric string of 1 through 64 characters.

- **server diameter_server**
  Clears Diameter server statistics for the specified Diameter server.
  `diameter_server` must be an alphanumeric string of 1 through 64 characters.

  | { grep grep_options | more } |
  Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
  For details on the usage of `grep` and `more`, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter.

**Usage**
Use this command to clear Diameter AAA statistics.

**Example**
The following command clears Diameter server statistics for the specified AAA group:

`clear diameter aaa-statistics group aaagroup3`
clear diameter route

Clears the Diameter routes in the Diabase.

Product

- ASN GW
- ePDG
- GGSN
- HA
- HSGW
- IPSG
- MME
- PDG/TTG
- PDSN
- P-GW
- SCM
- SGSN
- S-GW

Privilege

- Security Administrator, Administrator, Operator

Mode

- Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

```
clear diameter route dynamic [ endpoint endpoint_name | peer peer_name | facility { aaamgr | sessmgr } [ instance instance_number ] ] [ | { grep grep_options | more } ]
```

dynamic

Clears all dynamic routes under all the Diameter endpoints.

endpoint endpoint_name

Clears the dynamic routes for the specified endpoint.

*endpoint_name* must be the name of a Diameter endpoint, and must be an alphanumeric string of 1 through 63 characters.

peer peer_name

Clears the dynamic routes for the specified peer.

*peer_name* must be an alphanumeric string of 1 through 63 characters.
clear diameter route { aaamgr | sessmgr } [ instance instance_number ]

Clears the dynamic routes for the specified facility – AAA Manager or Session Manager. Specify the instance number to clear the dynamic routes for a particular facility’s instance. The instance_number must be an integer from 1 through 99999.

| { grep grep_options | more } |

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent. For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage

Use this command to clear the Diameter routing tables that gets added in the system whenever messages are routed through the Diameter proxy/Diabase. These message remain in the system for a long period. The user has the flexibility to clear the route based on any combination of these keyword options. Running the command clear diameter route dynamic endpoint endpoint-name peer peer-name will result in flushing of the routes that match both endpoint and peer value. Similarly, with this CLI command "clear diameter route dynamic endpoint endpoint-name peer peer-name facility { aaamgr | sessmgr } instance instance_number, the routes in a particular facility with the specified endpoint and peer name can be deleted.

Example

The following command clears all dynamic Diameter routes for the specified peer:

    clear diameter route dynamic peer p1
exec mode commands

---

clear diameter statistics

Clears Diameter statistics.

Product
All

Privilege
Security Administrator, Administrator, Operator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

```
clear diameter statistics [ [ proxy ] endpoint endpoint_name [ peer-host host_id [ peer-realm realm_id ] ] ] [ | { grep grep_options | more } ]
```

- **endpoint endpoint_name**
  Clears statistics for the specified endpoint.
  - `endpoint_name` must be the name of a diameter endpoint, and must be an alphanumeric string of 1 through 63 characters.

- **proxy**
  Clears proxy related statistics.

- **peer-host host_id**
  Clears statistics for the specified Diameter peer host ID.
  - `host_id` must be an alphanumeric string of 1 through 255 characters.

- **peer-realm realm_id**
  Clears statistics for the specified Diameter peer realm.
  - `realm_id` must be an alphanumeric string of 1 through 127 characters.

- `| { grep grep_options | more }`
  Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
  For details on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage

Use this command to clear Diameter statistics.

Example

The following command clears all Diameter statistics for the specified endpoint:
clear diameter statistics endpoint endpt345
clear diameter-service

Clears information pertaining to configured Diameter services.

**Product**
All

**Privilege**
Security Administrator, Administrator, Operator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local] host_name#
```

**Syntax**

```
clear diameter-service { eap { all | session-id session_id } | lte-s6b { all | session-id session_id } | lte-sta { all | session-id session_id } | lte-s6b { all | session-id session_id } | mbms { bearer-contexts { all | bmsc-bearer-service name service_name } | ue-context { all | bmsc-bearer-service name service_name } } | statistics name service_name [ vpn-name vpn context_name ] }
```

- **eap { all | session-id session_id }**
  Clears subscribers from the EAP interface.
  - **all**: Clears all subscribers.
  - **session-id session_id**: Clears a call for the session ID specified as an alphanumeric string of 1 through 63 characters.

- **lte-s6b { all | session-id session_id }**
  Clears subscribers from the S6b interface.
  - **all**: Clears all subscribers.
  - **session-id session_id**: Clears a call for the session ID specified as an alphanumeric string of 1 through 63 characters.

- **lte-sta { all | session-id session_id }**
  Clears subscribers from STa interface.
  - **all**: Clears all subscribers.
  - **session-id session_id**: Clears a call for the session ID specified as an alphanumeric string of 1 through 63 characters.

- **mbms { bearer-contexts { all | bmsc-bearer-service name service_name } | ue-context { all | bmsc-bearer-service name service_name } }**
  Clears information from the SGSN-APP interface.
  - **bearer-contexts { all | bmsc-bearer-service name service_name }**: Clears information from the bearer-context gmb-interface.
  - **ue-context { all | bmsc-bearer-service name service_name }**: Specifies the name of a bmsc-bearer-service as an alphanumeric string of 1 through 63 characters.
  - **all**: Clears all subscribers.
ue-context { all | bmsc-bearer-service name service_name }: Clear information UE context for gmb-interface.
  all: Clears all subscribers.
  bmsc-bearer-service name service_name: Specifies the name of a bmsc-bearer-service as an alphanumeric string of 1 through 63 characters.

  service_name
  service_name must be a name of a Diameter service expressed as an alphanumeric string of 1 through 63 characters.

statistics name service_name [ vpn-name vpn context_name ]
Clears the Diameter service associated with the specified statistics.
  name service_name: Specifies the name of a Diameter service as an alphanumeric string of 1 through 63 characters.
  vpn-name vpn context_name: Clears statistics for the vpn-context name specified as an alphanumeric string of 1 through 63 characters.

Usage
Use this command to clear information pertaining to configured Diameter services.

Example
The following command clears Diameter service information for all subscribers associated with EAP interface:

  clear diameter-service eap all
clear dns-client

Clears DNS cache and/or statistics for a specified DNS client.

Product
SCM

Privilege
Security Administrator, Administrator, Operator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local] host_name#

Syntax

clear dns-client name { cache [ query-name name | query-type { A | AAAA | NAPTR | SRV } ] | statistics }

dns-client name

Specifies the name of an existing DNS client whose cache and/or statistics are being cleared as an alphanumeric string of 1 through 255 characters.

cache [ query-name name | query-type { A | AAAA | NAPTR | SRV } ]

Specifies that the cache for the defined DNS client is to be cleared.

query-name name: Filters DNS results based on the domain name. The name is an alphanumeric string of 1 through 255 characters. that is the domain name used to perform the DNS query. This name is different from the actual domain name which is resolved. For example, to resolve the SIP server for service.com, the query name is _sip._udp.service.com and the query type is SRV.

query-type:
  • A: Filters DNS results based on domain IP address records (A records).
  • AAAA: Filters DNS results based on AAAA records (AAAA resource records).
  • NAPTR: Filters DNS results based on Name Authority Pointer records.
  • SRV: Filters DNS results based on service host records (SRV records).

statistics

Specifies that statistics for the defined DNS client are to be cleared.

Usage
Use this command to clear DNS cache and/or statistics for a specified DNS client.

Example
The following command clears statistics for a DNS client named domain1.com:

clear dns-client domain1.com statistics
clear dns-proxy statistics

Clears all DNS proxy statistics.

**Product**
SCM

**Privilege**
Security Administrator, Administrator, Operator

**Mode**
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

**Syntax**

```
 clear dns-proxy statistics
```

**Usage**
Use this command to clear all DNS proxy statistics.

**Example**
The following command clears DNS proxy statistics:

```
 clear dns-proxy statistics
```
clear dynamic-policy statistics

Clears policy control and charging (PCC) statistics from the interface communicating with the Policy and Charging Rules Function (PCRF) via Gx(x).

**Product**
- HSGW
- PDSN
- SAEGW
- S-GW

**Privilege**
- Inspector

**Mode**
- Exec

The following prompt is displayed in the Exec mode:

```
[local] host_name#
```

**Syntax**

```
clear dynamic-policy statistics { hsgw-service name | pdsn-service name | sgw-service name }
```

- **hsgw-service name**
  
  Clears policy control and charging statistics from the Gxa interface communicating with the PCRF. `name` must be an existing HSGW service name and be from 1 to 63 alphanumeric characters.

- **pdsn-service name**
  
  Clears policy control and charging statistics from the Gx interface communicating with the PCRF. `name` must be an existing PDSN service name and be from 1 to 63 alphanumeric characters.

- **sgw-service name**
  
  Clears policy control and charging statistics from the Gxc interface communicating with the PCRF. `name` must be an existing S-GW service name and be from 1 to 63 alphanumeric characters.

**Usage**

Use this command to clear PCC statistics for the specified service and its Gx interface communicating with the PCRF.

**Example**

The following command clears HSGW statistics for an HSGW service named `hsgw4`:

```
clear dynamic-policy statistics hsgw-service hsgw4
```

The following command clears PCC statistics for a PDSN service named `cdma4`:

```
clear dynamic-policy statistics pdsn-service cdma4
```
The following command clears S-GW statistics for an S-GW service named \textit{sgw4}:

\texttt{clear dynamic-policy statistics sgw-service sgw4}
clear egtpc

Clears enhanced GPRS Tunneling Protocol control plane (eGTP-C) statistics and counters found in show command outputs and bulk statistics associated with all eGTP-C-related services or those defined by the parameters in this command.

Product
MME
P-GW
S-GW
SAEGW

Privilege
Operator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

```
clear egtpc statistics [ egtp-service name | interface-type { interface-mme | interface-pgw-ingress | interface-sgsn | interface-sgw-egress | interface-sgw-ingress } | mme-address ip_address | pgw-address ip_address | sgsn-address ip_address | sgw-address ip_address ]
```

**egtp-service name**
Clears all statistics and counters associated with an existing eGTP service name specified as an alphanumeric string of 1 through 63 characters.

**interface-type { interface-mme | interface-pgw-ingress | interface-sgw-egress | interface-sgw-ingress }**

**interface-mme**: Clears statistics and counters derived from all MME interface types associated with this system.

**interface-pgw-ingress**: Clears statistics and counters derived from all P-GW ingress interface types associated with this system.

**interface-sgw-egress**: Clears statistics and counters derived from all S-GW egress interface types associated with this system.

**interface-sgsn**: Clears statistics and counters derived from all SGSN S4 interface types associated with this system.

**interface-sgw-ingress**: Clears statistics and counters derived from all S-GW ingress interface types associated with this system.

**mme-address ip_address**
Clears all statistics and counters derived from an existing MME IP address specified in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.
**pgw-address ip_address**
Clears all statistics and counters derived from an existing P-GW IP address specified in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

**sgw-address ip_address**
Clears all statistics and counters derived from an existing S-GW IP address specified in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

**sgsn-address ip_address**
Clears all statistics and counters derived from an existing SGSN S4 IP address specified in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

**Usage**
Use this command to clear running statistics and counters found in show command and bulk statistics outputs for all eGTP-C-related services or for specific interfaces, services, or IP addresses as specified by parameters in this command.

**Example**
The following command clears eGTP-C statistics and counter associated with all P-GW ingress interfaces configured on this system:

```
clear egtpc statistics interface-type interface-pgw-ingress
```

The following command clears eGTP-C statistics and counter associated with all MME interfaces configured on this system:

```
clear egtpc statistics interface-type interface-mme
```
clear event-notif statistics

Clears the statistical information collected over a configured Event Notification (SNMP) interface based on specific criteria.

**Product**
All

**Privilege**
Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local] host_name#
```

**Syntax**

```
clear event-notif statistics
```

**Usage**

Use this command to clear the statistical information collected over configured Event Notification interface based on specific criteria.

**Example**

The following command clears the counter information for all Event Notification collection servers configured in a context:

```
clear event-notif server all
```
clear firewall

This command is obsolete.
clear fng-service statistics

Deletes all previously gathered statistics for a specific Femto Network Gateway (FNG) service or all FNG services configured within a context.

**Product**
FNG

**Privilege**
Security Administrator, Administrator, Operator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
clear fng-service statistics {name service_name}
```

**name service_name**

Specifies the name of a specific FNG service configured in the context for which to clear statistics as an alphanumeric string of 1 through 63 characters that is case sensitive.

**Usage**

Statistics for a single FNG service can be cleared using the **name** keyword. Statistics for all FNG services in the context can be deleted by entering the command with no keywords.

If this command is executed from within the local context with no keywords, statistics will be cleared for every FNG service configured on the system regardless of context. In addition, if the **name** keyword is used when executing from within the local context, statistics for all FNG services configured with the specified name will be cleared regardless of context.

**Example**

The following command clears statistics for an FNG service named fng1:

```
clear fng-service statistics name fng1
```
clear gmb statistics

Deletes the collected statistics for the Gmb reference point. Gmb handles broadcast multicast service center (BM-SC) related signaling, which includes the user specific and bearer service messages for Multimedia Broadcast/Multicast Service (MBMS) service.

Product
GGSN

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

```
clear gmb statistics [ apn name | bmsc-profile profile_name ]
```

**apn name**
Deletes only the Gmb information for the specified Access Point Name (APN) specified as an alphanumeric string of 1 through 62 characters.

**bmsc-profile profile_name**
Deletes only the Gmb information for the specified BM-SC profile specified as an alphanumeric string of 1 through 79 characters.

Usage
Use this command to delete usage statistics for the Gmb reference point.

Example
The following command deletes all Gmb statistics:

```
clear gmb statistics
```
clear gmm-sm statistics

Deletes the collected statistics for the GPRS Mobility Management and Session Management (GMM/SM) configurations for various SGSN services.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```bash
clear gmm-sm statistics [ gmm-only | gprs-service service_name | iups-service service_name | plmn-id mcc mcc mcc | sgsn-service service_name | sm-only ]
```

**gmm-only**

Deletes only GPRS mobility management (GMM) information for the specified filter. Filter options include:

- `gprs-service service_name`
- `iups-service service_name`
- `plmn-id`
- `sgsn-service service_name`

**gprs-service srvc_name**

Deletes the statistics for a 2.5G GPRS service specified as an alphanumeric string of 1 through 63 characters that uniquely identifies a preconfigured GPRS service. The delete request can be narrowed by adding either the `nsei` or `routing-area` keywords.

**iups-service srvc_name**

Deletes the statistics for a IuPS service specified as an alphanumeric string of 1 through 63 characters that uniquely identifies a preconfigured IuPS service. The delete request can be narrowed by adding either the `rnc` or `routing-area` keywords.

**plmn-id mcc mcc mcc | access-type { gprs | umts }**

Deletes the statistics for services within a specified PLMN.

- `mcc` Specifies the mobile country code (MCC) as part of the identification of the RNC or RA. `mcc_id` must be an integer from 100 to 999.
- `mnc` Specifies the mobile network code (MNC) as part of the identification of the RNC or RA. `mnc_id` must be a 2- or 3-digit integer from 00 to 999.

**access-type** keyword fine-tunes the delete procedure and only deletes GMM/SM statistics for the IuPS (access-type UMTS) and/or the GPRS (access-type GPRS) services belonging to the PLMN.
**sgsn-service srvc_name**
Deletes the statistics for a 3G SGSN service specified as an alphanumeric string of 1 to 63 characters that uniquely identifies the SGSN service. The delete request can be narrowed by adding either the **rnc** or **routing-area** keywords.

**sm-only**
Deletes only session management (SM) information for the specified keyword parameters.

**mcc**

**mcc**  Specifies the mobile country code (MCC) as part of the identification of the RNC or RA. **mcc_id** must be an integer from 100 to 999.

**mnc**

**mnc**  Specifies the mobile network code (MNC) as part of the identification of the RNC or RA. **mnc_id** must be a 2- or 3-digit integer from 00 to 999.

**lac lac_id**
Specifies the location area code (LAC) as part of the identification of the RNC or RA. **lac_id** must be an integer from 1 to 65535.

**nsei nsei_id**
Deletes the GMM/SM session statistics for the identified network service entity (NSEI). **nsei_id** must be an integer from 0 to 65535 that uniquely identifies a configured NSEI.

**rnc rnc_id**
Fine-tunes the deletion of GMM/SM session statistics just for the specified radio network controller (RNC). **rnc_id** must be an integer from 0 to 4095.

**rac rac_id**
Specifies the routing area code (RAC) as part of the identification of the RNC or RA. **rac_id** must be an integer from 1 to 255.

**routing-area mcc mcc_id mnc mnc_id lac lac_id rac rac_id**
Enter the **routing-area** keyword to fine-tune the clearing of the GMM/SM statistics for a specified routing area (RA) identified by the MCC, MNC, LAC and RAC.

**Usage**
Use this command to delete usage statistics for the GMM/SM session configurations for SGSN services, including BSC attaches, activations, and throughput.

**Example**
The following command deletes GMM/SM statistics for a specific routing area defined for the SGSN’s GPRS service:
```
clear gmm-sm statistics gprs-service gprsl routing-area mcc 123 mcc 131 lac 24 rac 11
```
The following command displays all possible information for GMM/SM statistics:

```
show gmm-sm statistics verbose
```

**Important:** Output descriptions for `show` commands are available in the *Statistics and Counters Reference*. 
clear gprsns statistics

Deletes collected statistics for the 2.5G SGSN’s General Packet Radio Service (GPRS) Network Service (NS) layer (link level).

Product
SGSN

Privilege
Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

```
clear gprsns statistics { msg-stats nse nse_id | sns-msg-stats }[ | { grep grep_options | more } ]
```

- **msg-stats**
  Deletes collected transmit (tx) and receive (rx) message statistics for the NS layer.

- **consolidated nse nse_id**
  
  `nse_id`: Enter an integer from 0 to 65535.

- **nse nse_id**
  Deletes statistics for an NSE specified as an integer from 0 to 65535.

- **sns-msg-stats**
  Deletes subnetwork service (SNS) sublayer message statistics.

  `| { grep grep_options | more }`

  You must specify a command to which the output of this command will be sent.

  For details on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage

This command is used to display Frame Relay statistics configured for the NSE/NSVC with the commands documented in the Network Service Entity - Peer NSEI Configuration Mode chapter.

Collected statistics are cleared (deleted) with the clear gprsns statistics described in the Exec Mode Commands (A-C) chapter.

Example

The following command displays the collected message statistics for NSEI 1422:

```
show gprsns statistics msg-stats nse 1422
```
Important: Output descriptions for `show` commands are available in the *Statistics and Counters Reference*. 
clear gprsssf statistics

Deletes all Customized Applications for Mobile networks Enhanced Logic (CAMEL) service gprsSSF (GPRS Service Switching Function) statistics collected since the last reset or clear command.

Product
SGSN

Privilege
Security Administrator, Administrator, Operator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

```
clear gprsssf statistics [ camel-service srvc_name | gprs [ 2g-sgsn-app | 3g-sgsn-app ] | gmscfc-address { address | all } | sms ] [ | { grep | more } ]
```

**camel-service srvc_name**
Clears only CAMEL service statistics for the configured CAMEL service specified as an alphanumeric string of 1 through 63 characters.

**gprs [ 2g-sgsn-app | 3g-sgsn-app ]**
Clears only CAMEL service statistics for either a 2.5G or 3G SGSN.

**gmscfc-address { address | all }**
Filters the command to only clear CAMEL service statistics for specified GSM service control function (gsmSCF) addresses. *address* is a standard ISDN E.164 address of 1 to 15 digits.

**sms**
Filters the command to only clear CAMEL service statistics for SMS protocol information.

| { grep grep_options | more } |

For details on the usage of grep and more, refer to the *Regulating a Command’s Output* section of the Command Line Interface Overview chapter.

**Usage**

This command instructs the SGSN to delete collected CAMEL service statistics for either specified CAMEL services, or for SMS or GPRS applications in all contexts.

**Example**

The following command will delete gprsSSF statistics collected for the CAMEL service residing at SCP identified by the gsmSCF address:

```
clear gprsssf statistics gmscfc-address 412211411151
```
clear gtpc statistics

Deletes all previously gathered GTPC (GTPv0, GTPv1-C, GTPv1-U) statistics within the given context based on the specified criteria.

Product
GGSN

Privilege
Security Administrator, Administrator, Operator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

clear gtpc statistics [ [ custom1 | gtpc-mgr-instance gtpc_mgr_instance_number | smgr-instance sessmgr_instance_number ] [ apn apn_name | ggsn-service ggsn_service_name | mseg-service mseg_service_name | gsn-address gsn_ipv4_address ] ]

custom1
Clears the statistics of GTP-C messages for preservation mode and free of charge service. This keyword is a customer-specific function used for Preservation-Mode and Free-of-Charge Service that is enabled under customer-specific license. For more information on this support, contact your Cisco account representative.

gtpc-mgr-instance gtpc_mgr_instance_number
Clears GTP-C statistics for a GTPC Manager instance specified as an integer from 1 through 4294967295.

smgr-instance sessmgr_instance_number
Clears GTP-C statistics for a Session Manager instance specified as an integer from 1 through 4294967295.

apn apn_name
Clears GTP-C statistics for an existing APN specified as an alphanumeric string of 1 through 63 characters that is case sensitive.

ggsn-service ggsn_service_name
Clears GTP-C statistics for an existing GGSN service specified as an alphanumeric string of 1 through 63 characters that is case sensitive.

mseg-service mseg_service_name

Important: This keyword is not supported in this release.
clear gtpc statistics

sgsn-address sgsn_ipv4_address
Clears GTP-C statistics for an existing SGSN specified by IP address in IPv4 dotted-decimal notation.

Usage
GTPC statistics can be cleared for a single APN, GGSN service, or SGSN. All GTPC statistics in the context can be deleted by entering the command with no keywords.
This command can be executed from any context configured on the system.
If this command is executed from within the local context with no keywords, all GTPC statistics will be cleared regardless of context.
GTPP statistics are not affected by this command.

Example
The following command clears all GTPC statistics context:

clear gtpc statistics
clear gtpp statistics

Deletes all previously gathered GTPP statistics within the given context based for either single or all charging gateway functions (CGFs).

Product
GGSN

Privilege
Security Administrator, Administrator, Operator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

clear gtpp statistics [ cgf-address ip-address ]

cgf-address cgf_address

Deletes statistics for a CGF identified by its IP address entered in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

Usage
Statistics for a single CGF can be cleared using the cgf-address keyword. Statistics for all CGFs in the context can be deleted by entering the command with no keywords.
This command can be executed from any context configured on the system.
If this command is executed from within the local context with no keywords, statistics will be cleared for every CGF configured on the system regardless of context. In addition, if the cgf-address keyword is used when executing from within the local context, statistics for all CGFs configured with the specified name will be cleared regardless of context.

Example
The following command deletes all GTPP statistics for a CGF with an IP address of 192.168.1.42:

    clear gtpp statistics cgf-address 192.168.1.42
clear gtpp storage-server local file statistics

Clears AAA proxy GTTP group level statistics for CDRs stored on the local hard disk.

**Product**
GGSN
SGSN

**Privilege**
Security Administrator, Administrator, Operator

**Mode**
Exec
The following prompt is displayed in the Exec mode:

```
[local]host_name#
```  

**Syntax**

```
clear gtpp storage-server local file statistics [ group name name ]
```  

**Usage**
If executed from the local context, this command clears statistics for all GTTP groups configured on the system. If executed from the context within which the storage servers (hard disk) is configured, statistics are deleted for only that context.
clear gtpp storage-server statistics

Clears statistics for configured GTTP storage servers (GSS).

Product
GGSN

Privilege
Security Administrator, Administrator, Operator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

clear gtpp storage-server statistics

Usage

If executed from the local context, this command clears statistics for all GTTP storage servers configured on the system. If executed from the context within which the servers are configured, statistics are deleted for only those servers.
clear gtpu statistics

Clears enhanced GPRS Tunneling Protocol user plane statistics and counters found in `show` command outputs and bulk statistics associated with all GTP-U-related services or those defined by the parameters in this command.

**Product**
- P-GW
- S-GW
- MME
- SAEGW

**Privilege**
- Operator

**Mode**
- Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
clear gtpu statistics [ gtpu-service gtpu_service_name | mseg-service mseg_service_name | peer-address ipv4/ipv6_address ]
```

**Important:** This keyword is not supported in this release.

```
gtpu-service gtpu_service_name
```

Clears GTP-U statistics for an existing GTP-U service specified as an alphanumeric string of 1 through 63 characters.

```
mseg-service mseg_service_name
```

```
peer-address ipv4/ipv6_address
```

Clears GTP-U statistics for an existing peer IP address entered in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

**Usage**

Use this command to clear running statistics and counters found in show command and bulk statistics outputs for all GTP-U-related services or for specific services or IP addresses as specified by parameters in this command.

**Example**

The following command clears GTP-U statistics and counter associated with a GTP-U service name `gtpu-12` configured on this system:

```
clear gtpu statistics gtpu-service gtpu-12
```
clear hd-storage-policy

Clears statistic information for HD storage policies configured on the system.

**Product**

HSGW
P-GW
S-GW
SAEGW

**Privilege**

Operator

**Mode**

Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

**Syntax**

```
clear hd-storage-policy statistics { all | name name }
```

- `all`: Clears ACR statistical information for all HD storage policies configured on the system.
- `name name`: Clears ACR statistical information for an existing HD storage policy specified as an alphanumeric string of 0 through 63 characters.

**Usage**

Use this command to clear statistics for HD storage policies configured on the system.

**Example**

The following command clears statistics for an HD storage policy named pgwsgw:

```
clear hd-storage-policy statistics name pgwsgw
```
clear henbgw-access-service statistics

Clears HENBGW ACCESS service statistics.

Product
HeNB-GW

Privilege
Operator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

clear henbgw-access-service statistics [ henbgw-access-service henbgw_acc_svc_name | miscellaneous | peer-id peer_id_value | slap | sctp ] [ | { grep grep_options | more } ]

henbgw-access-service  henbgw_acc_svc_name

Clear statistics per specified HENBGW ACCESS service.

henbgw_acc_svc_name is a string of size 1 to 63.

miscellaneous

Clears Miscellaneous statistics.

peer-id

Clears information about HENB associations for the specified peer.

peer_id_value is an integer value ranging from 0 to 4294967295.

slap

Clears S1AP statistics.

sctp

Clears SCTP statistics.

| { grep grep_options | more }

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage

Use this command to clear HENBGW ACCESS service statistics

Example
The following command clears S1AP statistics:

```
clear henbgw-access-service statistics slap
```
clear henbgw-network-service statistics

Clears HENBGW NETWORK service statistics.

**Product**
HeNB-GW

**Privilege**
Operator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
clear henbgw-network-service statistics [ henbgw-network-service henbgw_net_svc_name | peer-id peer_id_value | slap | sctp ] [ | { grep grep_options | more }]
```

- **henbgw-network-service henbgw_net_svc_name**
  Clear statistics per specified HENBGW NETWORK service.
  *henbgw_net_svc_name* is a string of size 1 to 63.

- **peer-id**
  Clears information about MME associations for the specified peer.
  *peer_id_value* is an integer value ranging from 0 to 4294967295.

- **slap**
  Clears S1AP statistics.

- **sctp**
  Clears SCTP statistics.

```
| { grep grep_options | more }
```

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of *grep* and *more*, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage**
Use this command to clear HENBGW NETWORK service statistics

**Example**
The following command clears S1AP statistics:

```
clear henbgw-network-service statistics slap
```
clear hnbgw sessions

Clears the active/dormant session information about registered Nabs) on Home-NodeB Gateway (HNB-GW) service instances configured and running on this system based on different filter criteria.

Product
HNB-GW

Privilege
Operator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local] host_name#

Syntax

```
clear hnbgw sessions { all | cell-id cell_id | hnb-address hnb_ip_address | hnb-local-id hnb_id | hnbgw-service hnbgw_svc_name | hnbid hnb_glbl_id | mcc mcc mnc mnc [ -noconfirm ] [ lac lac | rac rac ] }
```

**all**
Clears the summarized or full information for all registered HNB sessions on an HNB-GW service instance running on system. Clearing the statistics can be filtered based on given filtering.

**cell-id cell_id**
Clears HNB session statistics for a registered cell ID on an HNB-GW service instance. cell_id is the identification number of the Femto cell where the user/subscriber is geographically located expressed as an integer from 0 through 268435455.

**hnb-address hnb_ip_address**
Clears the session statistics for HNB session(s) based on a registered HNB IP address entered in IPv4 dotted-decimal notation.

**hnb-local-id hnb_id**
Clears the session statistics of HNB session(s) for a registered local id of HNB specified as as an integer from 1 through 255.

**hnbgw-service hnbgw_svc_name**
Clears the session statistics for registered HNB session(s) on an existing HNB-GW service name specified as an alphanumeric string of 1 through 63 characters.

**hnbid hnb_glbl_id**
Clears the statistics for HNB session(s) based on the registered HNB global id specified as an integer from 1 through 255.
**mcc**

Clears statistics for HNB session(s) based on the registered Mobile Country Code (MCC) identification number of the UE. **mcc** must be an integer from 101 through 999.

**mnc**

Clears the statistics for HNB session(s) based on the registered Mobile Network Code (MNC) identification number of the UE. **mnc** must be a 2- or 3-digit integer from 00 through 999.

**lac**

Clears the statistics for HNB session(s) based on the registered Location Area Code (LAC) identification number of the UE. **lac** must be an integer from 1 through 65535.

**rac**

Clears the statistics for HNB session(s) based on the registered Radio Access Code (RAC) identification number of the UE. **rac** must be an integer from 1 through 255.

**rnc**

Clears the statistics for HNB session(s) based on the registered Radio Network Code (RNC) identification number of the HNB. **rnc** must be an integer from 1 through 65535.

**-noconfirm**

Executes the command without any additional prompt and confirmation from the user.

**Important:** The Operator privilege does not have access to this keyword.

**Usage**

Use this command to clear the session statistics of all or specific registered HNB session(s) or in selected part of user session for HNB-GW services configured and running on this system.

**Example**

The following command clears the session statistics for all registered HNBs on the HNB-GW service named **hnbgw1**:

```
clear hnbgw sessions hnbgw-service hnbgw1
```
clear hnbgw statistics

Clears the HNB-GW service and HNB related statistics from an HNB-GW node.

Product
HNB-GW

Privilege
Operator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local] host_name#

Syntax

clear hnbgw statistics [ gtpu-only ] [ hnb-access-mode { closed | hybrid | open } ] [ hnbap-only ] [ hnbgw-service hnbgw_svc_name [ gtpu-only | hnb-access-mode { closed | hybrid | open } | hnbap-only | ipne-only | ranap-only | rtp-only | rua-only | sabp-only | sctp-only ] ] [ hnbid hnb_identifier ] [ hnbap-only | ranap-only | rtp-only | rua-only ] ]

---

gtpu-only
Clears the statistics for GTP-U traffic only for the selected HNB/HNB-GW service.

---

hnb-access-mode { closed | hybrid | open }
Clears the session statistics of an existing HNB-GW service based on access mode filters.

- **closed**: clears the statistics of only those UEs which are connected through Closed HNBs to the HNB-GW services on a chassis. This command applies to all Closed HNB sessions on a chassis. If any other criteria specified it will filter the statistics based on given criteria.

- **hybrid**: clears the statistics of only those UEs which are connected through Hybrid HNBs to the HNB-GW services on a chassis. This command applies to all Hybrid HNB sessions on a chassis. If any other criteria specified it will filter the statistics based on given criteria.

- **open**: clears the statistics of only those UEs which are connected through Open HNBs to the HNB-GW services on a chassis. This command applies to all Open HNB sessions on a chassis. If any other criteria specified it will filter the statistics based on given criteria.

---

hnbap-only
Clears the statistics for Home NodeB Application Part (HNBAP) traffic only for the selected HNB/HNB-GW service.

---

hnbgw-service hnbgw_svc_name
Clears the session statistics for an existing HNB-GW service name specified as an alphanumeric string of 1 through 63 characters.
**clear hnbgw statistics**

- **hnbid hnb_identifier**
  Clears the session statistics for an existing Home-NodeB identifier specified as an alphanumerical string of 1 through 255 characters.

- **ranap-only**
  Clears the session statistics for Radio Access Network Application Protocol (RANAP) traffic only for the selected HNB/HNB-GW service.

- **rtp-only**
  Clears the session statistics for Real Time Protocol (RTP) traffic only for the selected HNB/HNB-GW service.

- **rua-only**
  Clears the session statistics for RANAP User Adaptation (RUA) traffic only for the selected HNB/HNB-GW service.

- **sabp-only**
  Clears the session statistics for Signaling Connection Control Part (SCCP) traffic only for the selected HNB-GW service.

- **sctp-only**
  Filters the session statistics to display only Stream Control Transmission Protocol (SCTP) traffic for the selected HNB-GW service.

**Usage**

Use this command to clear the session statistics for an overall session or in a selected part of a user session for HNB-GW services and/or HNBs configured and running on this system.

**Example**

The following command clears the session statistics for the HNBAP portion of session details for the HNB-GW service named *hnbgw1*:

```plaintext
clear hnbgw statistics hnbgw-service hnbgw1 hnbap-only
```

The following command clears the session statistics for the RANAP portion of session details for the HNB identified as *102*:

```plaintext
clear hnbgw statistics hnbid 102 ranap-only
```
clear hsgw-service

Clears HRPD Serving Gateway (HSGW) statistics and counters found in show command outputs and bulk statistics associated with all HSGW services or a specific service defined by the parameter in this command.

**Product**
HSGW

**Privilege**
Operator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
clear hsgw-service statistics [ dns-stats | name service_name [ dns-stats ] ] [ | { grep grep_options | more } ]
```

<table>
<thead>
<tr>
<th>dns-stats</th>
<th>Clears DNS-related statistics.</th>
</tr>
</thead>
<tbody>
<tr>
<td>name name</td>
<td>Clears statistics and counters for an existing HSGW service name specified as an alphanumeric string of 1 through 63 characters.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>grep grep_options</th>
<th>more</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent. For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.</td>
<td></td>
</tr>
</tbody>
</table>

**Usage**
Use this command to clear statistics for HSGW services configured on the system.

**Example**
The following command clears statistics for an HSGW service named hsgw3:

```
clear hsgw-service statistics name hsgw3
```
clear hss-peer-service

Clears statistic information for Home Subscriber Service (HSS) peer services configured on the system.

**Product**
MME

**Privilege**
Operator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
clear hss-peer-service statistics [ service name ]
```

- `statistics [ service name ]`
  - **statistics**: Clears HSS peer service statistical information for all HSS peer services configured on the system.
  - **service name**: Clears HSS peer service statistic information for an existing HSS peer service specified as an alphanumeric string of 1 through 64 characters.

**Usage**

Use this command to clear statistics for HSS peer services configured on the system.

**Example**

The following command clears statistics for an HSS peer service named `hss4`:

```
clear hss-peer-servicey statistics service name hss4
```
clear ims-authorization

Clears statistics for all or for a specified IP Multimedia System (IMS) Authorization Service.

**Product**
- GGSN
- SCM

**Privilege**
- Security Administrator, Administrator, Operator

**Mode**
- Exec

The following prompt is displayed in the Exec mode:

[local]\host_name#

**Syntax**

```
clear ims-authorization { policy-control statistics [ ims-auth-service service_name ] | service statistics [ name service_name ] } [ | { grep grep_options | more } ]
```

---

**ims-auth-service service_name**
Clears statistics for the specified IMSA service.
*service_name* must be an alphanumeric string of 1 through 64 characters.

---

**grep grep_options | more**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of *grep* and *more*, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter.

---

**Usage**

Use this command to clear IMSA Service statistics.

**Example**

The following command clears IMSA policy-control statistics for an IMSA service named *test_service*:

```
clear ims-authorization policy-control statistics ims-auth-service test_service
```
clear ims-sh-service statistics

Clears all IP Multimedia System (IMS) Sh interface (Diameter) statistics for a specific or all services using the Sh interface.

Product       PDIF
Privilege      Security Administrator, Administrator
Mode           Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

`clear ims-sh-service statistics [ service service_name ]`

**service service_name**

Clears statistics for the specified existing IMS service.

*service_name* must be an alphanumerical string of 1 through 64 characters.

Usage

Use this command to clear interface Sh interface statistics for a specified or all IMS services.

Example

The following command clears all Sh interface statistics:

```
clear ims-sh-service statistics
```
clear ip access-group statistics

Clears all interface access control list (ACL) statistics and the context level ACL statistics that have been configured in the current context. Be aware that updating an access list also causes all ip access-groups utilizing the list to be cleared.

Product
PDSN
GGSN
ASN-GW

Privilege
Security Administrator, Administrator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

clear ip access-group statistics

Usage
Use this command to clear all interface ACL statistics and the context level ACL statistics that have been configured in the current context.

Example

The following command clears the ACL statistics:

    clear ip access-group statistics
clear ip arp

Clears the address resolution protocol (ARP) cache for a given IP address.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
clear ip arp ip_address
```

*ip_address*

Specifies the IP address for which to clear the ARP cache in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

**Usage**

Clear the ARP cache when network changes have occurred for the case where the cached data may cause undue overhead in routing packets.

**Example**

The following command clears the ARP cache for the IP address 10.2.3.4:

```
clear ip arp 10.2.3.4
```
clear ip bgp peer

Resets Border Gateway Protocol (BGP) connections for all peers or for specified peers in the current context.

**Product**
HA

**Privilege**
Security Administrator, Administrator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
clear ip bgp peer { ip_address | all | as as_num } [ in | out | soft | vpnv4 | vpn6 | vrf vrf_name ] [ in | out | soft ]
```

- **ip_address**
  Specifies the IP address of the neighbor for which BGP connections should be reset in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

- **all**
  Resets BGP connections for all peers.

- **as as_num**
  Resets BGP connections for all peers in the specified autonomous system (AS). `as_num` must be an integer from 1 through 65535.

- **in**
  Softly reconfigures inbound updates.

- **out**
  Softly reconfigures outbound updates.

- **soft**
  Softly reconfigures inbound and outbound updates.

- **vpnv4**
  Clears BGP sessions within the VPNv4 address family.

- **vpnv6**
  Clears BGP sessions within the VPNv6 address family.
**clear ip bgp peer**

**vrf vrf_name**

Cleans BGP sessions within the specified VRF. `vrf_name` is an alphanumeric string of 1 through 63 characters.

**Usage**

Use this command to BGP information for the current context.

**Example**

The following command resets BGP connections for all neighbors:

```
clear ip bgp peer all
```
clear ip localhosts

Removes the host specified from the current context’s local host list for IP address mappings.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
clear ip localhosts [ host_name ]
```

**host_name**
Specifies the name of the host to be removed as an alphanumeric string of 1 through 127 characters. When omitted, all local host name mappings will be removed.

**Usage**
Clears a host name when it is no longer valid for the current context to access. The host name specified will be unrecognized by the current context once the command is performed.

**Example**

```
clear ip localhosts

clear ip localhosts 10.2.3.4

clear ip localhosts remoteABC
```
clear ip ospf process

Clears Open Shortest Path First (OSPF) database information for the current context and re-establishes neighbor adjacency.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

clear ip ospf process

Usage
Use this command to clear the OSPF database information for the current context and re-establishes neighbor adjacency.

Example
The following command clears the OSPF database information for the current context and re-establishes neighbor adjacency:

   clear ip ospf process
clear ipne statistics

Clears IP Network Enabler (IPNE) statistics for a specified or all IPNE services.

**Product**
MINE

**Privilege**
Administrator, Security Administrator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local] host_name#
```

**Syntax**

```
clear ipne statistics [ service service_name ]
```

**Usage**

Clears IPNE statistics for a specified or all IPNE services.

**Example**

The following example clears all IPNE statistics:

```
clear ipne statistics
```
clear ipsg statistics

Cleans IP Services Gateway (IPSG) statistics for a specified or all IPSG services.

**Product**
eWAG
IPSG

**Privilege**
Administrator, Security Administrator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
clear ipsg statistics [ service service_name ]
```

- **service service_name**
  Specifies the name of an IPSG service for which statistics will be cleared.
  *service_name* must be an alphanumeric string of 1 through 64 characters.

**Usage**
Cleans IPSG service statistics for a specified or all IPSG services.

**Example**
The following command clears statistics for all IPSG services:

```
clear ipsg statistics
```
clear ipv6 neighbors

Clears an IPv6 address from the neighbor cache.

**Product**
PDIF

**Privilege**
Administrator, Security Administrator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
clear ipv6 neighbors ip_address
```

*ip_address*

Specifies the IP address in IPv6 colon-separated-hexadecimal notation.

**Usage**
Clears a specific address from the neighbor cache.

**Example**

Use the following example to clear `3ffe:ffff:101::230:6eff:fe04:d9aa/48`:

```
```
clear ipv6 ospf process

Restarts Open Shortest Path First Version 3 (OSPFv3) with available configuration.

Product
- PDSN
- HA
- GGSN

Privilege
- Administrator, Security Administrator

Mode
- Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

clear ipv6 ospf process

Usage
Force a restart of OSPFv3 process using the available configuration.

Example

clear ipv6 ospf process
clear l2tp

Clears all or specific Layer 2 Tunnelling Protocol (L2TP) statistics or clears and disconnects all or specified sessions or tunnels.

**Product**
- PDSN
- GGSN
- LNS

**Privilege**
- Security Administrator, Administrator, Operator

**Mode**
- Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
clear l2tp { statistics [ lac-service service_name | lns-service service_name | peer-address ip_address ] | tunnels { all [ clear-sa ] | callid call_id | lac-service service_name [ clear-sa ] | lns-service service_name | peer-address ip_address [ clear-sa ] } }
```

**statistics [ lac-service service_name | lns-service service_name | peer-address ip_address ]**

With no optional keywords specified, this command clears all L2TP statistics for the current context.

- **lac-service service_name**: Clears all L2TP statistics for the specified LAC service in the current context.
- **lns-service service_name**: Clears all L2TP statistics for the specified LNS service in the current context.
- **peer-address ip_address**: Clears all L2TP statistics for the destination (peer LNS) at the specified IP address. The IP address is entered using IPv4 dotted-decimal notation.

**tunnels { all [ clear-sa ] | callid call_id | lac-service service_name [ clear-sa ] | lns-service service_name | peer-address ip_address [ clear-sa ] }**

- **all**: Clears all tunnels in the current context.
- **lac-service service_name**: Clears all tunnels in the current context that belong to the specified LAC service and closes the tunnels.
- **lns-service service_name**: Clears all tunnels in the current context that belong to the specified LNS service and closes the tunnels.
- **peer-address ip_address**: Clears all tunnels in the current context whose destination (peer LNS) is the system at the specified IP address. The IP address is specified using IPv4 dotted-decimal notation.
- **callid call_id**: Uses the unique identifier that specifies a particular tunnel in the system to clear that tunnel and disconnect it. The output of the command `show l2tp tunnels` contains a field labeled Callid Hint which lists the call id information to use with this command. This is an 8-byte hexadecimal number.
- **clear-sa**: If any security associations have been established they are cleared.
Usage
Clear L2TP all or specific L2TP statistics or clear sessions in a tunnel and disconnect the tunnel.

Example
To clear all L2TP statistics for the current context, use the following command:

```
clear l2tp statistics
```

To clear all L2TP statistics for the LAC service named `lac1`, use the following command:

```
clear l2tp statistics lac-service lac1
```

Use the following command to clear L2TP statistics for the LNS peer at the IP address `10.10.10.100`:

```
clear l2tp statistics peer-address 10.10.10.100
```

The following command clears and closes all tunnels in the current context:

```
clear l2tp tunnels all
```

The following command clears and closes all tunnels for the LAC service named `lac2`:

```
clear l2tp tunnels lac-service lac2
```

The following command clears and closes all tunnels the peer at the IP address `10.10.10.110`:

```
clear l2tp tunnels peer-address 10.10.10.110
```
clear lawful-intercept

Refer to the Lawful Intercept Configuration Guide for a description of this command.
clear llc statistics

Deletes collected traffic statistics for the GPRS logical link-control (LLC) layer.

**Product**
SGSN

**Privilege**
Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
clear llc statistics [ gprs-service srvc_name ] [ | { grep grep_options | more } ]
```

- **gprs-service srvc_name**
  Clears the collected statistics for an existing GPRS service specified as an alphanumeric string of 1 through 63 characters.

- **grep grep_options | more**
  Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
  For more information on the usage of **grep** and **more**, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Reference*.

**Usage**

This command deletes statistics collected for the traffic that has gone through the LLC layer for either all GPRS services or for a specified GPRS service.

**Example**

The following command deletes all LLC statistics for GPRS service **gprs1**:  

```
clear llc statistics gprs-service gprs1
```
clear lma-service statistics

Clears Local Mobility Anchor (LMA) statistics and counters found in show command outputs and bulk statistics associated with all LMA services or a specific service defined by the parameter in this command.

Product
P-GW
SAEGW

Privilege
Operator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

```
clear lma-service statistics [ name service_name ]
```

```
name service_name
```

Cleans statistics and counters for an existing LMA service name specified as an alphanumeric string of 1 through 63 characters.

Usage

Use this command to clear statistics and counters in show command outputs and bulk statistics for all LMA services or for a specific LMA service.

Example

The following command clears statistics and counters for an LMA service named lma3:

```
clear lma-service statistics name lma3
```
clear local-policy

Clears local Quality of Service (QoS) policy service statistics and counters found in show command outputs and bulk statistics associated with all local QoS policy services or a specific service defined by the parameter in this command.

Product

P-GW
SAEGW

Privilege

Operator

Mode

Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

```
clear local-policy statistics [ service service_name ]
```

<table>
<thead>
<tr>
<th>service service_name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clears statistics and counters for an existing local policy service name specified as an alphanumeric string of 1 through 64 characters.</td>
</tr>
</tbody>
</table>

Usage

Use this command to clear statistics and counters in show command outputs and bulk statistics for all local QoS policy services or a specific service.

Example

The following command clears statistics and counters for a local QoS policy service named lp3:

```
clear local-policy statistics service lp3
```
clear local-user

Clears information pertaining to local-user administrative accounts.

Product
All

Privilege
Security Administrator

Mode
Exec
The following prompt is displayed in the Exec mode:

[local] host_name#

Syntax

clear local-user { database [ -noconfirm ] | statistics | username name lockout }

clear local-user database
Clears the local-user database by deleting all information for all local-user accounts.

⚠ Caution: Use this command only in the event of security concerns or to address concerns of the local-user account database integrity.

-noconfirm
Executes the command without any additional prompt and confirmation from the user.

clear local-user statistics
Clears statistics pertaining to local-user accounts.

clear local-user username name lockout
Removes lockouts associated with the local-user account expressed as an alphanumeric string of 3 through 16 characters that is case sensitive.

Usage
This command can be used to remove local-user account lockouts, reset local-user-related statistics to 0, or to delete the local-user database.

Example
The following command removes the lockout placed on a local-user account named SecureAdmin:

clear local-user username SecureAdmin lockout
clear location-service

Clears collected statistics and information pertaining to Location Services.

**Product**
- MME
- SGSN

**Privilege**
Security Administrator

**Mode**
Exec
The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
clear location-services statistics [ service location_svc_name ]
```

**statistics**
Clears all location service statistics.

**service location_svc_name**
Clears statistics only for the specified location service.

**Usage**
Use this command to clear location service statistics.

**Example**
The following command clears the Location service statistics only for the location service named `location_service1`:

```
clear location-service statistics service location_service1
```
clear mag-service statistics

Clears Mobile Access Gateway (MAG) statistics and counters found in `show` command outputs and bulk statistics associated with all MAG services or a specific service defined by the parameter in this command.

**Product**
- HSGW
- S-GW
- SAEGW

**Privilege**
- Operator

**Mode**
- Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
clear mag-service statistics [ name service_name ]
```

**Usage**

Use this command to clears statistics and counters in `show` command outputs and bulk statistics for all MAG services or for a specific MAG service.

**Example**

The following command clears statistics and counters for a MAG service named `mag1`

```
clear mag-service statistics name mag1
```
clear map statistics

Clears Mobile Application Part (MAP) statistics (SS7) for a specified service or all services.

Product
GGSN
SGSN

Privilege
Security Administrator, Administrator, Operator

Mode
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

```clear map statistics [ name service_name ] [ recovered-values ]
```

- **name service_name**
  Clears statistics and counters for an existing MAP service name specified as an alphanumeric string of 1 through 63 characters.

Usage
Delete MAP statistics for a single or all GGSN/SGSN services.

Example
The following command deletes all MAP statistics.

```
   clear map statistics
```
clear maximum-temperatures

Clears information pertaining to component maximum temperatures. (ASR 5x00 only)

**Product**
All

**Privilege**
Security Administrator, Administrator, Operator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

**Syntax**

```plaintext
clear maximum-temperatures
```

**Usage**
Reset the timestamp to the current time and clear previous maximum temperatures for all temperature monitored components. This may be useful when preparing to study system performance, monitor usage, or trouble shoot the administrative interfaces.

**Example**
The following command resets the maximum temperature statistics for all monitored chassis components.

```
clear maximum-temperatures
```
clear mipfa statistics

Clears the statistics for the mobile IP foreign agent (MIPFA). The statistics for a specific foreign agent service may be cleared by an explicit command.

Product
- PDSN
- GGSN
- ASN-GW

Privilege
- Security Administrator, Administrator, Operator

Mode
- Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

```
clear mipfa statistics [ fa-service name | peer-address ip_address ]
```

- **fa-service name | peer-address ip_address**
  - **fa-service name**: Clears the statistics for an existing FA service specified as an alphanumeric string of 1 through 63 characters. “Total sessions” counters for all peers associated with the service are also reset.
  - **peer-address ip_address**: Clears the statistics for the peer IP address specified in IPv4 dotted-decimal notation. “Total sessions” counter for the specified peer is also reset.

Usage

Clear all statistics for the MIP foreign agent or for a specific service. This may be useful in monitoring performance and troubleshooting as the statistics may be cleared at a well known time and then collected and transferred for review.

Example

The following clears all statistics for the mobile IP foreign agent.

```
clear mipfa statistics
```

The following commands clear the statistics for the example service only.

```
clear mipfa statistics fa-service sampleService

clear mipfa statistics peer-address 10.2.3.4
```
clear mipha statistics

Clears the statistics for the mobile IP home agent (MIPHA). The statistics for a home agent service may be cleared by explicit command.

Product
PDSN
HA

Privilege
Security Administrator, Administrator, Operator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

```
clear mipha statistics [ ha-service name | peer-address ip_address ]
```

- **ha-service name**: Clears the statistics for an existing HA service name specified as an alphanumeric string of 1 through 63 characters. “Total sessions” counters for all peers associated with the service are also reset.
- **peer-address ip_address**: Clears the statistics for an IP address specified using IPv4 dotted-decimal notation. “Total sessions” counter for the specified peer is also reset.

Usage
Clear all statistics for the MIP home agent or for a specific service. This may be useful in monitoring performance and troubleshooting as the statistics may be cleared at a well known time and then collected and transferred for review.

Example
The following clears all statistics for the mobile IP foreign agent.

```
clear mipha statistics
```

The following command clears the statistics for the example service only.

```
clear mipha statistics ha-service sampleService
```

```
clear mipha statistics peer-address 10.2.3.4
```
clear mipmn statistics

Clears the statistics for mobile IP mobile node (MIPMN).

**Product**
PDSN
HA

**Privilege**
Security Administrator, Administrator, Operator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

clear mipmn statistics

**Usage**
Clear all statistics for MIP mobile node. This may be useful in monitoring performance and troubleshooting as the statistics may be cleared at a well known time and then collected and transferred for review.

**Example**
The following clears all statistics for MIP mobile node:

```
clear mipmn statistics
```
clear mipv6ha statistics

Clears the statistics for mobile IP IPv6 home agent (MIPv6HA).

**Product**
- PDSN
- HA

**Privilege**
- Security Administrator, Administrator, Operator

**Mode**
- Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
clear mipv6ha statistics
```

**Usage**
Clear all statistics for a MIP IPv6 home agent. This may be useful in monitoring performance and troubleshooting as the statistics may be cleared at a well known time and then collected and transferred for review.

**Example**
The following clears all statistics for MIPv6 home agent:

```
clear mipv6ha statistics
```
clear mme-service db record

Clears the MME database records all instances of session manager running for an MME service filtered with IMSI or GUTI as criteria.

**Product**
MME

**Privilege**
Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

**Syntax**

clear mme-service db record { all | guti plmn plmn_id group-id mme_grp_id code mme_code m-tmsi mtmsi_value | imsi imsi_identifier | instance instance_id }

- **all**
  Clears all detached database records.

- **guti plmn plmn_id group-id mme_grp_id code mme_code m-tmsi mtmsi_value**
  This set of keywords specifies the filter criteria as a Globally Unique Temporary Identifier (GUTI) to clear the database records for MME service.
  The GUTI is constructed from the GUMMEI and the M-TMSI where GUMMEI is constructed from PLMN (MMC and MNC) plmn_id and MME Identifier is constructed from an MME Group ID (MMEGI) mme_grp_id and an MME Code (MMEC) mme_code.
  Within the MME, the mobile is identified by the M-TMSI mtmsi_value

- **imsi imsi_identifier**
  Specifies the filter criteria as International Mobile Subscriber Identity (IMSI) to clear the database records of a session instance. imsi_identifier is a 15-character IMSI field that identifies the subscriber’s home country and carrier.

- **instance instance_id**
  Clears all detached database records in an existing session manager instance specified as an integer from 1 through 4294967295.

**Usage**

Use this command to clear/remove database records for all or a particular instance of session manager for MME services on this system.

**Example**

The following command clears the summary database records of a session instance for subscriber having IMSI as 123455432112345 in the MME service:
clear mme-service db record

```
clear mme-service db record imsi 123455432112345
```
clear mme-service db statistics

Clears the MME database statistics for MME sessions for all or specific session instances on this system.

Product
MME

Privilege
Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

clear mme-service db statistics [ instance smgr_instance ]

instance smgr_instance

Specifies that MME database statistics for a specific instance of session manager running for MME service are to be remove. The instance ID expressed is an integer from 0 through 4294967295. If an instance is not specified, database statistics of all instances will be removed.

Usage

Use this command to clear/remove database statistics for all or a particular instance of session manager for MME services on this system.

Example

The following command removes/clears the database statistics of all instances of the MME service on a system:

    clear mme-service db statistics
clear mme-service statistics

Clears MME service statistics based on various criteria.

**Product**
MME

**Privilege**
Security Administrator, Administrator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local] host_name#  
```

**Syntax**

```
clear mme-service statistics [ emm-only | esm-only | handover | mme-service mme_svc_name ]
emm-only | esm-only | handover | offload | slap | sctp ] | offload | peer-id
peer_identifier [ emm-only | esm-only | handover | offload | slap | sctp ] | slap | sctp
] [ | { grep grep_options | more } ]
```

---

**emm-only**
Clears EPS mobility management (EMM) related statistics for all MME services, or clears these statistics for a specific MME service name or a specific eNodeB association peer identifier.

---

**esm-only**
Clears EPS session management (ESM) related statistics for all MME services, or clears these statistics for a specific MME service name or a specific eNodeB association peer identifier.

---

**handover**
Clears handover related statistics (such as Intra-MME, EUTRAN<->EUTRAN via S10, EUTRAN<->UTRAN via GnGp, EUTRAN<->GERAN via GnGp, and EUTRAN<->UTRAN via S3) for all MME services, or clears these statistics for a specific MME service name or a specific eNodeB association peer identifier.

---

**mme-service mme_svc_name**
Clears all statistics for the specified MME service name.

---

**offload**
Clears all load rebalancing (UE offload) statistics for all MME services, or clears these statistics for a specific MME service name or a specific eNodeB association peer identifier.

---

**peer-id peer_identifier**
Clears all statistics for the specified eNodeB association peer identifier.
clear mme-service statistics

**slap**
Clears all S1-AP statistics for all MME services, or clears these statistics for a specific MME service name or a specific eNodeB association peer identifier.

**sctp**
Clears all SCTP statistics for all MME services, or clears these statistics for a specific MME service name or a specific eNodeB association peer identifier.

**grep grep_options | more**
Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter.

**Usage**
This command is used to clear the statistical information of an MME service based on various filter criteria.

**Example**
The following command clears the service statistics of all MME service on a system:

```
clear mme-service statistics
```
clear multicast-sessions

Disconnects broadcast-multicast sessions based on specified criteria.

Product

PDSN
SGSN

Privilege

Security Administrator Operator

Mode

Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

clearmulticast-sessions [ -noconfirm ] [ keywords ] [ verbose ]

-noconfirm
Executes the command without any additional prompt and confirmation from the user.

all
Disconnects all multicast sessions.

callid call_id
Clears the call specified by call_id. The call ID is as an 8-byte hexadecimal number.

card-num slot_num
Specifies the slot number of the packet processing card by which the multicast session is processed as a number from 1 through 7 or 10 through 16 (for the ASR 5000) or from 1 through 3 or 6 through 10 (for the ASR 5500).

flowid id
Clears calls for a specific Broadcast/Multicast Service (BCMCS) flow id, specified as a hexadecimal number.

flowid-type [ flow | program ]
Clears multicast sessions according to the type of flow.
flow: Clears all multicast sessions for the flow ID type “flow”.
program: Clears all multicast sessions for the flow ID type “program”.

mcast-address ipv4_address
Clears multicast sessions for a specific multicast address. Must be followed by the IP address of an interface in IPv4 dotted-decimal notation.
Exec Mode Commands (A-C)

clear multicast-sessions

pcf ipv4_address
Cleans multicast sessions connected via the packet control function defined by an IP address in IPv4 dotted-decimal notation.

pdsn_service name
Cleans multicast sessions connected to an existing packet data service name.

sgsn-service svc_name
Displays information for multicast sessions connected to an existing SGSN service name.

verbose
Displays as much information as possible. If this option is not specified, the output is the standard level which is the concise mode.

Usage
Clear multicast sessions to aid in troubleshooting the system when no additional subscribers may connect or when a specific service or remote address may be having connection problems. This command may also be useful when preparing for maintenance activities such that connections may be cleared to perform any necessary procedures.

The keywords are filters that modify or filter the criteria for deciding which sessions to clear and are described below. Multiple keywords can be entered on a command line.

When multiple keywords are specified, the multicast sessions deleted must meet the specifications of all of the keywords.

Example
The following command clears the broadcast-multicast sessions having multicast address 10.2.3.4:

    clear multicast-sessions mcast-address 10.2.3.4

The following command clears the broadcast-multicast session(s) having call id 00004e22:

    clear multicast-sessions callid 00004e22
clear orbem statistics

Clears the interface statistics for the object request broker element manager (ORBEM) interface.

**Product**
All

**Privilege**
Security Administrator, Administrator, Operator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name# 
```

**Syntax**

```
clear orbem statistics
```

**Usage**

Clear the statistics to reset them to zero for the ORBEM interface. This may be useful when preparing to study system performance, monitor usage, or troubleshoot the administrative interfaces.

**Example**

The following command resets the statistics for the ORB element manager.

```
clear orbem statistics
```
clear pcc-policy service statistics

Clears statistical information of all or a specific policy control and charging (PCC) service configured in a context.

Product
IPCF

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

```
clear pcc-policy statistics [ name pcc_plcy_svc_name ]
```

<table>
<thead>
<tr>
<th>name pcc_plcy_svc_name</th>
</tr>
</thead>
</table>
| Clears information only for an existing PCC-Policy service in the current context, expressed as an alphanumeric string of 1 through 79 characters.

Usage
Use this command to clears the statistical information of all or an specific PCC-Policy services configured in a context.
Clearing of statistics can further be filtered for specific PCC-Policy service name as well.

Example
The following command clears the statistical information for the PCC-Policy service named pcc_policy1 in summarized output:

```
clear pcc-policy service statistics name pcc_policy1
```
clear pcc-policy session

Clears the active/dormant session information about PCC-Policy service instances configured and running on this system based on different filter criteria.

Product
IPCF

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

clear pcc-policy sessions [ all ] [ apn | call-id call_id | imsi imsi_id | ip-address pcc_pcef_ip_address | service pcc_plcy_svc_name ] [ local-purge ]

all
Clears the session information of all registered IP-CAN session(s) on a PCC-Policy service instance running on the system. The display can be filtered based on given filtering criteria.

apn apn_name
Clears the session information for PCC-Policy service sessions connected via an existing APN.

imsi imsi_id
Clears the session information of IP-CAN session(s) based on the IMSI identifier of a subscriber on a PCC-Policy service instance. imsi_id is the International Mobile Subscriber Identity (IMSI) and must be a 15-character field which identifies the subscriber’s home country and carrier.

ip-address pcc_pcef_ip_address
Clears the session statistics of IP-CAN session(s) based on the registered PCEF (Policy and Charging Enforcement Function) node IP address expressed in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

call-id call_id
Clears the session statistics of IP-CAN session(s) based on the existing registered call id of an IP-CAN session subscriber specified in eight-byte hexadecimal format.

pcc-policy-service pcc_plcy_svc_name
Clears the session statistics of registered IP-CAN session(s) based on an existing PCC-Policy service name, expressed as an alphanumeric string of 1 through 63 characters.

local-purge
Clears the session information for PCC-Policy service sessions locally only.
Usage

Use this command to clear the session statistics of all or specific registered IP-CAN session(s) or in selected part of user session for PCC-Policy services configured and running on this system.

Example

The following command clears the session statistics for all registered PCC-Policy service instances on a system/context locally only:

```plaintext
clear pcc-policy sessions all local-purge
```
clear pcc-sp-endpoint statistics

Clears the statistical information of all or specific PCC-Sp-Endpoint instance configured in a context.

Product
IPCFC

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

```
clear pcc-sp-endpoint statistics [ name sp_endpt_name ]
```

```
name sp_endpt_name
```

Clears information only for an existing PCC-Sp-Endpoint instance specified as an alphanumeric string of 1 through 79 characters.

Usage

Use this command to clears the statistical information of all or specific PCC-Sp-Endpoint interface configured in a context.

Clearing of statistics can further be filtered for specific PCC-Sp-Endpoint instance name as well.

Example

The following command clears the statistical information for the PCC-Sp-Endpoint instance named sp1 in summarized output:

```plaintext
clear pcc-sp-endpoint statistics name sp1
```
clear pdg-service statistics

Deletes all previously gathered statistics for a specific Packet Data Gateway (PDG) service or all PDG services configured within a context.

Product
PDG/TTG

Privilege
Security Administrator, Administrator, Operator

Mode
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

```
clear pdg-service statistics [ name service_name ]
```

**name service_name**
Clears the statistics for the PDG service name configured in the context, expressed as an alphanumeric string of 1 through 63 characters that is case sensitive.

Usage
Usage Statistics for a single PDG service can be cleared using the name keyword. Statistics for all PDG services in the context can be deleted by entering the command with no keywords. If this command is executed from within the local context with no keywords, statistics will be cleared for every PDG service configured on the system regardless of context. In addition, if the name keyword is used when executing from within the local context, statistics for all PDG services configured with the specified name will be cleared regardless of context.

Example
Example(s) The following command clears statistics for a PDG service named pdgl:

```
clear pdg-service statistics pdgl
```
clear pgw-service

Clears PDN Gateway (P-GW) statistics and counters found in `show` command outputs and bulk statistics associated with all P-GW services or a specific service defined by the parameter in this command.

**Product**
P-GW
SAEGW

**Privilege**
Operator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local] host_name#
```

**Syntax**

```
clear pgw-service statistics [ name service_name ] [ | { grep grep_options | more } ]
```

- `name service_name`
  Clears statistics and counters for an existing P-GW service name, expressed as an alphanumeric string of 1 through 63 characters.

- `grep grep_options | more`
  Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
  For details on the usage of `grep` and `more`, refer to the *Regulating a Command’s Output* section of the Command Line Interface Overview chapter.

**Usage**

Use this command to clear statistics and counters in show command outputs and bulk statistics for all P-GW services or for a specific P-GW service.

**Example**

The following command clears statistics and counters for an P-GW service named `pgw5`:

```
clear pgw-service statistics name pgw5
```
clear port

Clears port related statistics.

**Product**
All

**Privilege**
Security Administrator, Administrator, Operator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
clear port { datalink counters { all | slot/port } | npu counters { all | slot/port [ untagged | vlan tag_id ] } }
```

- **clear port datalink counters**
  Clears data link port statistics.

- **clear port npu counters**
  Clears statistics for the network processing unit(s).

- **all**
  Clears counters for all datalink or NPU ports.

- **slot/port**
  Clears the statistics for the specified slot and port number.

- **untagged**
  Clears NPU statistics for all ports that do not have a VLAN tag.

- **vlan tag_id**
  Clears NPU statistics for the port that has a previously configured VLAN tag ID.

**Usage**
Manually clear the statistics for a specified port. This is useful when preparing to trouble shoot or monitor the system.

**Example**
The following command clears the data link related statistics for port 1 in slot 17.

```
clear port datalink counters 17/1
```

The following command clears the network processing unit related statistics for port 1 in slot 17.
clear port npu counters 17/1

The following command clears the network processing unit related statistics for port 10 in slot 5.

clear port npu counters 5/10
clear ppp statistics

Clears point-to-point protocol (PPP) related statistics. All PPP statistics may be cleared or just those for a specific packet data service may be cleared.

Product

PDSN
GGSN

Privilege

Security Administrator, Administrator, Operator

Mode

Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

clear ppp statistics [ ggsn-service ggsn_name | lns-service lns_name | pcf-address [ pcf_ip_addr | all ] | pdsn-service pdsn_name ]

<table>
<thead>
<tr>
<th>ggsn-service ggsn_name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clears statistics only for the time the session is connected to the named GGSN service.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>lns-service lns_name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clears statistics only for the time the session is connected to the named LNS service.</td>
</tr>
</tbody>
</table>

| pcf-address [ pcf_ip_addr | all ] |
|-----------------------------------|
| Clears statistics only for the time the session is connected to the specified PCF (Packet Control Function) or for all PCFs. *pcf_ip_addr* must be entered using IPv4 dotted-decimal notation. |

<table>
<thead>
<tr>
<th>pdsn-service pdsn_name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clears statistics only for the named PDSN service.</td>
</tr>
</tbody>
</table>

Usage

Allows you to manually reset PPP statistics when it is desired to have counts begin again from a specific point in time.

Example

The following clears the statistics for all PPP counters and services.

```
clear ppp statistics
```

The following clears only the point-to-point protocol statistics for the service named *sampleService*.

```
clear ppp statistics pdsn-service sampleService
```
clear prepaid 3gpp2 statistics

Clears all of the statistics counters for 3GPP2 Pre-paid accounting. Statistics may be cleared for all services or for an individual service.

Product
PDSN
GGSN

Privilege
Security Administrator, Administrator, Operator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local] host_name#

Syntax

clear prepaid 3gpp2 statistics { all | { ggsn-service | ha-service | lns-service | pdsn-service | pdsnclosedrp-service } { all | name service_name } }

   all
   Clears prepaid statistics for all services.

   ggsn-service
   Clears statistics for GGSN service(s).

   ha-service
   Clears statistics for HA service(s).

   lns-service
   Clears statistics for LNS service(s).

   pdsn-service
   Clears statistics for PDSN service(s).

   { all | name service_name }
   all: Clears statistics for all services of the specified type.
   name service_name: Clears statistics for the named service of the specified service type.

Usage
Use this command to clear Pre-paid statistics for a particular named service or for all services.

Example
To clear statistics for a PDSN service name PDSN1, enter the following command:
clear prepaid 3gpp2 statistics pdn-service name PDSN1
clear prepaid wimax

Clears all of the statistical counters for WiMAX prepaid accounting. Statistics may be cleared for all services or for an individual service.

**Product**
ASN-GW

**Privilege**
Operator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
clear prepaid wimax statistics { all | asngw-service { all | name service_name } | ha-service { all | name service_name } }
```

- **all**
  Clears prepaid statistics for all services.

- **asngw-service**
  Clears prepaid statistics for ASN-GW service(s).

- **ha-service**
  Clears prepaid accounting statistics for HA service(s).

  `{ all | name service_name }

  - **all**: Clears statistics for all services of the specified type.
  - **name service_name**: Clears statistics for the named service of the specified service type.

**Usage**

Use this command to clear prepaid WiMAX accounting statistics for named service or for all services.

**Example**

The following command clears prepaid WiMAX accounting statistics for an ASN-GW service name `asn1`:

```
clear prepaid wimax statistics asngw-service name asn1
```
clear ps-network statistics

Clears the HNB-Packet Switched (PS) network service associated with an HNB-GW service instance.

Product
HNB-GW

Privilege
Operator

Mode
Exec

The following prompt is displayed in the Exec mode:

[llocal]host_name#

Syntax

clear ps-network statistics [ name cs_svc_name | gtpu-only | ranap-only | rtp-only | sccp-only ]

name ps_svc_name

Clears the session statistics based on an existing HNB-PS network service name, expressed as an alphanumeric string of from 1 through 63 characters.

gtpu-only

Clears the session statistics for GTP-U traffic only for the specified HNB-PS Network service.

ranap-only

Clears the session statistics for Radio Access Network Application Protocol (RANAP) traffic only for the specified HNB-PS Network service.

sccp-only

Clears the session statistics for Signaling Connection Control Part (SCCP) traffic only for the specified HNB-PS Network service.

Usage

Use this command to clear the session statistics for overall session or in selected part of user session for HNB-CS Network services configured and running on a system.

Example

The following command clears the session statistics for RANAP part of session for the HNB-PS Network service hnb_PS_1:

    clear ps-network statistics name hnb_PS_1 ranap-only
clear qos npu stats

Clears information pertaining to NPU QoS priority queue bandwidth allocation and sharing.

Product
GGSN

Privilege
Security Administrator, Administrator, Operator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

```
clear qos npu stats inter-subscriber traffic slot slot_num
```

inter-subscriber traffic slot slot_num

Clears inter-subscriber traffic statistics for the ASR 5000 application or line card or the ASR 5500 DPC or MIO card installed in the specified slot.

slot_num indicates the number of the chassis slot in which the card is installed and can be configured to an integer value from 1 through 48 (for the ASR 5000) or 1 through 10 (for the ASR 5500).

Usage

Allows you to manually reset statistics pertaining to NPU QoS priority queue bandwidth allocation.

Example

The following command clears statistics for a card installed in chassis slot 3:

```
clear qos npu stats inter-subscriber traffic slot 3
```
clear radius accounting archive

Clears archived RADIUS accounting messages associated with an AAA group, or all the archived RADIUS accounting messages in the context in which the command is executed depending on the option chosen. The scope of the command is limited to the context in which it is executed (including the local context).

**Important:** This command is only available in StarOS 8.3 and later. For more information, please contact your local service representative.

**Product**
- All

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec
  
  The following prompt is displayed in the Exec mode:

  ```
  [local]host_name# 
  ```

**Syntax**

```
clear radius accounting archive { all | radius group group_name } [ -noconfirm ]
```

- `all`
  
  Clears all archived RADIUS accounting messages in the context.

- `radius group group_name`
  
  Clears all archived RADIUS accounting messages for the specified RADIUS group. `group_name` must be the name of a RADIUS server group, and must be an alphanumeric string of 0 through 64 characters.

- `-noconfirm`
  
  Executes the command without any additional prompt and confirmation from the user.

**Usage**

Use this command to clear the archived RADIUS accounting messages associated with an AAA group, or all the archived RADIUS accounting messages in the context in which the command is executed.

**Example**

Use the following command to clear all archived RADIUS accounting messages for the group named `test12`.

```
clear radius accounting archive radius group test12
```
clear radius counters

Clears statistics for RADIUS servers or a server group. The statistics for all RADIUS servers or a server group may be cleared.

**Product**
- PDSN
- GGSN
- ASN-GW
- P-GW
- SAEGW

**Privilege**
Security Administrator, Administrator, Operator

**Mode**
Exec
The following prompt is displayed in the Exec mode:

```
[local] host_name#
```

**Syntax**

```
clear radius counters { all | radius group group_name | server ip_address [ port number ] }
```

- `all`: Clears statistics for all servers.
- `radius group group_name`: Clears all configured authentication/accounting servers in the specified RADIUS group. `group_name` must be the name of server group configured in a specific context for authentication/accounting, expressed as an alphanumeric string of 1 through 63 characters.
- `server ip_address [ port number ]`: Clears statistics only for the server specified using IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation. Optionally, you can specify the port which is to have its RADIUS statistics cleared as an integer from 0 through 65535.

**Usage**
Clear the statistics to reset them to zero prior to logging or monitoring the system for troubleshooting, performance measurements, etc.

**Example**
The following command clears the statistics for all RADIUS servers.

```
clear radius counters all
```

The following command resets the statistics only for the server 10.2.3.4.

```
clear radius counters server 10.2.3.4
```

The following command resets the statistics only for the server group named `star1`.

```
clear radius counters radius group star1
```
clear rlf-context-statistics

Clears the statistics for all active Rate Limiting Function (RLF) contexts.

Product
GGSN
P-GW

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

```
clear rlf-context-statistics { diamproxy [ endpoint endpoint_name [ peer-realm realm_name [ peer-host host_name ] ] ] grep_options] ingress ] } [ | { grep | more }]
```

```
endpoint endpoint_name
Clears the context information only for the endpoint specified as a string of size ranging from 1 through 63 characters.
```

```
realm realm_name
Clears the context information only for the realm specified as a string of size ranging from 1 through 127 characters.
```

```
peer-host host_name
Clears the context information only for the host specified as a string of size ranging from 1 through 63 characters.
```

```
| { grep grep_options | more }
```

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the `grep` and `more` commands, refer to the `Regulating a Command’s Output` section of the `Command Line Interface Overview` chapter.

Usage

Use this command to clear the statistics for all active RLF contexts.

Example

The following command clears the statistics for all active RLF contexts:

```
clear rlf-context-statistics diamproxy
```
clear rohc statistics

Clears statistics and counters collected since the last reload or clear command was issued for RObust Header Compression (ROHC) [RFC 3095].

Product
PDSN
ASN-GW
HSGW

Privilege
Administrator, Config-administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

`clear rohc statistics [ pdsn-service pdsnsvc_name | asngw-service asngwsvc_name ]`

- **pdsn-service pdsnsvc_name**
  Cuts ROHC statistics and counters for the specified PDSN service.

- **asngw-service asngwsvc_name**
  Cuts ROHC statistics and counters for the specified ASN-GW service.

Usage

Use this command to clear ROHC statistics for all services or for a specific PDSN or ASNGW service.

Example

The following command clears ROHC statistics and counters for the PDSN service named `pdsn1`:

```
clear rohc statistics pdsn-service pdsn1
```
clear rp service-option

Clears the radio-packet (R-P) interface service option statistics.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator, Operator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

**Syntax**

```
clear rp service-option statistics [ number option_num | pdsn-service pdsn_name ]
```

- `number option_num | pdsn-service pdsn_name`
  - Default: clears the statistics for all service options and all packet data services.
  - `number option_num`: Specifies the R-P service option number for which the statistics are to be cleared as an integer from 0 through 1000.
  - `pdsn-service pdsn_name`: Specifies the PDSN service name for which statistics will be cleared.

**Usage**
Clear the R-P service option statistics prior to monitoring the system for benchmarking or for detecting areas of further research.

**Example**
The following resets the service option statistics for service option 23 and packet data service sampleService, respectively.

```
clear rp service-option statistics number 23

clear rp service-option statistics pdsn-service sampleService
```
clear rp statistics

Clears the radio-packet (R-P) interface statistics. The statistics for a specific packet data server or peer node may be cleared if specified.

Product
PDSN

Privilege
Security Administrator, Administrator, Operator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

```
clear rp statistics [ pdsn-service name | peer-address [ peer_address | all ] ]
```

```
pdsn-service name | peer-address [ peer_address | all ]
```

Default: clears all R-P associated statistics.

- `pdsn-service name`: Specifies the packet data service name that is to have its statistics reset.
- `peer-address [ ip_address | all ]`: Specifies that statistics for the specified peer, or all peers, are to be cleared. The `ip_address` must be specified using IPv4 dotted-decimal notation.

Usage
Clear the statistics to prepare for monitoring the system.

Example
The following command resets all the associated statistics for the R-P interfaces.

```
clear rp statistics
```

The following command clears the statistics for the packet data service `sampleService`.

```
clear rp statistics pdsn-service sampleService
```

The following command resets the statistics associated with peer node with IP address `10.2.3.4`.

```
clear rp statistics peer-address 10.2.3.4
```
clear rsvp statistics

Clears the Resource Reservation Protocol (RSVP) statistics.

**Product**
All

**Privilege**
Security Administrator, Administrator, Operator

**Mode**
Exec
The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**
```
clear rsvp statistics
```

**Usage**
Clear RSVP statistics.

**Example**
The following command resets all RSVP statistics.

```
clear rsvp statistics
```
The following command resets the statistics associated with peer node with IP address
clear saegw-service

Clears System Architecture Evolution Gateway (SAEGW) statistics and counters found in show command outputs and bulk statistics associated with all SAEGW services or a specific service defined by the parameter in this command.

**Product**
SAEGW

**Privilege**
Operator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
clear saegw-service statistics { all | name service_name } [ | { grep grep_options | more } ]
```

---

**all**

Clears all SAEGW node-level statistics.

**name service_name**

Clears statistics and counters for an existing SAEGW service name, expressed as an alphanumeric string of 1 through 63 characters.

**grep grep_options | more**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

---

**Usage**

Use this command to clear statistics and counters in show command outputs and bulk statistics for all SAEGW services or for a specific SAEGW service.

**Example**

The following command clears statistics and counters for an SAEGW service named *saegw5*:

```
clear saegw-service statistics name saegw5
```
clear samog-service statistics

Clear statistics associated with S2a Mobility Over GTP (SaMOG) services.

Product
SAMOG

Privilege
Inspector

Syntax

clear samog-service statistics samog_service_name

clear samog-service statistics samog_service_name
Clears SaMOG service-related statistical information. Service name should be between 1 and 63.

Usage
Use this command to clear statistics and counters in show command outputs and bulk statistics for all SaMOG services or for a specific SaMOG service.

Example
Below command clears SaMOG Statistics 21:

clear samog-service statistics 21
clear sccp statistics

Clears SS7 Signaling Connection Control Part (SCCP) statistics collected for services that use the SCCP protocol.

**Product**
SGSN

**Privilege**
Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

**Syntax**

```
clear sccp statistics [ iups-service iups_srvc_name | map-service map_srvc_name | sccp-network ntwk_index [ dpc dpc [ ssn ssn ] | global-title-translation { address-map instance add_map_inst | association instance assoc_inst } [ sessmgr instance sessmgr_inst ] ] [ | { grep grep_options | more } ]
```

**clear sccp statistics**

Deletes collected SCCP protocol statistics for an existing Iu-PS service in the current context specified as an alphanumeric string of 1 through 63 characters.

**map-service** map_srvc_name

Deletes collected SCCP protocol statistics for an existing MAP service specified as an alphanumeric string of 1 through 63 characters.

**sccp-network** ntwk_index

Deletes collected SCCP protocol statistics for the SSCP network configuration with a network index specified as an integer from 1 through 12.

The following filters can be added to limit the clearing of SCCP network statistics:

- **dpc** dpc: Specifies a differentiated pointcode address to limit the deletion of collected SCCP network statistics to those for the identified destination.
- **ssn** ssn: Specifies a subsystem number as an integer from 1 to 255 to limit the deletion of collected SCCP network statistics.
- **global-title-translation address-map** instance add_map_inst: Specifies an identified GTT address-map as an integer from 1 to 4096 to limit the deletion of collected SCCP network statistics.
- **global-title-translation association** instance assoc_inst: Specifies an identified GTT association as an integer from 1 to 16 to limit the deletion of collected SCCP network statistics.
- **sessmgr** instance sessmgr_inst: Specifies an identified session manager instance as an integer from 1 to 384 to limit the deletion of collected SCCP network statistics.
Usage
Use this command to delete all collected SCCP statistics or to delete SCCP statistics for a specified service, SCCP network, or session manager.

Example
The following command deletes all collected SCCP statistics:

```
clear sccp statistics
```

The following command clears all collected SCCP statistics for the IuPS service named `iups-serv1`:

```
clear sccp statistics iups-service iups-serv1
```
clear session disconnect-reasons

Clears the session disconnect reason statistics for all sessions on the system.

Product
All

Privilege
Security Administrator, Administrator, Operator

Mode
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

clear session disconnect-reasons

Usage
Sets the counters for session disconnect reasons to zero (0) in preparation for a monitoring or troubleshooting session.

Example

clear session disconnect-reasons
clear session-event-record statistics

Clears statistics collected during session event module transfers.

Product
S-GW
SAEGW

Privilege
Operator

Mode
Exec
The following prompt is displayed in the Exec mode:

[local] host_name#

Syntax

```
clear session-event-record statistics
```

Usage
Use this command to delete all collected session event record statistics.
clear session setuptime

Clears the session setup time statistics for Packet Control Functions (PCFs) or SGSNs. If no keyword is specified the summary statistics displayed by the `show session setuptime` command are cleared.

**Product**
All

**Privilege**
Security Administrator, Administrator, Operator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
clear session setuptime [ pcf [ pcf_addr | all ] | sgsn-address [ sgsn_addr | all ] ]
```

- **pcf [ pcf_addr | all ]**
  - `pcf_addr`: Clears the setup time counters for the PCF at the IP address specified in IPv4 dotted-decimal notation.
  - `all`: Clears the setup time counters for all PCFs.

- **sgsn-address [ sgsn_addr | all ]**
  - `sgsn_addr`: Clears the setup time counters for the SGSN at the IP address specified in IPv4 dotted-decimal notation.
  - `all`: Clears the setup time counters for all SGSNs.

**Usage**

Sets the counters for session disconnect reasons to zero (0) in preparation for a monitoring or troubleshooting session.

**Example**

To clear the statistics for the PCF at IP address `192.168.100.10`, enter the following command:

```
clear session setuptime pcf 192.168.100.10
```
clear session subsystem

Clears all session subsystem statistics for the current context.

Product
All

Privilege
Security Administrator, Administrator, Operator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

clear session subsystem

Usage
Clear the statistics in preparation for a troubleshooting or monitoring session so that the counters are at a well known values.

Example

clear session subsystem
clear sgsn-fast-path statistics

Clears information related to SGSN fast-path.

**Product**
SGSN

**Privilege**
Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

**Syntax**

```
show sgsn-fast-path statistics [ all | smgr-instance smgr_inst ] [ | { grep grep_options | more } ]
```

- **all**
  Deletes collected fast-path statistics for all session managers.

- **smgr-instance smgr_inst**
  Clears collected fast-path statistics for a session manager instance specified as an integer from 1 to 65535.

- **| grep grep_options | more**
  Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent. Please refer to the *Regulating the Command Output* section in this reference for details on the usage of `grep` and `more`.

**Usage**

Use this command to clear all statistics for SGSN fast-path configurations.

**Example**

The following command deletes all collected fast-path statistics for all SGSN session managers:

```
clear sgsn-fast-path statistics
```
clear sgsn-map-app

Deletes collected statistics for the SGSN Mobile Application Part (MAP).

Product
SGSN

Privilege
Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

clear sgsn-map-app statistics [ | { grep grep_options | more } ]

clear sgsn-map-app statistics

Clears all collected statistics for the SGSN MAP application.

| grep grep_options | more

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

Please refer to the Regulating the Command Output section in this reference for details on the usage of grep and more.

Usage

Use this command to deleted collected statistics for the SGSN MAP application.

Example

The following command clears all collected SGSN MAP statistics:

    clear sgsn-map-app statistics
clear sgs-service

Clears SGs interface statistics associated with a Visitor Location Register (VLR).

**Product**
MME

**Privilege**
Operator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name# 
```

**Syntax**

```
clear sgs-service { statistics [ name name ] | vlr-status [ service-name name ] [ vlr-name name ] }
```

### statistics [ name name ]
Clears statistics for all SGs services or a specific SGs service.

- **name name**: Clears the statistics for an existing SGs service specified as an alphanumeric string of 1 through 63 characters.

### vlr-status [ service-name name ] [ vlr-name name ]
Clears statistics for all VLRs, a VLR related to a SGs service, or a specific VLR.

- **service-name name**: Clears the SGs statistics for an existing VLR specified as an alphanumeric string of 1 through 63 characters.

**Usage**

Use this command to clear statistics for all SGs services, Visitor Location Registers (VLRS), or a specific SGs service or VLR name.

**Example**

The following command clears statistics for an SGs service named *sgs2*:

```
clear sgs-service statistics name sgs2
```
clear sgtpc statistics

Clears all SGSN GTP-C (SGTPC) interface statistics for the current context.

Product
MME
SGSN

Privilege
Security Administrator, Administrator, Operator

Mode
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

clear sgtpc statistics [ gsn-address ipv4_address | sgtp-service sgtp_srvc_name ]

**gsn-address ipv4_address**
Clears GTPC packet statistics for the interface specified as an IP address in IPv4 dotted-decimal notation.

**sgtp-service sgtp_srvc_name**
Clears GTPC packet statistics for an existing SGTP service specified as an alphanumeric string of 1 through 63 characters.

Usage
Use this command to clear the statistics in preparation for a troubleshooting or monitoring session.

**Important:** Statistics are vital for troubleshooting. We recommend that you check with your Cisco support personnel prior to clearing these statistics.

Example

clear sgtpc statistics sgtp-service SGSN1sgtp12
**clear sgtpu statistics**

Clears all SGSN GTP-U (SGTPU) statistics for the current context.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator, Operator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local] host_name#
```

**Syntax**

```
clear sgtpu statistics [ ggsn-address ipv4_address | gprs-service gprs_svc_name nsei nse_id | iups-service iups_srvc_name | iups-bind-address ipv4_address | recovered-values | rnc-address ipv4_address | sgtp-service sgtp_svc_name ]
```

- **ggsn-address ipv4_address**
  Clears GTPU packet statistics for a specific GGSN specified as an IP address in IPv4 dotted-decimal notation.

- **gprs-service gprs_svc_name nsei nse_id**
  **gprs-service gprs_svc_name**: Clears GTPU packet statistics for the interface for a specific GPRS service specified as an alphanumeric string of 1 through 63 characters.
  **nsei nse_id**: Specifies a network service entity (NSEI) as an integer from 0 through 65535.

- **iups-bind-address ipv4_address**
  Clears GTPU packet statistics for the bind address of an IuPS interface specified as an IP address in IPv4 dotted-decimal notation.

- **iups-service iups_svc_name**
  Clears GTPU packet statistics for an active IuPS service interface specified as an alphanumeric string of 1 through 63 characters.

- **rnc-address ipv4_address**
  Clears GTPU packet statistics for an RNC specified as an IP address in IPv4 dotted-decimal notation.

- **sgtp-service sgtp_svc_name**
  Clears GTPU packet statistics for an active SGTP service interface specified as an alphanumeric string of 1 through 63 characters.

**Usage**

Use this command to clear the statistics in preparation for a troubleshooting or monitoring session.
**Important:** Statistics are vital for troubleshooting. We recommend that you check with your Cisco support personnel prior to clearing these statistics.

**Example**

Use this command to clear collected SGTPU statistics for a specific NSEI of a configured GPRS service:

```
clear sgtpu statistics gprs-service SGSN1Gprsl nsei 2445
```
clear sgw-service statistics

Clears Serving Gateway (S-GW) statistics and counters found in `show` command outputs and bulk statistics associated with all S-GW services or a specific service defined by the parameter in this command.

**Product**
- S-GW
- SAEGW

**Privilege**
- Operator

**Mode**
- Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
clear sgw-service statistics { all | name service_name }
```

- `all`
  Clears statistics and counters for all S-GW services configured on the system.

- `name service_name`
  Clears statistics and counters for an existing S-GW service name specified as an alphanumeric string of 1 through 63 characters.

**Usage**

Use this command to clears statistics and counters in show command outputs and bulk statistics for all S-GW services or for a specific S-GW service.

**Example**

The following command clears statistics and counters for an S-GW service named `sgw3`:

```
clear sgw-service statistics name sgw3
```
clear sms statistics

Deletes collected traffic statistics for the Short Message Service (SMS).

**Product**
SGSN

**Privilege**
Administrator, Security Administrator, Operator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
clear sms statistics [ name map_srvc ] [ | { grep grep_options | more } ]
```

- **name map_srvc**
  
  Specifies a MAP Service as an alphanumeric string of 1 to 63 characters.

- **| { grep grep_options | more }**
  
  Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

  For details on the usage of the `grep` and `more` commands, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

**Usage**

Use this command to delete collected traffic statistics for SMS. It is possible to clear the statistics of a specific MAP service associated with the SMS by including the `name` filter.

**Example**

Use the following command to clear SMS statistics for MAP service `MAP-LONDON1`:

```
clear sms statistics name MAP-LONDON1
```
clear sndcp statistics

Deletes all collected statistics for the packet traffic going through the Subnetwork Dependent Convergence Protocol (SNDCP) layer.

Product
SGSN

Privilege
Security Administrator, Administrator, Operator

Mode
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax
clear sndcp statistics [ gprs-service srvc_name ] [ | { grep grep_options | more } ]

gprs-service srvc_name
Specifies a GPRS service as an alphanumeric string of 1 through 63 characters.

| { grep grep_options | more }
Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of the grep and more commands, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference.

Usage
Use this command to delete all collected SNDCP traffic statistics. Include the gprs-service keyword to filter the clearing action to only deleted statistics for one GPRS service.

Example
Use the following command to clear all collected SNDCP layer traffic statistics:

clear sndcp statistics

Use the following command to delete SNDCP layer traffic statistics for the test1 GPRS service:

clear sndcp statistics gprs-service test1
clear snmp trap

Clears all SNMP event trap notifications from the buffer.

**Product**
All

**Privilege**
Security Administrator, Administrator, Operator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
clear snmp trap { history | statistics }
```

- **history**
  Clears all SNMP historical trap information from the system buffer.

- **statistics**
  Clears all SNMP event trap information from the system buffer.

**Usage**

Use this command to empty the buffer of all SNMP trap notifications.

**Example**

The following command clears the all historical SNMP traps from the system buffer:

```
clear snmp trap history
```
clear srp

Clears system Service Redundancy Protocol (SRP) statistics.

Product
All products that support Interchassis Session Recovery (ICSR)

Privilege
Security Administrator, Administrator, Operator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

```
clear srp { audit-statistics | call-loss statistics | checkpoint statistics | statistics }
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>audit-statistics</td>
<td>Clears SRP audit statistics.</td>
</tr>
<tr>
<td>call-loss statistics</td>
<td>Clears SRP call loss history.</td>
</tr>
<tr>
<td>checkpoint statistics</td>
<td>Clears SRP checkpoint interface statistics.</td>
</tr>
<tr>
<td>statistics</td>
<td>Clears SRP statistics.</td>
</tr>
</tbody>
</table>

Usage
Clears the SRP statistics to prepare the system for SRP monitoring.

Example
The following command resets all the associated statistics for SRP checkpoints.
```
clear srp checkpoint statistics
```

The following command resets all the associated statistics for SRP.
```
clear srp statistics
```
clear ss7-routing-domain

Deletes specified statistics for an SS7 routing domain.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator, Operator

**Mode**
Exec
The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
clear ss7-routing-domain domain_index { asp | mtp2 | mtp3 | qsaal | sscf }
```

- **domain_index**
  Specifies the index number of the SS7 routing domain as an integer from 1 through 12.

- **asp**
  Clears statistics and status information for the SS7 Application Service Part (ASP) in the specified SS7 routing domain.

- **m3ua**
  Clears statistics and status information for the SS7 MTP3 User Adaptation Layer (M3UA) in the specified SS7 routing domain.

- **mtp2**
  Clears statistics and status information for the SS7 Message Transfer Part-2 (MTP2) in the specified SS7 routing domain.

- **mtp3**
  Clears statistics and status information for the SS7 Message Transfer Part-3 (MTP3) in the specified SS7 routing domain.

- **qsaal**
  Clears statistics and status information for the Service Specific Connection-Oriented Protocol (SSCOP) sub-layer of the Quasi Signaling Application Adaptation Layer (QSAAL) in the specified SS7 routing domain.

- **sscf**
  Clears statistics and status information for the Service Specific Coordination Function (SSCF [q.2140]) in the specified SS7 routing domain.
clear ss7-routing-domain

Usage
Deletes statistics for the specified SS7 routing domain.

Example
The following command clears SS7 ASP routing statistics for domain index 4:

    clear ss7-routing-domain 4 asp
clear ssl statistics

Deletes all previously gathered Secure Sockets Layer (SSL) statistics for a specific P-CSCF service or all P-CSCF services, either system-wide or within a context.

Product
SCM (P-CSCF, A-BG)

Privilege
Security Administrator, Administrator, Operator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

```
clear ssl statistics [ service-name name ]
```

- **service-name name**
  Specifies the name of a P-CSCF service for which to clear SSL statistics as an alphanumeric string of 1 through 63 characters that is case sensitive.

Usage
SSL statistics for a single P-CSCF service can be cleared using the `service-name` keyword. SSL statistics for all P-CSCF services can be deleted by entering the command with no keywords.
If this command is executed from within the local context with no keywords, SSL statistics will be cleared for every P-CSCF service configured on the system regardless of context. In addition, if the `service-name` keyword is used when executing from within the local context, SSL statistics for all P-CSCF services configured with the specified name will be cleared regardless of context.

Example
The following command clears SSL statistics for the P-CSCF service `pcscf_service_1`:

```
clear ssl statistics service-name pcscf_service_1
```
clear subscribers

Disconnects subscribers based on specified criteria.

Product
All

Privilege
Security Administrator, Administrator, Operator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local] host_name#

Syntax

`clear subscribers [ keywords ] [ verbose ] [ -noconfirm ]`

The keywords are filters that modify or filter the criteria for deciding which subscriber sessions to clear and are described below. Multiple keywords can be entered on a command line. When multiple keywords are specified, the subscriber sessions deleted must meet the specifications of all of the keywords.

For example; if you enter the following command:

`clear subscribers ip-pool pool1 card-num 1`

Only subscriber sessions that were assigned an IP address from the IP pool named `pool1` and are also being processed by the processing card in slot 1 are cleared. All other subscriber sessions that do not meet these criteria remain and are not cleared.

`-noconfirm`

Executes the command without any additional prompt and confirmation from the user.

**Important:** The Operator privilege does not have access to this keyword.

**active**

Only disconnects subscribers who currently have active sessions.

**active-charging-service** `ecs_service_name`

Clears information for subscribers using the Active charging Service. `ecs_service_name` must be the name of the Active Charging Service, expressed as an alphanumeric string of 1 through 15 characters.

**all**

Disconnects all subscribers.
### Exec Mode Commands (A-C)

**clear subscribers**

**Important:** The Operator privilege does not have access to this keyword.

**apn apn_name**

Clears all PDP contexts accessing a specific access point name (APN).

*apn_name* is the name of the APN expressed as an alphanumeric string of 1 through 63 characters that is case sensitive.

**asn-peer-address ip_address**

Clears information for subscribers on an ASN-GW trusted peer.

*ip_address* is the address of the ASN-GW peer server entered using IPv4 dotted-decimal notation.

**asngw-service service_name**

Clears counters for subscribers accessing the ASN-GW service.

*service_name* must be an existing service expressed as an alphanumeric string of 1 through 63 characters.

**asnpc-service service_name**

Clears counters for subscribers accessing the ASN PC service.

*service_name* must be an existing service expressed as an alphanumeric string of 1 through 63 characters.

**bandwidth-policy bandwidth_policy_name**

Clears information for subscribers using the specified bandwidth policy.

*bandwidth_policy_name* must be the name for an existing bandwidth policy, expressed as an alphanumeric string of 1 through 63 characters.

**bearer-establishment { direct-tunnel | normal | pending }**

Clears all subscribers from the specified bearer establishment type.

*direct-tunnel*: Select subscribers having direct tunnel established with the RNC.

*normal*: Select subscribers having bearer established with SGSN.

*pending*: Select subscribers for whom bearer is not fully established.

**bng-only**

Clears information related to BNG calls only.

**bng-service service_name**

Clears all subscribers from the specified BNG service.

*service_name* must be an existing service expressed as an alphanumeric string of 1 through 63 characters.

**callid id**

Clears the call specified by call_id. The call ID must be specified as a 4-byte hexadecimal number.

**card-num card_num**

The slot number of the processing card by which the subscriber session is processed. *card_num* is a slot number from 1 through 7 or 10 through 16 (for the ASR 5000) or from 1 through 4 or 7 through 10 (for the ASR 5500).
**clear subscribers**

**cbb-policy** `cbb_policy_name`
Clears information for subscribers using the specified CBB policy.
`cbb_policy_name` must be the name for an existing CBB policy expressed as an alphanumeric string of 1 through 63 characters.

**ccoa-only**
This option clears the subscribers that registered a MIP co-located COA directly with the HA. This option is only valid when MIPHA session license is enabled.

**cgw-only**
Clears information related to CGW calls only.

**configured-idle-timeout** `[ < | > | greater-than | less-than ] value`
Disconnects subscribers whose idle timeout matches the specified criteria. A value of 0 (zero) indicates that the subscribers idle timeout is disabled.
`<`: Filters output so that only information less than the specified value is cleared.
`: Filters output so that only information greater than the specified value is cleared.
`greater-than`: Filters output so that only information greater than the specified value is cleared.
`less-than`: Filters output so that only information less than the specified value is cleared.
`value`: If no other filtering options are specified only output matching `value` is cleared. If `value` is not specified all data is cleared. `value` must be an integer from 0 through 4294967295.

**connected-time** `[ < | > | greater-than | less-than ] value`
Disconnects subscribers who have been connected for the specified length of time.
`<`: Filters output so that only information less than the specified value is cleared.
`: Filters output so that only information greater than the specified value is cleared.
`greater-than`: Filters output so that only information greater than the specified value is cleared.
`less-than`: Filters output so that only information less than the specified value is cleared.
`value`: If no other filtering options are specified only output matching `value` is cleared. If `value` is not specified all data is cleared. `value` must be an integer from 0 through 4294967295.

**cscf-service** `service_name`
Clears all subscribers from the specified CSCF service.
`service_name` must be an existing service expressed as an alphanumeric string of 1 through 63 characters.

**css-delivery-sequence** `name`

**Important:** This is a restricted keyword. In StarOS 9.0 and later, this keyword is obsoleted.

**css-service** `name`

**Important:** This is a restricted keyword. In StarOS 9.0 and later, this keyword is obsoleted.

**dhcp-server** `address`
Clears all PDP contexts that currently possess an IP address assigned from a specific DHCP server.
`dhcp_address` is the IP address of the DHCP server expressed in IPv4 dotted-decimal notation.
**dormant**

Only disconnects subscriber sessions that are dormant (not transmitting or receiving data).

**ebi number**

Clears subscribers based on an EPS bearer identity (EBI). `number` must be a valid EBI and an integer value from 5 to 15.

**enodeb-address ip_address**

Clears subscribers based on the eNodeB to which they are attached. `ip_address` must be a valid IP address of an existing eNodeB entered using IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

**epdg-address ip_address**

Clears subscribers based on the ePDG to which they are attached. `ip_address` must be a valid IP address of an existing ePDG entered using IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

The following filter keywords are valid with this command:

```
epdg-address,
```

**epdg-service service_name**

Clears subscribers of a configured ePDG service. `service_name` must be a valid string of size 1 to 63. The following filter keywords are valid with this command:

```
epdg-address,
```

**fa ip_address**

Disconnects all subscribers connected to the foreign agent specified by the IP address in IPv4 dotted-decimal notation.

**fa-service fa_name**

Disconnects all subscribers connected to an existing foreign agent name.

**firewall { not-required | required }**

Clears all subscriber information for the specified subscribers:

- **not-required**: Subscribers for whom firewall processing is not-required.
- **required**: Subscribers for whom firewall processing is required.

**firewall-policy fw_policy_name**

This keyword is obsolete.

**fw-and-nat policy fw&nat_policy_name**

Clears information for subscribers using the specified Firewall-and-NAT policy. `fw&nat_policy_name` must be the name of an existing Firewall-and-NAT policy expressed as an alphanumeric string of 1 through 63 characters.
**fng-service service_name**

Clears subscriber sessions connected to the FNG service. `service_name` must be an existing service expressed as an alphanumeric string of 1 through 63 characters.

**ggsn-service name**

Clears all PDP contexts accessing an existing GGSN service specified as an alphanumeric string of 1 through 63 characters that is case sensitive.

**gprs-service name**

Clears all PDP contexts associated with the 2G SGSN. This keyword can be used with filtering keywords that are part of the `clear subscriber` command set. Using this keyword can trigger a network-initiated service request (paging) procedure. `name` identifies a specific GPRS service configuration expressed as an alphanumeric string of 1 through 63 characters.

**gsm-traffic-class { background | conversational | interactive { priority } | streaming }**

Subscribers whose traffic matches the specified 3GPP traffic class.

- **background**: 3GPP QoS background class.
- **conversational**: 3GPP QoS conversational class.
- **interactive**: 3GPP QoS interactive class. Must be followed by a traffic priority. Priority can be configured to any integer value from 1 to 3.
- **streaming**: 3GPP QoS streaming class.

**gtpu-bind-address ip_address**

Disconnects all subscribers connected to the GTP-U service bind address. `ip_address` must be specified in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

**gtpu-service service_name**

Disconnects all subscribers and erase subscriber information based on the GTP-U service name. `service_name` must be an existing GTP-U service expressed as an alphanumeric string of 1 through 63 characters.

**gtp-version**

Displays the specific GTP version number. Must be followed by one of the supported GTP versions (0 or 1). The following filter keywords are valid with this command:

active-charging-service, apn, asgw-service, asmpc-service, asn-peer-address, bearer-establishment, callid, card-num, coaa-only, configured-idle-timeout, connected-time, csf-service, dhcp-server, fa, fa-service, firewall, ggsn-service, gprs-service, gsm-traffic-class, gtp-version, ha, ha-ipsecc-service, ha-service, idle-time, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, lac, lac-service, lns, lns-service, long-duration-time-left, mip-udp-tunnel-only, mipv6ha-service, msid, msisdn, network-requested, network-type, pcf, pdg-service, pdif-service, pdsn-service, plmn-type, rulebase, rx-data, session-time-left, sgsn-address, sgsn-service, tx-data, username, grep, more

**ha address**

Disconnects all subscribers connected to the home agent.
**clear subscribers**

*ha_address* must be specified using IPv4 dotted-decimal notation.

**ha-ipsec-only**

Disconnects all MIP HA sessions with IPSec tunnels.

**ha-service name**

Disconnects all subscribers connected to the home agent specified by *ha_name* must have been previously defined.

**hnbgw-service svc_name**

Disconnects all subscribers and erase subscriber information based on the HNB-GW service name. *svc_name* must be an existing HNB-GW service expressed as an alphanumeric string of 1 through 63 characters.

**hsgw-only**

Disconnects subscribers emerging from a HRPD Serving Gateway (HSGW) service configured on this system.

**hsgw-service name**

Disconnects subscribers using this HRPD Serving Gateway (HSGW) service configured on this system. *name* must be an existing HSGW service expressed as an alphanumeric string of 1 through 63 characters.

**idle-time [ < | > | greater-than | less-than ] value**

Disconnects subscribers whose idle time matches the specified length of time. 
*<:* Filters output so that only information less than the specified value is cleared.

*>:* Filters output so that only information greater than the specified value is cleared.

*greater-than:* Filters output so that only information greater than the specified value is cleared.

*less-than:* Filters output so that only information less than the specified value is cleared.

*value:* If no other filtering options are specified only output matching *value* is cleared. If *value* is not specified all data is cleared. *value* must be an integer from 0 through 4294967295.

**imei imei**

SGSN only.

Disconnects one or more subscribers based on the international mobile equipment identity (IMEI or IMEI-SV) of the subscriber’s mobile equipment.

*imei:* enter 14 to 16 digits to match the first 14 digits of a retrieved IMEI/IMEISV for a single subscriber. to match a range of subscribers, the string may be shorter and include ‘$’ as a wildcard for a single digit or ‘*’ as a wildcard for multiple digits.

**ims-auth-service imsa_service_name**

Disconnects subscribers using this IMS Authorization Service configured on this system.

*imsa_service_name* must be an existing IMS Authorization Service expressed as an alphanumeric string of 1 through 63 characters.

**imsi id**

Disconnects the subscriber with the specified id. The IMSI (International Mobile Subscriber Identity) ID is a 50-bit field which identifies the subscriber’s home country and carrier. Wildcard characters $ and * are
allowed. The * wildcard matches multiple characters and the $ wildcard matches a single character. If you do not want the wildcard characters interpreted as a wildcard enclose them in single quotes (‘ ’). For example: ‘$’.

```
interface-type \{ S2bGTP | S5S8GTP \}
```
Disconnects subscribers based on their interface type.

**S2bGTP:** Indicates that the GTP protocol is used on the S2b interface for the subscribers being disconnected.

**S5S8GTP:** Indicates that the GTP protocol is used on the S5/S8 interface for the subscribers being disconnected.

```
ip-address address
```
Disconnects all subscribers connected to the specified ip_address. The address must be specified using IPv4 dotted-decimal notation.

**Note:** This keyword is not supported for use with the MME or SGSN.

```
ip.alloc-method \{ aaa-assigned | dhcp \{ relay-agent | proxy-client \} | dynamic-pool | l2tp-lns-assigned | mip-ha-assigned | ms-provided-static | not-ms-provided-static | static-pool \}
```
Displays the specific IP Allocation Method. Must be followed by one of the IP Allocation Methods:

- **aaa-assigned:** Selects subscribers whose IP Addresses were assigned by AAA.
- **dhcp:** Selects subscribers whose IP Addresses were assigned by DHCP.
- **dynamic-pool:** Selects subscribers whose IP Addresses were assigned from a dynamic IP address pool.
- **l2tp-lns-assigned:** Selects subscribers whose IP Addresses were assigned by the Layer 2 Tunnelling Protocol Network Server.
- **mip-ha-assigned:** Selects subscribers whose IP Addresses were assigned by the Mobile IP Home Agent.
- **ms-provided-static:** Selects subscribers whose IP Addresses were provided by the Mobile Station.
- **not-ms-provided-static:** Selects subscribers whose IP Addresses were not provided by the Mobile Station.
- **proxy-client:** Selects subscribers whose IP Addresses were assigned by the DHCP Proxy Client
- **relay-agent:** Selects subscribers whose IP Addresses were assigned by the DHCP Relay Agent
- **static-pool:** Selects subscribers whose IP Addresses were assigned from a static IP address pool.

```
ip.pool name
```
Disconnects all subscribers assigned addresses from the IP address pool pool_name. pool_name must be the name of an existing IP pool or IP pool group.

```
ip4
```
Clears all subscribers with IPv4 Firewall enabled/disabled.

```
ip6
```
Clears all subscribers with IPv6 Firewall enabled/disabled.
clear subscribers

**ipv6-address ipv6_address**
Clears all subscribers connected to the specified IPv6 `ipv6_address` must be specified in IPv6 colon-separated-hexadecimal notation.
Note: This keyword is not supported for use with the MME or SGSN.

**ipv6-prefix prefix**
Clears subscribers from a specific IPv6 address prefix.

**13-tunnel-local-addr ip_address**
Disconnects all calls for this Layer 3 tunneling interface.
`ip_address` must be specified in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

**13-tunnel-remote-addr ip_address**
Disconnects all calls for this Layer 3 tunneling peer.
`ip_address` must be specified in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

**lac ip_address**
Disconnects all calls to the peer LAC (L2TP access concentrator).
`ip_address` must be specified using IPv4 dotted-decimal notation.

**lac-service service_name**
Disconnects all calls for this LAC service.
`service_name` is an alphanumeric string of 1 through 63 characters.

**lma-service lma_name**
Disconnects subscribers using this LMA service configured on this system. `lma_name` must be an existing LMA service expressed as an alphanumeric string of 1 through 63 characters.

**lns ip_address**
Disconnects calls to the peer LNS (L2TP network server) specified by `ip_address` must be specified using IPv4 dotted-decimal notation.

**lns-service name**
Disconnects calls associated with the LNS service named `name`. `name` is an alphanumeric string of 1 through 63 characters.

**long-duration-time-left [ < | > | greater-than | less-than ] value**
Disconnects subscriber sessions whose time left for the maximum duration of their session matches the length of time specified.
`<`: Filters output so that only information less than the specified value is cleared.
`:`: Filters output so that only information greater than the specified value is cleared.
greater-than: Filters output so that only information greater than the specified value is cleared.
less-than: Filters output so that only information less than the specified value is cleared.
`value`: If no other filtering options are specified only output matching `value` is cleared. If `value` is not specified all data is cleared. `value` must be an integer from 0 through 4294967295.
mag-service name
Disconnects subscribers using this Mobile Access Gateway (MAG) service configured on this system. 
name must be an existing MAG service and be from 1 to 63 alphanumeric characters.

max-subscribers max_count [ uniform ]
The maximum number of subscribers to be cleared.
max_count must be an integer from 0 through 20000000.
uniform: Subscribers will be cleared uniformly.

mip-udp-tunnel-only
This option clears the subscribers that negotiated MIP-UDP tunneling with the HA.
This option is only valid when MIP NAT Traversal license is enabled.

mipv6ha-service service_name
Disconnects subscribers using this MIPV6 Home Agent service configured on this system.
service_name must be an existing MIPV6 HA service and be from 1 to 63 alphanumeric characters.

mme-address ipv4_addr
Disconnects subscribers using this peer Mobility Management Entity (MME). ipv4_addr must be an 
existing peer MME IP address entered using IPv4 dotted-decimal notation.

mme-only
Disconnects all MME subscriber sessions on the system.

mme-service name
Disconnects subscribers using this MME service configured on this system. name must be an existing MME 
service expressed as an alphanumeric string1 through 63 characters.

mseg-only

Important: This keyword is not supported in this release.

mseg-service mseg_service_name

Important: This keyword is not supported in this release.

msid id
Disconnects the mobile user identified by ms_id.ms_id must be from 7 to 16 digits specified as an IMSI, 
MIN, or RMI. Wildcard characters $ and * are allowed. The * wildcard matches multiple characters and the $ 
wildcard matches a single character. If you do not want the wildcard characters interpreted as a wildcard 
enclose them in single quotes (‘'). For example; ‘$'.
In case of enforce imsi-min equivalence is enabled on the chassis and MIN or IMSI numbers 
supplied, this filter will clear subscribers with a corresponding MSID (MIN or IMSI) whose lower 10 digits 
matches to lower 10 digits of the supplied MSID.
clear subscribers msid 111110123456789 or
clear subscribers msid 0123456789
will clear any subscriber with a MSID that match the lower 10 digits of MSID supplied, i.e. 0123456789.

msisdn msisdn
Clears information for the mobile user identified by Mobile Subscriber ISDN Number (MSISDN). msisdn must be from 7 to 16 digits specified as an IMSI, MIN, or RMI.

nat { not-required | required [ nat-ip nat_ip_address | nat-realm nat_realm_name ] }
Clears all subscriber information for the specified subscribers:
not-required: Subscribers for whom NAT processing is not required.
required: Subscribers for whom NAT processing is required.

Important: The nat-ip keyword is only available in StarOS 8.3 and later.

nat-ip nat_ip_address: Subscribers for whom NAT processing is enabled and are using the specified NAT IP address. nat_ip_address specifies the NAT IP address using IPv4 dotted-decimal notation.
nat-realm nat_realm_name: Subscribers for whom NAT processing is enabled and are using the specified NAT realm. nat_realm_name specifies the NAT realm name expressed as an alphanumeric string of 1 through 63 characters.

network-requested
Disconnect subscriber sessions that were initiated by the GGSN network requested create PDP context procedure.

network-type { gre | ipv4 | ipv6 | ipip | l2tp | mobile-ip | proxy-mobile-ip }
Disconnects subscriber sessions based on the network type. The following network types can be selected:
• gre: Generic Routing Encapsulation (GRE) per RFC 2784
• ipv4: Internet Protocol version 4 (IPv4)
• ipv6: Internet Protocol version 6 (IPv6)
• ipip: IP-in-IP encapsulation per RFC 2003
• l2tp: Layer 2 Tunneling Protocol encryption per RFC 2661
• mobile-ip: Mobile IP
• proxy-mobile-ip: Proxy Mobile IP

pcf [ < | > | less-than | greater-than ] ipv4_address [ [ < | > | less-than | greater-than ] ipv4_address ]
Displays information for subscribers connected via the packet control function with a specific or range of IP address ipv4_address. The address must be specified using IPv4 dotted-decimal notation.
• <: Filters output so that only information less than the specified IPv4 address value is displayed.
• >: Filters output so that only information greater than the specified IPv4 address value is displayed.
• less-than: Filters output so that only information less than the specified IPv4 address value is displayed.
• greater-than: Filters output so that only information greater than the specified IPv4 address value is displayed.
Note: It is possible to define a limited range of IP addresses by using the less-than and greater-than options to define minimum and maximum values.

```plaintext
pcp { not-required | required }
```

Clears all subscriber information for the specified subscribers:
- **not-required**: Subscribers for whom PCP processing is not required.
- **required**: Subscribers for whom PCP processing is required.

```plaintext
pdsn-service name
```

Disconnect all subscribers connected to the packet data service `pdsn_name`. The packet data service must have been previously configured.

```plaintext
pdg-service service_name
```

Disconnects subscriber sessions that are using the PDG service.
- `service_name` must be an existing service expressed as an alphanumeric string of 1 through 63 characters.

```plaintext
pdif-service service_name
```

Clears counters for subscribers accessing the Packet Data Interworking Function (PDIF) service.
- `service_name` must be an existing service expressed as an alphanumeric string of 1 through 63 characters.

```plaintext
pgw-address ip_address
```

Clears specific P-GW interface.
- `ip_address` must be followed by IP address of interface, using IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

The following filter keywords are valid with this command:

```plaintext
epdg-address,
```

```plaintext
pgw-only { all [ del-cause { none | reactiv-req } ] [ max-subscribers max_count ] | imsi id ebi id | mag-address ip_addr | pgw-service name | sgw-address ip_addr }
```

- **all**: Disconnects all subscribers for all P-GW services on this system.
- **imsi id**: Disconnects subscribers based on their International Mobile Subscriber Identification (IMSI). `id` must be the 3-digit MCC (Mobile Country Code), follow by the 2 or 3 digits of the MNC (Mobile Network Code) and the MSIN (Mobile Subscriber Identification Number).
  - `id` should not exceed 15 digits.
  - Example: 123-45-678910234 must be entered as 12345678910234
- **ebi id**: The EBI (EPS Bearer Identity)
  - `id` must be a valid EBI and be an integer value from 5 to 15.
- **mag-service ip_addr**: Disconnects all subscribers using this MAG address.
- **pgw-service name**: Disconnects all subscribers using this P-GW service.
  - `name` must be an existing P-GW service expressed as an alphanumeric string of 1 through 63 characters.
- **sgw-address ip_addr**: Disconnects all subscribers using this S-GW IP address.
  - `ip_addr` must be an existing IP address entered using IPv4 dotted-decimal notation or IPv6 colon-separated-hexadecimal notation.

```plaintext
plmn-type { home | roaming | visiting }
```

For GGSN, disconnects subscribers whose subscriber type matches the specified type.
clear subscribers

**profile-id id**
Cleans information for subscribers using the granted profile-id for the flow.
_id_ must be an integer from 0 to 4294967295.

**profile-name name**
Cleans information for subscribers using the specified policy profile name.
_name_ must be name of an existing profile expressed as an alphanumeric string of 1 through 63 characters.

**qci number**
Disconnects subscribers based on their QCI identity.
_number_ must be an integer from 0 to 9.

**rulebase rulebase_name**
Cleans information for subscribers using the specified rulebase.
_rulebase_name_ must be name of an existing rulebase expressed as an alphanumeric string of 1 through 63 characters.

**rx-data [ < | > | greater-than | less-than ] value**
Disconnects subscribers who have received the specified number of bytes of data.
_<>: Filters output so that only information less than the specified value is cleared.
_>: Filters output so that only information greater than the specified value is cleared.
_greater-than_: Filters output so that only information greater than the specified value is cleared.
_less-than_: Filters output so that only information less than the specified value is cleared.
_value_: If no other filtering options are specified only output matching value is cleared. If _value_ is not specified all data is cleared. _value_ must be an integer from 0 through 18446744073709551615.

**slu-state { active | idle | idle-active }**
Disconnects subscribers based on their S1-User Plane Protocol State.
_active_: Selects subscribers having S1-U state set to active.
_idle_: Selects subscribers having S1-U state set to idle.
_idle-active_: Selects subscribers having S1-U state set to idle-active.

**s5-proto { gtp | pmip }**
Disconnects subscribers based on their S5 interface protocol type.
_gtp_: Indicates that the GTP protocol is used on the S5 interface for the subscribers being disconnected.
_pmip_: Indicates that the PMIP protocol is used on the S5 interface for the subscribers being disconnected.

**saegw-only { all [ max-subscribers max_count ] | co-located | imsi id ebi id | pgw-anchored | saegw-service name | sgw-address ip_addr | sgw-anchored }**
_all_: Disconnects all subscribers for all SAEGW services on this system.
_co-located_: Disconnects only co-located subscribers which have both S-GW and P-GW functions.
_imsi id_: Disconnects subscribers based on their International Mobile Subscriber Identification (IMSI). _id_ must be the 3-digit MCC (Mobile Country Code), follow by the 2 or 3 digits of the MNC (Mobile Network Code) and the MSIN (Mobile Subscriber Identification Number).
_id_ should not exceed 15 digits.
Example: 123-45-678910234 must be entered as 12345678910234
_ebi id_: The EBI (EPS Bearer Identity)
_id_ must be a valid EBI and be an integer value from 5 to 15.
clear subscribers

**pgw-anchored**: Disconnects only PGW-anchored subscribers.

**saegw-service name**: Disconnects all subscribers using this SAEGW service.

*name* must be an existing SAEGW service expressed as an alphanumeric string of 1 through 63 characters.

**sgw-address ip_addr**: Disconnects all subscribers using this S-GW IP address.

*ip_addr* must be an existing IP address entered using IPv4 dotted-decimal notation or IPv6 colon-separated-hexadecimal notation.

**sgw-anchored**: Disconnects only SGW-anchored subscribers.

---

**saegw-service name**

Disconnects all subscribers using this SAEGW service. *name* must be an existing SAEGW service expressed as an alphanumeric string of 1 through 63 characters.

---

**session-time-left [ < | > | greater-than | less-than ] value**

The amount of time left for the subscriber session.

*<*: Filters output so that only information less than the specified value is cleared.

*>*: Filters output so that only information greater than the specified value is cleared.

*greater-than*: Filters output so that only information greater than the specified value is cleared.

*less-than*: Filters output so that only information less than the specified value is cleared.

*value*: If no other filtering options are specified only output matching *value* is cleared. If *value* is not specified all data is cleared. *value* must be an integer from 0 through 4294967295.

---

**sgsn-address ip_address**

Clears all PDP contexts currently being facilitated by a specific SGSN.

*ip_address* is the IP address of the SGSN entered using IPv4 dotted-decimal notation.

---

**sgsn-service name**

Clears all PDP contexts associated with SGSN. This keyword can be used with filtering keywords that are part of the clear subscriber command set.

Using this keyword can trigger a network-initiated service request (paging) procedure.

*name* identifies a specific SGSN-service configuration expressed as an alphanumeric string of 1 through 63 characters.

---

**sgw-address ip_address**

Disconnects subscribers using the Serving Gateway (S-GW) IP address.

*ip_address* must be specified in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

---

**sgw-only all [ max-subscribers max_count [ uniform ] ] [ verbose ]**

Disconnects all S-GW subscriber sessions on the system.

---

**sgw-service name**

Disconnects subscribers using this Serving Gateway (S-GW) service configured on this system. *name* must be an existing S-GW service expressed as an alphanumeric string of 1 through 63 characters.

---

**smgr-instance sessmgr_instance_number**

Disconnects subscribers on the specified sessmgr instance.

*sessmgr_instance_number* must be an integer from 1 to 4294967295.
clear subscribers

tpo { not-required | required }

**Important:** The Traffic Performance Optimization (TPO) in-line service is not supported in this release.

tax-data { < | > | greater-than | less-than } value

Disconnects subscribers who have transmitted the specified number of bytes of data.

- `<`: Filters output so that only information less than the specified value is cleared.
- `>`: Filters output so that only information greater than the specified value is cleared.
- `greater-than`: Filters output so that only information greater than the specified value is cleared.
- `less-than`: Filters output so that only information less than the specified value is cleared.

**value:** If no other filtering options are specified only output matching value is cleared. If value is not specified all data is cleared. value must be an integer from 0 through 18446744073709551615.

username name

Disconnect the subscriber with the specified username

name is the username of the subscriber to be cleared. name must be a sequence of characters and/or wildcard characters ('$' and '*') from 1 to 127 characters. The * wildcard matches multiple characters and the $ wildcard matches a single character. If you do not want the wildcard characters interpreted as wildcard enclose them in single quotes ('). For example; ‘$’.

verbose

Indicates the output should provide as much information as possible. If this option is not specified then the output is the standard level which is the concise mode.

wsg-service name

Disconnects subscribers using this WSG service configured on this ASR 9000 VSM. name must be an existing WSG (SecGW) service expressed as an alphanumeric string of 1 through 63 characters.

grep grep_options | more

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage

Clear subscribers sessions to aid in troubleshooting the system when no additional subscribers may connect or when a specific service or remote address may be having connection problems. This command may also be used to clear connections when preparing for maintenance activities.

Related commands to clear subscription data - for SGSN use only

- For a 2G SGSN, the admin-disconnect-behavior clear-subscription command in the GPRS Service Configuration mode enables the SGSN to clear subscription data after the administrative disconnect - clear subscribers all has been issued.

- For a 3G SGSN, the admin-disconnect-behavior clear-subscription command in the SGSN Service Configuration mode enables the SGSN to clear subscription data after the administrative disconnect - clear subscribers all has been issued.

Example
The following examples illustrate the basic command usage as well as the redirection of the command output. Not all options are exemplified as all options follow the same basic constructs.

The following are basic subscriber clearing examples:

```
clear subscribers username ser1

clear subscribers ha sampleService

clear subscribers ip-pool pool2 verbose
```

The following command disconnects users connected to the foreign agent with IP address 10.2.3.4.

```
clear subscribers fa 10.2.3.4
```
clear super-charger

Deletes the subscriber’s backed-up subscription data with an SGSN supercharger subscription configuration (3GPP, TS.23.116).

**Product**
SGSN

**Privilege**
Security Administrator, Administrator, Operator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
clear super-charger { imsi | all }
```

**imsi**

Specifies a subscriber’s international mobile subscriber identity (IMSI) number. This 15-digit number includes the MCC (mobile country code), the MNC (mobile network code) and the MSIN (mobile station identification number).

**all**

Instructs the SGSN to delete subscription data for all super charger subscribers.

**Usage**

Use this command to clear (delete) the subscription data records for one or all subscribers within a supercharger subscription configuration.

**Example**

The following command deletes the backed up records for the subscriber identified by the IMSI 90121882144672.

```
clear super-charger imsi 90121882144672
```
clear supplementary-service statistics

Clears the statistics for Supplementary Service Information.

Product
SGSN

Privilege
Security Administrator, Administrator, Operator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local] host_name#

Syntax

clear supplementary-service statistics

Usage
Use this command to clear the Supplementary Service Information.

Example

The following command clears the Supplementary Service Information:

clear supplementary-service statistics
clear task resources

Deletes the collected resource statistics for system tasks.

Product
All

Privilege
Security Administrator, Administrator, Operator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

clear task resources { card card_num { facility facility { all | instance id max } | facility facility { all | instance id max } | max } } card card_num

Default: all powered on cards.
Specifies a single card for which task information is to be cleared where card_num must be from 1 to 48 for the ASR 5000 and 1 through 20 for the ASR 5500.

facility facility { all | instance id max }

Default: all facilities.
Specifies the list of facilities for which task information will be cleared. A specific instance of the facility may be cleared as specified by ID or all instances may be cleared. The value of id must be an integer from 0 through 10000000. facility must be one of:

• a11mgr: A11 Interface Manager facility
• aaamgr: AAA Manager Facility
• aaaproxy: AAA Proxy manager Facility
• acsctrl: Active Charging Service (ACS) Controller Facility [Release 11.0 and earlier versions only]
• acsmgr: Active Charging Service (ACS) Manager Facility
• afctrl: Fabric Manager [ASR 5500 only]
• afmgr: Fabric Manager [ASR 5500 only]
• alcapmgr: Access Link Control Application Part (ALCAP) Manager
• asngwmgmr: ASN Gateway Manager
• asnpcrmgr: ASN Paging/Location-Registry (ASN-PC) Manager
• bfd: Bidirectional Forwarding Detection
• bgp: Border Gateway Protocol (BGP) Facility
• bngmgr: Broadband Network Gateway (BNG) Manager
• bulkstat: Bulk Statistics Manager Facility
• **callhome**: Call Home Controller
• **cbsmgr**: Cell Broadcasting Service (CBS) Manager
• **cdfctrl**: Charging Data Function (CDF) Controller
• **cdfmgr**: CDF Manager
• **cdrmod**: Charging Detail Record (CDR) Module
• **cli**: Command Line Interface (CLI) Facility
• **connproxy**: Proxy for connections from same card/chassis
• **cscfepmgr**: CSCFPMGR Logging Facility
• **cscfmgr**: SIP Call Session Control Function (CSCF) Manager
• **cscfttmgr**: SIP CSCFTT Manager
• **cspctrl**: Card Slot Port controller Facility
• **cssctrl**: Content Service Steering Controller
• **dcardctrl**: IPSec Daughter-card Controller Logging Facility
• **dcardmgr**: IPSec Daughter-card Manager Logging Facility
• **dgmbmgr**: Diameter Gmb Application Manager
• **dhmgr**: Distributed Host Manager
• **diamproxy**: Diameter Proxy
• **drvctrl**: Driver Controller Facility
• **egtpegmgr**: EGTP Egress Demux Manager
• **egtpinmgr**: EGTP Ingress Demux Manager
• **evlogd**: Event Log Daemon Facility
• **famgr**: Foreign Agent Manager Facility
• **gtpcmgr**: GTP-C Protocol Logging facility (GGSN product only)
• **gtpumgr**: GTP-U Demux Manager
• **h248prt**: H.248 Protocol Task [Release 11.0 and earlier versions only]
• **hamgr**: Home Agent Manager Facility
• **hatscp**: High Availability Task CPU Facility
• **hatsystem**: High Availability Task Facility
• **hdctrl**: Hard Disk Controller
• **henbgwdemux**: Home eNodeB Gateway demux manager
• **henbgwmg**: Home eNodeB Gateway Manager
• **hnbgmgr**: HNBGW HNB Manager
• **hwctrl**: Hardware Monitor Controller
• **hwmg**: Hardware Monitor Manager
• **imsimgr**: SGSN IMSI Manager
• **ipsecctr**: IP Security Controller Facility
• **ipsecmgr**: IP Security Manager Facility
• **ipsgmgr**: IP Services Gateway Facility
• **kvctrl**: KV Controller
• **kvmgr**: KV Manager
• **l2tpdemux**: L2TP Demultiplexor (LNS) Facility
• **l2tpmgr**: L2TP Manager Facility
• **lagmgr**: Link Aggregation Group (LAG) Manager
• **linkmgr**: SGSN/SS7 Link Manager
• **magmgr**: Mobile Access Gateway (MAG) Manager
• **megadiammgr**: MegaDiameter Manager
• **mmedemux**: MME Demux Manager logging facility
• **mmemgr**: MME Manager logging facility
• **mmgr**: SGSN/SS7 Master Manager
• **mpls_sig**: Multiprotocol Label Switching
• **mptest**: Migration Performance Test on Packet Accelerator Card
• **netwstrg**: Network Storage Manager [Release 11.0 and earlier versions only]
• **npuctrl**: Network Processor Unit Control Facility
• **npudrv**: Network Processor Unit Driver Facility [ASR 5500 only]
• **npumgr**: Network Processor Unit Manager Facility
• **npusim**: Network Processor Unit Simulator [ASR 5500 only]
• **nputst**: Network Processor Unit Tester
• **nsctrl**: Charging Service Controller [Release 11.0 and earlier versions only]
• **nsmgr**: Charging Service Process Manager [Release 11.0 and earlier versions only]
• **orbs**: Object Request Broker System Facility
• ** ospf**: Open Shortest Path First Facility
• ** ospfv3**: Open Shortest Path First (OSPFv3)
• **pdgmgr**: Packet Data Gateway (PDG) Manager
• **phsgwmgr**: PHS Gateway manager
• **phspemgr**: PHS Paging Controller manager
• **rct**: Recovery Control Task Facility
• **rdt**: Redirect Task Facility
• **rip**: Routing Information Protocol Facility
• **rmctrl**: Resource Manager Controller Facility
• **rmmgr**: Resource Manager Facility
• **sct**: Shared Configuration Task Facility
• **sessctrl**: Session Controller Facility
• **sessmgr**: Session Manager Facility
clear task resources

- **sesstrc**: Session Trace Collection task
- **sft**: Switch Fabric Monitoring Task
- **sgtpcmgr**: SGSN GTP-C Manager
- **sipcdprt**: SIP Call Distributor Task [Release 11.0 and earlier versions only]
- **sitmain**: System Initialization Task Main Facility
- **sitparent**: Card based system initialization facility that applies to packet processing cards and system management cards (SMC - ASR 5000, MIO - ASR 5500) [Replaces the sitpac, sitspe and sittac facilities]
- **snmp**: SNMP Protocol Facility
- **srdb**: Static Rating Database
- **testctr**: Test Controller
- **testmgr**: Test Manager
- **threshold**: Threshold Server Facility
- **vpnctrl**: Virtual Private Network Controller Facility
- **vpnmgr**: VPN Manager Facility
- **zebos**: ZEBOS™ OSPF Message Facility

**all**: Clears information for all instances of the specified facility.

**instance id**: Clears information for the facility instance specified as an integer from 0 through 1000000.

**max**

Default: current usage levels are cleared.
Clears just the maximum usage levels for tasks as opposed to all current usage levels.

**Usage**

Use this command to clear (delete) the collected resource statistics for system tasks.

**Example**

The following command deletes the Switch Fabric Monitoring Task statistics for instance 100 running on card 2.

```
clear task resources card 2 facility sft instance 100 max
```
clear tcap statistics

Deletes the collected statistics for traffic that has passed through the SS7 TCAP (Transaction Capabilities Application Part) layer.

Product
SGSN

Privilege
Security Administrator, Administrator, Operator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

```
clear tcap statistics [ camel-service [ all | name camel_srvc ] | map-service [ all | name map_srvc ] ] [ | { grep grep_options | more } ]
```

- **camel-service [ all | name camel_srvc ]**
  Deletes TCAP statistics for either all CAMEL (Customized Applications for Mobile Network Enhanced Logic, GSM 09.78) services or only for the named CAMEL service.

- **map-service [ all | name mapl_srvc ]**
  Deletes TCAP statistics for either all MAP services or only for the named MAP service.

- **grep grep_options | more**
  Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent. For details on the usage of `grep` and `more`, refer to the `Regulating a Command’s Output` section of the `Command Line Interface Overview` chapter.

Usage
Use this command to clear (delete) the collected TCAP statistics for MAP or CAMEL services.

Example
The following command deletes the collected statistics for a MAP service named `MAP-Tewk`.

```
clear tcap statistics map-service name MAP-Tewk
```
clear wsg-service statistics

Deletes statistics collected for a Wireless Security Gateway (WSG) service.

**Privilege**
Security Administrator, Administrator, Operator

**Product**
SecGW (WSG)

**Mode**
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

**Syntax**

clear wsg-service statistics [ name srvc_name ]

**Usage**

Deletes statistics for all WSG services or for a specified WSG service.

**Example**
The following command deletes statistics for all WSG services:

clear wsg-service
cli

Specifies command line interface (CLI) session behavior.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

[ no ] cli { history | stop-on-first-error | test-commands [encrypted] password password_string }

no
Disables the specified keyword functionality.

history
Enables command line history for the current command line session. Default: Enabled

stop-on-first-error
When enabled and a configuration file is loaded, the system stops loading the configuration file on the first syntax error. Default: Disabled

test-commands [encrypted] password password_string
If you are logged in as a Security Administrator or Administrator enabling this command displays diagnostic commands and supplemental keywords to existing commands. The cli hidden command in Global Configuration mode must be enabled to grant access to this keyword. Default: Disabled

⚠️ Caution: CLI test-commands are intended for diagnostic use only. Access to these commands is not required during normal system operation. These command are intended for use only by Cisco TAC personnel. Some of these commands can slow system performance, drop subscribers, and/or render the system inoperable.

[encrypted] password password_string: Password must be entered to access the CLI test-commands. This password must have been previously configured by a Security Administrator via the Global Configuration mode tech-support test-commands password command. The password is an alphanumeric string of 1 through 64 characters (plain text password) or 1 through 524 characters (encrypted password). If the password keyword is not entered, the user is prompted (no-echo) to enter the password. If tech-support test-commands password has not been enabled, you will be unable to execute cli test-commands.
**Important:** An SNMP trap is generated whenever a user enables `cli test-commands` (StarTestModeEntered). Refer to the *SNMP MIB Reference* for additional information.

Usage

This command controls CLI settings pertaining to the maintenance of a per-session command history and syntax error monitoring during configuration file loading. By default, the system maintains a list of commands executed during each CLI session. This list is referred to as a history.

In addition, the system can be configured to stop loading a configuration if a syntax error is detected. By default, the system identifies the error but continues to process the configuration file.

Example

The following command disables the keeping of a CLI history for the current session:

```plaintext
no cli history
```
clock set

Sets the system time.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

```
clock set date_time
```

`date_time`

Specifies the date and time to set the system clock in the format YYYY:MM:DD:HH:mm or YYYY:MM:DD:HH:mm:ss. Where:

- YYYY = 4-digit year
- MM = 2-digit month in the range 01 through 12
- DD = 2-digit day in the range 01 through 31
- HH = 2-digit hour in the range 00 through 23
- mm = 2-digit minute in the range 00 through 59
- ss = 2-digit second in the range 00 through 59

Usage

Set the clock to adjust the system clock for such things as timing drift, day-light savings adjustment, etc. New settings are immediately applied to all CPUs in the system.

**Important:** This command should only be used if there is no NTP server enabled for any context. If NTP is running on the system, this command returns a failure.

Example

The following commands set the system clock where one sets the exact second as well.

```
clock set 2011:08:05:02:30

clock set 2011:08:05:02:31:30
```
cmp enroll current-cert

Triggers a Certification Request (CR) after generating a public and private key pair, as well as an X.509 certificate to be included in the CR for a second certificate from the same Certificate Authority (CA). This is a Certificate Management Protocol v2 command.

**Product**

All products supporting IPSec CMPv2 features

**Important:** This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

**Privilege**

Security Administrator

**Mode**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name# 
```

**Syntax**

```
cmp enroll current-cert old-cert-name modulus mod_type subject-name "subject_string" 
cert-name name ca-root ca_name ca-url url 
```

- **current-cert old-cert-name**
  Specifies a valid security gateway certificate as an alphanumeric string of 1 through 129 characters.

- **modulus mod_type**
  Specifies the modulus of the generated certificate. `mod_type` is one of the following integers: 1024, 2048, 4096 or 512.

- **subject-name "subject_string"**
  Specifies the subject string of the certificate in double quotation marks. "subject_string" is an alphanumeric string of 1 through 256 characters.

- **cert-name name**
  Specifies the name of the newly obtained certificate which also serves as the filename to be stored on /flash disk. `name` is an alphanumeric string of 1 through 129 characters.

- **ca-root ca_name**
  Specifies the root certificate of the CA server. `ca_name` is an alphanumeric string of 1 through 129 characters.
ca-url url

Specifies the URL to which the CA server listens. url is in the format: http://<host>[:<port>]/<directory>/<filename>.

Usage

Use this command to trigger a certification request for a second certificate from the same CA.

Example

The following command requests a second certificate from the same CA:

    cmp enroll current-cert aqaw12345 modulus 1024 subject-name "test_certificate" cert-name cert01 ca-root ca001 ca-url http://excel:2033/certificates/aqaw12345
cmp fetch cert-name

This command is only applicable for the ASR 9000 running VPC-SI on a Virtualized Services Module (VSM). CMPv2 operations are performed only on one VSM in the chassis. The certificates along with the private key file and the root certificate are stored on the supervisor card. When invoked on other VSMs in the chassis, this command reads the certificate, private key and the root certificate from the supervisor card.

Product
All products supporting IPSec CMPv2 features

⚠️ Important: This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

Privilege
Security Administrator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

```
cmp fetch current-cert old-cert-name ca-root ca_name
```

- **current-cert old-cert-name**
  Specifies a valid security gateway certificate as an alphanumeric string of 1 through 129 characters.

- **ca-root ca_name**
  Specifies the root certificate of the CA server. `ca_name` is an alphanumeric string of 1 through 129 characters.

Usage
Use this command to read the certificate, private key and the root certificate from the supervisor card in an ASR 9000.

Example
The following command fetches a certificate from a specified CA:

```
cmp fetch current-cert aqaw12345 ca-root ca001
```
cmp initialize

Triggers an Initial Certification Request (CR) after generating a public and private key pair, as well as an X.509 certificate to be included in the CR. This is a Certificate Management Protocol v2 command.

Product

All products supporting IPSec CMPv2 features

⚠️ Important: This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

Privilege

Security Administrator

Mode

Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

```
cmp initialize modulus mod_type cert-name name subject-name "subject_string" ca-psk key ca-root ca_name ca-url url
```

- **modulus mod_type**
  Specifies the modulus of the generated certificate. `mod_type` is one of the following integers: 1024, 2048, 4096 or 512.

- **cert-name name**
  Specifies the name of the newly obtained certificate which also serves as the filename to be stored on /flash disk. `name` is an alphanumeric string of 1 through 129 characters.

- **subject-name "subject_string"**
  Specifies the subject string of the certificate in double quotation marks. "subject_string" is an alphanumeric string of 1 through 256 characters.

- **ca-psk key**
  Specifies the Pre-Shard Key provided by the CA server for CMPv2 operation. `key` is an alphanumeric string of 1 through 129 characters.

- **ca-root ca_name**
  Specifies the root certificate of the CA server. `ca_name` is an alphanumeric string of 1 through 129 characters.
**ca-url url**

Specifies the URL to which the CA server listens. *url* is in the format:
http://<host>[:<port>]/[<directory>]/<filename>.

**Usage**

Use this command to trigger an initial certification request from the CA.

**Example**

The following command sends an Initial Certification Request to a specified CA:

```
cmp initialize modulus 1024 cert-name cert001 subject-name "test" ca-psk
AB33569 ca-root cert1 ca-url http://excel:2033/certificates/aqaw12345
```
**cmp poll**

Triggers a pollReq for the specified certificate. This is a Certificate Management Protocol v2 command.

**Product**

All products supporting IPSec CMPv2 features

**Important**: This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

**Privilege**

Security Administrator

**Mode**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
cmp poll current-cert old-cert-name
```

```
current-cert old-cert-name
```

Specifies a valid security gateway certificate as an alphanumeric string of 1 through 129 characters.

**Usage**

Use this command to poll the current certificate.

**Example**

The following command polls the current certificate:

```
cmp poll current-cert aqaw12345
```
cmp update

Triggers a Key Update Request after generating a public and private key pair, as well an X.509 certificate to be included in the Key Update Request for a certificate that is about to expire. This is a Certificate Management Protocol v2 command.

Product

All products supporting IPSec CMPv2 features

Important: This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

Privilege

Security Administrator

Mode

Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

```
cmp update current-cert old-cert-name modulus mod_type ca-root ca_name ca-url url
```

```
modulus mod_type
Specifies the modulus of the generated certificate. `mod_type` is one of the following integers: 1024, 2048, 4096 or 512.
```

```
current-cert old-cert-name
Specifies a valid security gateway certificate as an alphanumeric string of 1 through 129 characters.
```

```
ca-root ca_name
Specifies the root certificate of the CA server. `ca_name` is an alphanumeric string of 1 through 129 characters.
```

```
ca-root ca_name
Specifies the root certificate of the CA server. `ca_name` is an alphanumeric string of 1 through 129 characters.
```

```
ca-url url
Specifies the URL to which the CA server listens. `url` is in the format: http://<host>[:<port>][/<directory>]/<filename>.
```

Usage

Usage

Example

Use this command to initiate a manual update of the current certificate.
The following command requests a second certificate from the same CA:

```plaintext
cmp update modulus 1024 current-cert aqaw12345 ca-root ca001 ca-url http://excel:2033/certificates/aqaw12345
```
commandguard

Enable / disable Commandguard feature to prevent operators from accidentally entering configuration modes by presenting yes/no confirmation prompts.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

commandguard

[ default | no ] commandguard

[ default | no ]
Restores the default behavior for confirmation prompting and disables the Commandguard feature.

Usage

When commandguard is enabled it affects the configure and autoconfirm CLI commands by causing them to prompt (Y/N) for confirmation. This feature protects operators from accidentally entering configuration mode via CLI or file replay.

> **Important**: When autoconfirm is enabled, commandguard has no affect.

Example

The following command enables the Commandguard feature:

commandguard

The following command restores system default confirmation prompts:

default commandguard

The following command instructs the SGSN to ignore Commandguard when enabled:

autoconfirm
configure

Sets the mode to the global configure mode. May also be used to set the mode to the configure mode and pre-load the configuration referred to by the options.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec
The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
configure [ url [ verbose ] ]
```

*url*

Specifies the location of a configuration file to pre-load. *url* may refer to a local or a remote file. *url* must be entered using the following format:

For the ASR 5000:

- `{ file: }{ /flash | /pcmcia | /hd } [ /directory ]/file_name`
- `{ tftp://{ host[ :port# ] } [ /directory ]/file_name`
- `{ http: | ftp: | sftp: }//{ username [ :password ] @ } { host } [ :port# ] [ /directory ]/file_name`

For the ASR 5500:

- `{ file: }{ /flash | /usb1 | /hd } [ /directory ]/file_name`
- `{ tftp://{ host[ :port# ] } [ /directory ]/file_name`
- `{ http: | ftp: | sftp: }//{ username [ :password ] @ } { host } [ :port# ] [ /directory ]/file_name`

**Important**: Use of the SMC hard drive is not supported in this release.

**Important**: Do not use the following characters when entering a string for the field names below: “/” (forward slash), “.” (colon) or “@” (at sign).

- `directory` is the directory name.
- `filename` is the actual file of interest.
- `username` is the user to be authenticated.
- `password` is the password to use for authentication.
- `host` is the IP address or host name of the server.
- `port#` is the logical port number that the communication protocol is to use.
**verbose**

Displays the line number and actual line content from the configuration as it is processed.

---

**Usage**

If no URL is specified, executing this command causes the CLI to enter the Global Configuration Mode. If a URL is specified, executing this command loads the specified configuration file.

**Example**

The following simply changes the mode to the command line interface global configuration mode.

```
configure
```

The following command loads a configuration file from the node `sampleNode` given the path specified and a local file, respectively.

```
configure ftp://sampleNode/pub/glob.cfg
```

For the ASR 5000:

```
configure /pcmcia1/pub/glob.cfg verbose
```

For the ASR 5500:

```
configure /usb1/pub/glob.cfg verbose
```
context

Sets the current context to the context specified.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

context name

name
Specifies the context of interest as an alphanumeric string of 1 through 79 characters. Must be a previously defined context.

Usage
Change the current context when it is desired to configure and/or manage a specific context.

Example
The following sets the current context to the sampleContext context.

context sampleContext
**copy**

Copies files from one location to another. Allows files to be copied to/from locally, as well as from one remote location to another.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Mode**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
copy from_url to_url [ passive ] [ -noconfirm ]
```

- **from_url**
  - Specifies the source of the copy. `url` may refer to a local or a remote file. `url` must be entered using the following format:
  - For the ASR 5000:
    - `file: { /flash | /pcmcia1 | /hd-raid }{ /directory }/file_name`
    - `tftp:// { host[:port#] }{ /directory }/file_name`
    - `{ http: | ftp: | sftp: }// { username [ :password ]@ } { host }{ :port# }{ /directory }/file_name`
  - For the ASR 5500:
    - `file: { /flash | /usb1 | /hd-raid }{ /directory }/file_name`
    - `tftp:// { host[:port#] }{ /directory }/file_name`
    - `{ http: | ftp: | sftp: }// { username [ :password ]@ } { host }{ :port# }{ /directory }/file_name`

**Important:** Use of the ASR 5000 SMC hard drive is not supported in this release.

**Important:** Do not use the following characters when entering a string for the field names below: “/” (forward slash), “:” (colon) or “@” (at sign).

- `directory` is the directory name.
- `filename` is the actual file of interest.
- `username` is the user to be authenticated.
- `password` is the password to use for authentication.
- `host` is the IP address or host name of the server.
- `port#` is the logical port number that the communication protocol is to use.
to_url

Specifies the destination of the copy. url may refer to a local or a remote file. url must be entered using the following format:

For the ASR 5000:

- `[ file: ]{ /flash | /pcmcia1 | /hd-raid }[ /directory ] /file_name
- `tftp://{ host[ :port ] } [ /directory ] /file_name

For the ASR 5500:

- `[ file: ]{ /flash | /usb1 | /hd-raid }[ /directory ] /file_name
- `tftp://{ host[ :port ] } [ /directory ] /file_name

**Important:** Use of the SMC hard drive is not supported in this release.

directory is the directory name.
filename is the actual file of interest.
username is the user to be authenticated.
password is the password to use for authentication.
host is the IP address or host name of the server.
port# is the logical port number that the communication protocol is to use.

**passive**

Indicates the file copy is to use the passive mode FTP.

**-noconfirm**

Executes the command without any additional prompt and confirmation from the user.

**Important:** Use of the **-noconfirm** option allows the over writing of an existing file if the destination file already exists.

**Usage**

Copy configuration files, log files, etc., to provide backups of data through the network.

**Example**

For the ASR 5000, the following copies files from the local `/flash/pub` directory to remote node remoteABC's `/pcmcia2/pub` directory with and without confirmation respectively.

```
copy http://remoteABC/pub/june.cfg /flash/pub/june.cfg

copy tftp://remoteABC/pub/june.cfg /pcmcia2/pub/june.cfg -noconfirm
```

For the ASR 5500, the following copies files from the local `/flash/pub` directory to remote node remoteABC's `/flash/pub` directory with and without confirmation respectively.

```
copy http://remoteABC/pub/june.cfg /flash/pub/june.cfg
```
copy tftp://remoteABC/pub/june.cfg /flash/pub/june.cfg -noconfirm

The following copies files from remote node remoteABC to remote node remote123.

copy ftp://remoteABC/pub/may.cfg ftp://remote123/pub/may.cfg
crash copy

Copies individual crash files (one-at-a-time) and optionally the core dump file from the stored crash records on the chassis to a user-specified location.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

```
crash copy number number url to_url [ core ]
```

<table>
<thead>
<tr>
<th>number number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the identification number of the crash record as an integer representing a valid record number from 1 through 120. To determine the numeric identity of a specific crash file, use the <code>show crash list</code> command in Exec mode.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>url to_url</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the destination of the copy. <code>url</code> may refer to a local or a remote file and must be entered using the following format:</td>
</tr>
</tbody>
</table>

For the ASR 5000:

```
*tftp://( host[ :port# ] ) [ /directory ] /
*{ ftp: | sftp: }//( username [ :password ] 0 ) { host } [ :port# ] [ /directory ] /
```

For the ASR 5500:

```
*tftp://( host[ :port# ] ) [ /directory ] /
*{ ftp: | sftp: }//( username [ :password ] 0 ) { host } [ :port# ] [ /directory ] /
```

<table>
<thead>
<tr>
<th>directory:</th>
</tr>
</thead>
<tbody>
<tr>
<td>the name of the target directory.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>username:</th>
</tr>
</thead>
<tbody>
<tr>
<td>the username to be authenticated to provide access to targeted server.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>password:</th>
</tr>
</thead>
<tbody>
<tr>
<td>the username’s password to be authenticated.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>host:</th>
</tr>
</thead>
<tbody>
<tr>
<td>the IP address or host name of the targeted server.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>port#:</th>
</tr>
</thead>
<tbody>
<tr>
<td>the number of the target server’s logical port used for the selected communication protocol.</td>
</tr>
</tbody>
</table>

Important: Use of the SMC hard drive is not supported in this release.
## crash copy

**Important:** Do not specify a target filename as this will prevent the file from writing to the target server. The system generates and provides a timestamp-based filename that appears at the destination when the `copy` command completes.

### core

Copies the core dump to the targeted storage server. The core cannot be copied alone; it must be part of a `crash copy` action included when copying a crash file.

### Usage

Copy crash files of core dump to another location for backup or analysis.

### Example

The following uses FTP to copy stored record number 5 and the core dump from the crash record list to a targeted remote node directory called `crasharchive` through port 22 of the targeted server `remoteABC` with access through user `homeboy` whose password is `secret.7.word`.

```
crash copy number 5 url ftp://homeboy:secret.7.word@remoteABC:22/crasharchive/ core
```
crypto blacklist file update

Updates the blacklist (access denied) file using the path specified when the blacklist was enabled.

**Product**
All products supporting IPSec crypto blacklisting

**Important:** This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

**Privilege**
Security Administrator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
crypto blacklist file update
```

**Usage**

Update the blacklist file. For additional information on blacklisting, refer to the *System Administration Guide*.

**Example**

The following command updates the blacklist file:

```
crypto blacklist file update
```
crypto rsa-keygen modulus

Generates an RSA key pair and Certificate Signing Request (CSR) using information to authenticate the site.

**Product**
All products that support IPSec

**Important:** This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

**Privilege**
Security Administrator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local] host_name#
```

**Syntax**

```
crypto rsa-keygen modulus { 1024 | 2048 | 4096 | 512 }
```

**Usage**
Generate an RSA key pair and Certificate Signing Request (CSR) using information to authenticate the site. You can specify the modulus (key size of the generated certificate) as 512, 1024, 2048 or 4096 bits. A CSR is a message sent to a Certification Authority (CA) to request a public key certificate for an entity, where the entity is the subject of the certificate. The software creating the CSR must first generate an RSA key pair; the key pair comprises a public and private key. The public key is bundled with the subject's name, and other information to form the CSR.

**Example**
The following command generates a CSR for a certificate with a modulus of 2048 bits:

```
crypto rsa-keygen modulus 2048
```
crypto whitelist file update

Updates the whitelist (access granted) file using the path specified when the whitelist was enabled.

**Product**

All products supporting IPSec crypto whitelisting

**Important:** This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

**Privilege**

Security Administrator

**Mode**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
crypto whitelist file update
```

**Usage**

Update the whitelist file. For additional information on whitelisting, refer to the *System Administration Guide*.

**Example**

The following command updates the whitelist file:

```
crypto whitelist file update
```
crypto-group

Allows the manual switchover of redundant IPSec tunnels belonging to a specific crypto group.

Product
PDSN
GGSN

Privilege
Security Administrator, Administrator, Operator

Mode
Exec
The following prompt is displayed in the Exec mode:

[local] host_name#

Syntax

crypto-group name group_name activate { primary | secondary }

name group_name
Specifies the name of an existing crypto group with which the tunnels to be switched are associated.

activate { primary | secondary }
Allows you to specify which tunnel to activate:
- primary: Switches traffic to the primary tunnel in the group.
- secondary: Switches traffic to the secondary tunnel in the group.

Usage
This command is used in conjunction with the Redundant IPSec Tunnel Fail-over feature. Use this command to manually switch traffic to a specific tunnel in a crypto group if the automatic switchover options have been disabled. Refer to the switchover command in the Crypto Group configuration mode for more information.

Example
The following command manually switches user traffic to the secondary tunnel in the crypto group called group1:

crypto-group group1 activate secondary
Chapter 125
Exec Mode Commands (D-S)

This chapter contains the commands in the Exec Mode from debug to system.

The Exec Mode is the initial entry point into the command line interface system. Exec mode commands are useful in troubleshooting and basic system monitoring.

Mode

Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
debug

The following commands send information to the logging facility for review:

- debug bfd
- debug ip
- debug ip bgp
- debug ip ospf all
- debug ip ospf event
- debug ip ospf ism
- debug ip ospf lsa
- debug ip ospf nsm
- debug ip ospf packet
- debug ip ospf route
- debug ip ospf router
- debug ipv6 ospf all  (OSPFv3)
- debug ipv6 ospf event  (OSPFv3)
- debug ipv6 ospf ifsm  (OSPFv3)
- debug ipv6 ospf lsa  (OSPFv3)
- debug ipv6 ospf nsm  (OSPFv3)
- debug ipv6 ospf packet  (OSPFv3)
- debug ipv6 ospf route  (OSPFv3)
**debug bfd**

Enables or disables the debug options for Bidirectional Forwarding Detection (BFD) debugging. If logging is enabled, results are sent to the logging system.

**Product**

All

**Privilege**

Security Administrator, Administrator, Operator

**Mode**

Exec

The following prompt is displayed in the Exec mode:

`[local] host_name#`

**Syntax**

```
[ no ] debug bfd { all | events ipc-error | ipc-events | nsm | packet | session }
```

- **no**
  Indicates the IP debugging is to be disabled for the IP interfaces/function specified.

- **bfd | interface name | route**
  Specifies which IP interfaces/function to debug.
  - **all**: enables debug for all BFD items.
  - **events**: enables debug for BFD events.
  - **ipc-error**: enables debug for BFD Inter-process communication (IPC) errors.
  - **ipc-events**: enables debug for BFD Inter-process communication (IPC) events.
  - **nsm**: enables debug for BFD Network Service Manager messages.
  - **packet**: enables debug for BFD packets.
  - **session**: enables debug for BFD sessions.

**Usage**

The debug bfd command is valuable when troubleshooting network problems with BFD-enabled BGP routers. The debugging is stopped by using the **no** keyword.

⚠️ **Caution:** Issuing this command could negatively impact system performance depending on system configuration and/or loading.

**Example**

The following commands enable/disable debugging for BFD.

```
dump bfd
no debug bfd
```
**debug ip**

Enables or disables the debug options for IP debugging. If logging is enabled, results are sent to the logging system.

**Product**
All

**Privilege**
Security Administrator, Administrator, Operator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
[ no ] debug ip { arp | interface | route }
```

- **no**
  Indicates the IP debugging is to be disabled for the IP interfaces/function specified.

- **arp | interface name | route**
  Specifies which IP interfaces/function to debug.
  - **arp**: indicates debug is to be enabled for the address resolution protocol.
  - **interface**: indicates debug is to be enabled for the IP interfaces.
  - **route**: indicates debug is to be enabled for the route selection and updates.

**Usage**
The debug IP command is valuable when troubleshooting network problems between nodes. The debugging is stopped by using the **no** keyword.

**Caution:** Issuing this command could negatively impact system performance depending on system configuration and/or loading.

**Example**
The following commands enable/disable debugging for ARP.

```
debug ip arp
no debug ip arp
```

The following enables/disables debugging for IP interfaces.

```
debug ip interface
no debug ip interface
```

The following enables/disables debugging for routing.

```
debug ip route
no debug ip route
```
**debug ip bgp**

Enables or disables BGP (Border Gateway Protocol) debug flags. If logging is enabled, results are sent to the logging system.

**Product**

HA

**Privilege**

Security Administrator, Administrator, Operator

**Mode**

Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

**Syntax**

```plaintext
[ no ] debug ip bgp { all | event | filters | fsm | keepalives | updates { inbound | outbound } }
```

- **no**
  Disables the specified BGP debug flags.

- **all**
  Enables all BGP debug flags.

- **event**
  Enables debugging of all BGP protocol events.

- **filters**
  Enables debugging of all BGP filters.

- **fsm**
  Enables debugging of BGP Finite State Machine

- **keepalives**
  Enables debugging of all BGP keepalives.

- **updates {inbound | outbound}**
  Enables debugging of BGP updates.
  - **inbound**: Debug all BGP inbound updates.
  - **outbound**: Debug all BGP outbound updates.

**Usage**

Use this command to enable or disable BGP debug flags.
Example

The following command disables all BGP debug flags enabled by any of the `debug ip bgp` commands:

```
no debug ip bgp all
```

The following command enables all BGP debug flags:

```
depug ip bgp all
```
**debug ip ospf all**

Enables or disables all OSPF (Open Shortest Path First) debug flags. If logging is enabled, results are sent to the logging system.

**Product**
- PDSN
- HA
- GGSN

**Privilege**
- Security Administrator, Administrator, Operator

**Mode**
- Exec

The following prompt is displayed in the Exec mode:

```plaintext
[local] host_name#
```

**Syntax**

```
[ no ] debug ip ospf all
```

- **no**
  
  Disable all OSPF debug flags.

**Usage**

Use this command to enable or disable all OSPF debug flags.

**Example**

The following command disables all OSPF debug flags enabled by any of the `debug ip ospf` commands:

```
no debug ip ospf all
```

The following command enables all OSPF debug flags:

```
dump ip ospf all
```
**debug ip ospf event**

Enables or disables debugging of OSPF protocol events. If logging is enabled, results are sent to the logging system. If no keywords are specified, all events are enabled for debugging.

**Product**
- PDSN
- HA
- GGSN

**Privilege**
- Security Administrator, Administrator, Operator

**Mode**
- Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```  

**Syntax**

```
[ no ] debug ip ospf event [ abr | asbr | vl | lsa | os | router ]
```

- **no**
  
  Disables debugging the specified OSPF event. If no keywords are specified, all events are disabled.

- **abr**
  
  Enables debugging of Area Border Router (ABR) events.

- **asbr**
  
  Enables debugging of Autonomous System Boundary Router (ASBR) events.

- **vl**
  
  Enables debugging of Virtual Link (VL) events.

- **lsa**
  
  Enables debugging of link state advertisement (LSA) events.

- **os**
  
  Enables debugging of operating system (OS) events.

- **router**
  
  Enables debugging of router events.

**Usage**

Use this command to output debug information for OSPF events.
Example

To enable all event debug information, enter the following command;

```
debug ip ospf event
```

To disable all event debug information, enter the following command;

```
no debug ip ospf event
```
**debug ip ospf ism**

Enables or disables OSPF Interface State Machine (ISM) troubleshooting, based on ISM information type. If no keywords are specified all ISM information types are enabled. If logging is enabled, results are sent to the logging system.

**Product**
- PDSN
- HA
- GGSN

**Privilege**
- Security Administrator, Administrator, Operator

**Mode**
- Exec

The following prompt is displayed in the Exec mode:

```
[local] host_name#
```

**Syntax**

```
[ no ] debug ip ospf ism [ events | status | timers ]
```

- **no**
  - Disables debugging the specified ISM information. If no keywords are specified, all information is disabled.

- **events**
  - Enables debugging ISM event information.

- **status**
  - Enables debugging ISM status information.

- **timers**
  - Enables debugging ISM timer information.

**Usage**

Use this command to output ISM debug information.

**Example**

To enable all ISM debug information, enter the following command:

```
dump ism
```

To disable all ISM debug information, enter the following command:

```
no debug ism
```
**debug ip ospf lsa**

Enables or disables troubleshooting on OSPF Link State Advertisements (LSAs), based on the specific LSA option. If no keywords are specified, all options are enabled. If logging is enabled, results are sent to the logging system.

**Product**

PDSN
HA
GGSN

**Privilege**

Security Administrator, Administrator, Operator

**Mode**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
[ no ] debug ip ospf lsa [ flooding | generate | install | refresh | maxage | refresh ]
```

- **no**
  
  Disables the specified LSA debug information. If no keyword is specified, all LSA debug information is disabled.

- **flooding**
  
  Enables LSA flooding information.

- **generate**
  
  Enables LSA generation information.

- **install**
  
  Enables LSA install information.

- **maxage**
  
  Enables LSA maximum age information in seconds. The maximum age is 3600 seconds.

- **refresh**
  
  Enables LSA refresh information.

**Usage**

Use this command to output debug information for LSAs.

**Example**

To enable all LSA debug information, enter the following command:
**debug ip ospf lsa**

To disable all LSA debug information, enter the following command:

```
no debug ip ospf lsa
```
**debug ip ospf nsm**

Enables or disables troubleshooting OSPF Neighbor State Machines (NSMs), based on the specific NSM information type. If no keyword is specified, all NSM information types are enabled. If logging is enabled, results are sent to the logging system.

**Product**
PDSN
HA
GGSN

**Privilege**
Security Administrator, Administrator, Operator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
[ no ] debug ip ospf nsm [ status | events | timers ]
```

- **no**
  Disables the debugging the specified NSM information type. If no keyword is specified, all information types are disabled.

- **events**
  Enables debugging NSM event information.

- **status**
  Enables debugging NSM status information.

- **timers**
  Enables debugging NSM timer information.

**Usage**

Use this command to output debug information for OSPF NSMs

**Example**

To enable all NSM debug information, enter the following command;

```
dump ip ospf nsm
```

To disable all NSM debug information, enter the following command;

```
no debug ip ospf nsm
```
debug ip ospf packet

Enables or disables troubleshooting of specific OSPF packet information. If logging is enabled, results are sent to the logging system.

Product
- PDSN
- HA
- GGSN

Privilege
Security Administrator, Administrator, Operator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

[ no ] debug ip ospf packet { all | dd | hello | ls-ack | ls-request | ls-update } [ send | recv ] [ detail ]

- **no**
  Disable debugging of the specified packet information.

- **all**
  Enables debugging all OSPF packet information.

- **dd**
  Enables debugging database descriptions.

- **hello**
  Enables debugging hello packets.

- **ls-ack**
  Enables debugging link state acknowledgements.

- **ls-request**
  Enables debugging link state requests.

- **ls-update**
  Enables debugging link state updates.

- **send**
  Enables debugging only on sent packets.
### debug ip ospf packet

**recv**

Enables debugging only on received packets.

**detail**

Enables detailed information in the debug output.

---

**Usage**

Use this command to output specific OSPF packet information.

**Example**

To enable all packet debug information, enter the following command;

```
depth ip ospf packet all
```

To disable all route debug information, enter the following command;

```
no debug ip ospf packet all
```
debug ip ospf route

Sets the route calculation method to use in debugging OSPF routes. If no route calculation method is specified, all methods are enabled. If logging is enabled, results are sent to the logging system.

Product
PDSN
HA
GGSN

Privilege
Security Administrator, Administrator, Operator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local] host_name#

Syntax

[ no ] debug ip ospf route [ ase | ia | install | spf ]

- **no**
  - Disables debugging of route information. If no keyword is specified all information types are disabled.

- **ase**
  - Enables debugging information on autonomous system external (ASE) route calculations.

- **ia**
  - Enables debugging information on Inter-Area route calculations.

- **install**
  - Enables debugging information on route installation.

- **spf**
  - Enables debugging information on Shortest Path First (SPF) route calculations.

Usage
Use this command to output debug information for OSPF routes.

Example
To enable all route debug information, enter the following command:

```
    debug ip ospf route
```

To disable all route debug information, enter the following command:

```
    no debug ip ospf route
```
debug ip ospf router

Sets the debug option for OSPF router information. If no keyword is specified, all router information is enabled. If logging is enabled, results are sent to the logging system.

Product
- PDSN
- HA
- GGSN

Privilege
- Security Administrator, Administrator, Operator

Mode
- Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

[ no ] debug ip ospf router [ interface | redistribute ]

- no
  Disables the specified router debug information. If no keyword is specified, all router information is disabled.

- interface
  Enables router interface information.

- redistribute
  Enables router redistribute information.

Usage

Use this command to output debug information for the OSPF router.

Example

To enable all router debug information, enter the following command;

   debug ip ospf router

To disable all router debug information, enter the following command;

   no debug ip ospf router
**debug ipv6 ospf all**

Enables or disables all OSPFv3 (Open Shortest Path First Version 3) debug flags. If logging is enabled, results are sent to the logging system.

**Product**
- PDSN
- HA
- GGSN

**Privilege**
- Security Administrator, Administrator, Operator

**Mode**
- Exec

The following prompt is displayed in the Exec mode:

```
[local] host_name#
```

**Syntax**

```
[ no ] debug ipv6 ospf all
```

- **no**
  - Disable all OSPFv3 debug flags.

**Usage**

Use this command to enable or disable all OSPFv3 debug flags.

**Example**

The following command disables all OSPFv3 debug flags enabled by any of the `debug ip ospf` commands:

```
no debug ipv6 ospf all
```

The following command enables all OSPFv3 debug flags:

```
debug ipv6 ospf all
```
**debug ipv6 ospf event**

Enables or disables debugging of OSPFv3 protocol events. If logging is enabled, results are sent to the logging system. If no keywords are specified, all events are enabled for debugging.

**Product**
- PDSN
- HA
- GGSN

**Privilege**
- Security Administrator, Administrator, Operator

**Mode**
- Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
[ no ] debug ipv6 ospf event [ abr | asbr | os | router ]
```

- **no**
  
  Disables debugging the specified OSPFv3 event. If no keywords are specified, all events are disabled.

- **abr**
  
  Enables debugging of Area Border Router (ABR) events.

- **asbr**
  
  Enables debugging of Autonomous System BOundary Router (ASBR) events.

- **os**
  
  Enables debugging of operating system (OS) events.

- **router**
  
  Enables debugging of router events.

**Usage**

Use this command to output debug information for OSPFv3 events.

**Example**

To enable all event debug information, enter the following command:

```
debug ipv6 ospf event
```

To disable all event debug information, enter the following command:

```
no debug ipv6 ospf event
```
**debug ipv6 ospf ifsm**

Enables or disables OSPFv3 Interface State Machine (ISM) troubleshooting, based on ISM information type. If no keywords are specified all ISM information types are enabled. If logging is enabled, results are sent to the logging system.

**Product**
- PDSN
- HA
- GGSN

**Privilege**
- Security Administrator, Administrator, Operator

**Mode**
- Exec

The following prompt is displayed in the Exec mode:

```
[local] host_name#
```

**Syntax**

```
[ no ] debug ipv6 ospf ism [ events | status | timers ]
```

- **no**
  - Disables debugging the specified ISM information. If no keywords are specified, all information is disabled.

- **events**
  - Enables debugging ISM event information.

- **status**
  - Enables debugging ISM status information.

- **timers**
  - Enables debugging ISM timer information.

**Usage**

Use this command to output ISM debug information.

**Example**

To enable all ISM debug information, enter the following command:

```
debug ipv6 ospf ism
```

To disable all ISM debug information, enter the following command:

```
no debug ipv6 ospf ism
```
debug ipv6 ospf lsa

Enables or disables troubleshooting on OSPFv3 Link State Advertisements (LSAs), based on the specific LSA option. If no keywords are specified, all options are enabled. If logging is enabled, results are sent to the logging system.

Product

PDSN
HA
GGSN

Privilege

Security Administrator, Administrator, Operator

Mode

Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

[ no ] debug ip ospf lsa [ flooding | generate | install | maxage | refresh ]

- **no**
  
  Disables the specified LSA debug information. If no keyword is specified, all LSA debug information is disabled.

- **flooding**
  
  Enables LSA flooding information.

- **generate**
  
  Enables LSA generation information.

- **install**
  
  Enables LSA install information.

- **maxage**
  
  Enables LSA maximum age information in seconds. The maximum age is 3600 seconds.

- **refresh**
  
  Enables LSA refresh information.

Usage

Use this command to output debug information for LSAs.

Example

To enable all LSA debug information, enter the following command;
debug ipv6 ospf lsa

To disable all LSA debug information, enter the following command:

no debug ipv6 ospf lsa
debug ipv6 ospf nsm

Enables or disables troubleshooting OSPFv3 Neighbor State Machines (NSMs), based on the specific NSM information type. If no keyword is specified, all NSM information types are enabled. If logging is enabled, results are sent to the logging system.

Product
- PDSN
- HA
- GGSN

Privilege
Security Administrator, Administrator, Operator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

[ no ] debug ipv6 ospf nsm [ interface | redistribute ]

no
Disables the debugging the specified NSM information type. If no keyword is specified, all information types are disabled.

interface
Enables debugging NSM on this interface.

redistribute
Enables debugging NSM redistribution information.

Usage
Use this command to output debug information for OSPFv3 NSMs

Example
To enable all NSM debug information, enter the following command;

d debug ipv6 ospf nsm

To disable all NSM debug information, enter the following command;

no debug ipv6 ospf nsm
debug ipv6 ospf packet

Enables or disables troubleshooting of specific OSPFv3 packet information. If logging is enabled, results are sent to the logging system.

Product
PDSN
HA
GGSN

Privilege
Security Administrator, Administrator, Operator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local] host_name#

Syntax
[ no ] debug ipv6 ospf packet { dd | hello | ls-ack | ls-request | ls-update } [ recv | send ] [ detail ]

- no
  Disable debugging of the specified packet information.

- dd
  Enables debugging database descriptions.

- hello
  Enables debugging hello packets.

- ls-ack
  Enables debugging link state acknowledgements.

- ls-request
  Enables debugging link state requests.

- ls-update
  Enables debugging link state updates.

- recv
  Enables debugging only on received packets.

- send
  Enables debugging only on sent packets.
**detail**

Enables detailed information in the debug output.

**Usage**

Use this command to output specific OSPFv3 packet information.

**Example**

To enable all packet debug information, enter the following command;

```
debug ipv6 ospf packet all
```

To disable all route debug information, enter the following command;

```
no debug ipv6 ospf packet all
```
**debug ipv6 ospf route**

Sets the route calculation method to use in debugging OSPFv3 routes. If no route calculation method is specified, all methods are enabled. If logging is enabled, results are sent to the logging system.

**Product**
PDSN
HA
GGSN

**Privilege**
Security Administrator, Administrator, Operator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
[ no ] debug ipv6 ospf route [ ase | ia | install | spf ]
```

- **no**
  
  Disables debugging of route information. If no keyword is specified all information types are disabled.

- **ase**
  
  Enables debugging information on autonomous system external (ASE) route calculations.

- **ia**
  
  Enables debugging information on Inter-Area route calculations.

- **install**
  
  Enables debugging information on route installation.

- **spf**
  
  Enables debugging information on Shortest Path First (SPF) route calculations.

**Usage**

Use this command to output debug information for OSPF routes.

**Example**

To enable all route debug information, enter the following command:

```
debug ipv6 ospf route
```

To disable all route debug information, enter the following command:

```
no debug ipv6 ospf route
```
default terminal

Restores the system default value for the terminal options.

**Product**
All

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

**Syntax**

```
default terminal { length | width }
```

| length | width
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>length: Resets the terminal length to the system default.</td>
<td>width: Resets the system default terminal width.</td>
</tr>
</tbody>
</table>

**Usage**

Restore the default terminal settings when the current paging and display wraps inappropriately or pages to soon.

**Example**

The following sets the default length then width in two commands.

```
default terminal length

default terminal width
```
**delete**

Removes the specified file(s) permanently from the local.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

**Syntax**

```
delete filepath [ -noconfirm ]
```

*filepath*

Specifies the location of the file to rename. The path must be formatted as follows:

For the ASR 5000:

```
[ file: ]{ /flash | /pcmcia1 | /hd-raid }[ /directory ]/file_name
```

**Important:** Use of the ASR 5000 SMC hard drive is not supported in this release.

For the ASR 5500:

```
[ file: ]{ /flash | /usb1 | /hd-raid }[ /directory ]/file_name
```

**Important:** Do not use the following characters when entering a string for the field names below: "/" (forward slash), "::" (colon) or "@" (at sign).

*directory is the directory name
filename is the actual file of interest

- *-noconfirm*

Executes the command without any additional prompt and confirmation from the user.

**Important:** Use of the -noconfirm option should be done with extra care to ensure the file is specified accurately as there is no method of recovering a file that has been deleted.
Usage
Deleting files is a maintenance activity which may be part of periodic routine procedures to reduce system space utilization.

Example
The following removes files from the local /flash/pub directory.

```
delete /flash/pub/june03.cfg
```
delete support record

Removes a Support Data Record (SDR) with s specified record-id or all SDRs in the specified range of record-ids.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
delete support record <record-id> [ to <record-id> ]
```

*record-id*

Specifies a single SDR as an integer from 0 to 65536. Each SDR is identified by a time index called the record-id. For example, the most recent record is always record-id 0 (filename = sdr.0.gz). The next older record is record-id 1 (filename = sdr.1.gz), and so on.

*to record-id*

Specifies the endpoint record-id when deleting a range of SDRs.

**Usage**

Use this command to delete one or more SDRs stored on the system. For additional information on the Support Data Collector feature, refer to the System Administration Guide.

**Example**

The following command deletes the SDR with a record-id of 5 (filename = sdr.5.gz):

```
delete support record 5
```
dhcp force

Tests the lease-renewal for DHCP-assigned IP addresses for a particular subscriber.

Product

- GGSN
- ASN-GW
- P-GW
- SAEGW

Privilege

Security Administrator, Administrator, Operator

Mode

Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

`dhcp force lease-renewal { callid id | imsi imsi [ nsapi nsapi ] | msid msid }

- **callid id**
  Clear the call ID specified as a 4-byte hexadecimal number.

- **imsi msid**
  Disconnects the subscriber with the specified msid. The IMSI (International Mobile Subscriber Identity) ID is a 50-bit field which identifies the subscriber’s home country and carrier. Wildcard characters $ and * are allowed. The * wildcard matches multiple characters and the $ wildcard matches a single character. If you do not want the wildcard characters interpreted as a wildcard enclose them in single quotes (‘ ’). For example; ‘$’.

- **nsapi nsapi**
  Specifies a Network Service Access Point Identifier (NSAPI) an integer from 5 to 15.

- **msid msid**
  Disconnects the mobile user identified by `ms_id.ms_id` must be from 7 to 16 digits specified as an IMSI, MIN, or RMI. Wildcard characters $ and * are allowed. The * wildcard matches multiple characters and the $ wildcard matches a single character. If you do not want the wildcard characters interpreted as a wildcard enclose them in single quotes (‘ ’). For example; ‘$’.

Usage

Use this command tests a forced IP address lease renewal for a specific subscriber.

Example

The following command tests DHCP lease renewal for a subscriber with an MSID of 1234567:

```
dhcp force lease-renewal msid 1234567
```
dhcp test

Tests DHCP (Dynamic Host Configuration Protocol) functions for a particular DHCP service.

Product

GGSN
ASN-GW
P-GW
SAEGW

Privilege

Security Administrator, Administrator, Operator

Mode

Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

```plaintext
dhcp test dhcp-service svc_name [ all | server ip_address ]
```

- **dhcp-service svc_name**

  Specifies the name of the DHCP service as an alphanumeric string of 1 through 63 characters that is case sensitive.

- **all**

  Tests DHCP functionality for all servers.

- **server ip_address**

  Tests DHCP functionality for the server specified by an IP address entered using IPv4 dotted-decimal notation.

Usage

Once DHCP functionality is configured on the system, this command can be used to verify that it is configured properly and that it can successfully communicate with the DHCP server.

Executing this command causes the system to request and allocate an IP address and then release it. If a specific DHCP server is not specified, then each server configured in the service is tested.

Example

The following command tests the systems ability to get an IP address from all servers a DHCP service called **DHCP-Gi** is configured to communicate with:

```plaintext
dhcp test dhcp-service DHCP-Gi all
```
diameter disable endpoint

Disables a Diameter endpoint without removing the peer’s configuration.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
diameter disable endpoint endpoint_name peer peer_id
```

- **endpoint_name**
  Specifies the endpoint in which the peer is configured as an alphanumeric string of 1 through 63 characters.

- **peer peer_id**
  Specifies the Diameter peer host name to be disabled as an alphanumeric string of 1 through 63 characters.

**Usage**

Use this command to administratively disable a Diameter peer without removing the peer configuration. This command will tear down all connections on the specified peer (by sending a DPR if the configuration demands the same at peer level configuration). The peer will remain in disabled state until it is enabled again. Also see the `diameter enable endpoint` command.

**Example**

This command disables the Diameter peer `peer12`:

```
diameter disable endpoint endpoint1 peer peer12
```
diameter enable endpoint

Enables a Diameter endpoint that is disabled.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name# 
```

**Syntax**

```
diameter enable endpoint  endpoint_name  peer  peer_id
```

- **endpoint_name**
  Specifies the endpoint in which the peer is configured as an alphanumeric string of 1 through 63 characters.

- **peer peer_id**
  Specifies the Diameter peer host name to be enabled as an alphanumeric string of 1 through 63 characters.

**Usage**

Use this command to administratively enable a Diameter peer. Also see the `diameter disable endpoint` command.

**Example**

This command enables the Diameter peer `peer12`:

```
diameter enable endpoint endpoint1 peer peer12
```
**diameter reset connection**

Resets individual TCP/SCTP connections for a specified Diameter endpoint.

**Product**
All

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
diameter reset connection { endpoint endpoint_name peer peer_id }
```

- **endpoint endpoint_name**
  Resets connection to the endpoint specified as an alphanumeric string of 1 through 63 characters.

- **peer peer_id**
  Resets connection to the Diameter peer host name specified as an alphanumeric string of 1 through 63 characters.

**Usage**

Use this command to reset the TCP/SCTP connections for the specified endpoint/peer. With this command, the connection will be closed temporarily after DPR/DPA. If there is any traffic to be sent to the particular peer, then the connection will be re-established.

This command overrides the endpoint configured in any other configuration mode.

This command is applicable only when the specified peer is enabled.

**Example**

This command resets connection to the endpoint named **test123**:

```
diameter reset connection endpoint test123
```
**diameter reset route failure**

Resets the failed route status of a Diameter destination-host combination via peer to AVAILABLE status.

**Product**
All

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local] host_name#
``` 

**Syntax**

```
diameter reset route failure [ endpoint endpoint_name ] [ host host_name ] [ peer peer_id ]
```

**endpoint endpoint_name**

Resets paths to the endpoint specified as an alphanumeric string of 1 through 63 characters.

**host host_name**

Resets the FAILED status of all Diameter destination-host combination routes via peer for every Diameter client within the chassis having a specific host name to AVAILABLE.

Specifies the Diameter host name as an alphanumeric string of 1 through 63 characters.

**peer peer_id**

Resets the FAILED status of all Diameter destination-host combination routes via a peer having specific peer Id for every Diameter client within the chassis to AVAILABLE.

Specifies the Diameter peer host name as an alphanumeric string of 1 through 63 characters.

**Usage**

Use this command to reset the FAILED status of all Diameter destination-host combination routes via peer for every Diameter client within the chassis to AVAILABLE status.

This command also resets the failure counts used to determine the AVAILABLE/FAILED status of a destination-host combination.

When executed from local context, this command matches all contexts. If an optional keyword is not supplied, a wildcard is used for the value.

The status of every matching combination of destination-host via peer for every matching Diameter client within the chassis will be reset to AVAILABLE. The failure counts that are used to determine AVAILABLE/FAILED status will also be reset.

Also see the `route-entry` and `route-failure` commands in the **Diameter Endpoint Configuration Mode Commands** chapter.

Default value: N/A

**Example**
The following command resets the FAILED status of all Diameter destination-host combination routes via peer for every Diameter client within the chassis for specified endpoint name to AVAILABLE.

```
diameter reset route failure endpoint endpoint123
```
**directory**

Lists the files in a specified location.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
directory filepath [ -size ] [ -reverse ] [ -time ]
```

*filepath*

Specifies the directory path to list the contained files using the following format:

For the ASR 5000:

```
[ file: ]{ /flash | /pcmcia1 | /hd }[ /directory ]/file_name
```

**Important:** Use of the ASR 5000 SMC hard drive is not supported in this release.

For the ASR 5500:

```
[ file: ]{ /flash | /usb1 | /hd }[ /directory ]/file_name
```

**Important:** Do not use the following characters when entering a string for the field names below: “/” (forward slash), “:” (colon) or “@” (at sign).

*directory* is the directory name

*filename* is the actual file of interest

- **size**

  Indicates the size of each file should be displayed in the output.

- **reverse**

  Indicates the order of files listed should be in descending order (z-aZ-A9-0). Default is to sort in ascending order (0-9A-Za-z).

- **time**

  Indicates the last modification timestamp of each file should be displayed in the output.
Usage

Lists such things as log and crash files from multiple nodes within the network. The optional arguments may be specified individually or in any combination.

Example

The following command will list the files in the local /flash/pub directory sorted in reverse order.

```
directory /flash/pub -reverse
```
disable radius

Prevents the system from making requests of a selected RADIUS server.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local] host_name#

Syntax

disable radius { [ charging ] [ accounting ] server ipv4/ipv6_address [ group group_name | port port_number + ] }

[charging] [ accounting ]
Specifies the type of RADIUS server to disable.
- accounting: Specifies accounting servers
- charging: Specifies charging servers
- charging accounting: Specifies charging accounting servers

server ipv4/ipv6_address
Specifies the RADIUS server by IP address entered using IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

port port_number
Specifies the port number of the RADIUS server being disabled an integer from 0 through 65535. Default: 1812 (authentication) 1813 (accounting)

group group_name
Specifies the RADIUS group to which the server belongs as an alphanumeric string of 1 through 63 characters. Use this option in the event that the RADIUS server belongs to multiple groups and you only want to disable the server within the specific group. Default: default

Usage
Use this command to gracefully stop the system from making requests of a specific RADIUS server.

Example
The following command disables a RADIUS accounting server with an IP address of 10.2.3.4, the default accounting server port number, and that resides in the Group5 server group:

    disable radius accounting server 10.2.3.4 group Group5
**dns-client**

Performs DNS (Domain Name System) query on the basis of specified DNS client name, DNS query domain name, and type of query criteria.

**Product**
All

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
dns-client  dns_client_name  [  query-type  {  A  |  AAAA  |  NAPTR  |  SRV  }  ]  query-name
query_domain_name
```

- **dns-client  dns_client_name**
  Specifies the name of the DNS client whose cache and/or statistics are to be queried. It must be an existing DNS client expressed as an alphanumeric string of 1 through 64 characters.

- **query-type  {  A  |  AAAA  |  NAPTR  |  SRV  }  ]**
  Specifies that the type of query to perform for the defined DNS client is to be displayed.
  - **A**: Filters DNS results based on domain IPv4 address records (A records). This is the default query type.
  - **AAAA**: Filters DNS results based on domain IPv6 address records (AAAA records).
  - **NAPTR**: Filters DNS results based on Naming Authority Pointer records (NAPTR).
  - **SRV**: Filters DNS results based on service host records (SRV records).

- **query-name  query_domain_name**
  Filters the DNS results based on the query domain name expressed as an alphanumeric string of 1 through 255 characters.  
  **query_domain_name** is the domain name used to perform the DNS query and is different from the actual domain name which is resolved. For example, to resolve the SIP server for service.com, the query name is `_sip._udp.service.com` and the query type is **SRV**.

**Usage**

Use this command to perform DNS query on the basis of DNS Client name and filters the query results based on query type and query name. This command also populates the result into DNS Cache. This command used the current context to DNS request.

**Example**

The following command displays statistics for a DNS client named **test_dns** with query type for IP address as **A** and query name as **domain1.com**.
dns-client test_dns query-type A query-name domain1.com
egtpc test echo

Tests the ability of a GGSN/P-GW service to exchange GTP-C echo request messages with specified peer(s).

**Product**
- GGSN
- P-GW
- SAEGW

**Privilege**
Operator, Config-Administrator, Administrator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
egtpc test echo gtp-version version src-address ip_address { all | peer-address ip_address }
```

<table>
<thead>
<tr>
<th><strong>gtp-version version</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies version number for sending Echo request message.</td>
</tr>
<tr>
<td><em>version</em> must be an integer from 0 through 2.</td>
</tr>
</tbody>
</table>

**Important:** If peer is not a new peer for service bind to *src-address*, then echo request is sent with the last known highest version of the peer.

<table>
<thead>
<tr>
<th><strong>src-address ip_address</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the IP address of a Gn interface configured on the system.</td>
</tr>
<tr>
<td><em>ip_address</em> must be entered using IPv4 dotted-decimal notation or IPV6 colon-separated-hexadecimal notation.</td>
</tr>
</tbody>
</table>

**Important:** The IP address of the system’s Gn interface must be bound to a configured GGSN/P-GW service prior to executing this command.

<table>
<thead>
<tr>
<th><strong>all</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Sends GTP-C echo requests to first 100 peers that currently have sessions with the GGSN/P-GW service.</td>
</tr>
</tbody>
</table>

**Important:** If this keyword is selected, additional confirmation is required after the following message, “Warning: Due to possibility of huge number of connected peers, considering system performance impacts, issue echo request to only 100 peers”.

---

Cisco ASR 5x00 Command Line Interface Reference

3859
**peer-address ip_address**

Specifies that GTP-C echo requests will be sent to a specific peer.

*ip_address* must be entered using IPv4 dotted-decimal notation or IPv6 colon-separated-hexadecimal notation.

**Usage**

This command tests the GGSN’s or P-GW’s ability to exchange GPRS Tunneling Protocol control plane (GTP-C) packets with the specified peer. This command is useful for troubleshooting and/or monitoring. This command must be executed from within the context in which the GGSN/P-GW service is configured.

**Important:** In StarOS v14.0 and later, this command replaces the *gtpv0 test echo* and *gtpc test echo* commands.

**Example**

The following command issues GTP-C echo packets from a GGSN service bound to address 192.168.157.43 to an SGSN with an address of 192.168.1.52:

```
egtpc test echo gtp-version 1 src-address 192.168.157.43 peer-address 192.168.1.52
```
enable radius

Enables the system to start making requests of a specific RADIUS server.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Mode**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
enable radius { [ charging ] [ accounting ] server ipv4/ipv6_address [ group group_name | port port_number + ] }
```

- **[ charging ] [ accounting ]**
  Specifies the type of RADIUS server to enable.
  - **accounting**: Specifies accounting servers
  - **charging**: Specifies charging servers
  - **charging accounting**: Specifies charging accounting servers

- **server ipv4/ipv6_address**
  Specifies the RADIUS server by an IP address entered using IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

- **port port_number**
  Specifies the port number of the RADIUS server being enabled as an integer from 0 through 65535. Default: 1812 (authentication) 1813 (accounting)

- **group group_name**
  Specifies the RADIUS group to which the server belongs as an alphanumeric string of 1 through 63 characters. Use this option in the event that the RADIUS server belongs to multiple groups and you only want to disable the server within the specific group. Default: default

**Usage**

Use this command to allow the system to start making requests of a specific RADIUS server.

**Example**

The following command enables a RADIUS accounting server with the IP address 10.2.3.4, the default accounting server port number, and in the Group5 server group:

```
enable radius accounting server 10.2.3.4 group Group5
```
exit

Terminates the current CLI session.

**Product**
All

**Privilege**
Any

**Syntax**
```
exit
```

**Usage**
Use this command to terminate the current CLI session.
filesystem

Use this command to check, format or repair the filesystem on internal and external storage devices.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

For the ASR 5000:

```bash
filesystem { check | format | repair | synchronize } { /flash | /pcmcial | /hd-raid } [ card slot_num ]
```

For the ASR 5500:

```bash
filesystem { check | format | repair | synchronize } { /flash | /usb1 | /hd-raid } [ card slot_num ]
filesystem { check | format | repair | synchronize | update } { /flash | /hd-raid | /usb1 | /usb2 | cdrom1 }
```

The following devices are supported based on platform type:

- /flash – ASR 5x00, VPC
- /hd-raid – ASR 5x00, VPC
- /pcmcia1 – ASR 5000 only
- /usb1 – ASR 5500, VPC (if configured via hypervisor)
- /usb2 – VPC (if configured via hypervisor)
- /cdrom1 – VPC (if configured via hypervisor)

<table>
<thead>
<tr>
<th>check</th>
</tr>
</thead>
<tbody>
<tr>
<td>Checks for filesystem corruption.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>format</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reformats file system.</td>
</tr>
</tbody>
</table>

⚠️ **Caution:** This keyword erases all data on the device.
Formatting /flash will remove all boot configurations and the ASR 5x00 chassis-ID. Before running format, be sure to review or save the output of the `show boot` command. After running `format`, be sure to restore boot entries as needed, generate a new chassis-ID, and execute `save configuration` to save the running configuration.

---

**repair**

Repairs file system corruption.

---

**synchronize**

See the description of the `filesystem synchronize` command for detailed information. **Not supported on VPC-SI.**

---

**update**

Updates the boot code on the file system. **Supported on VPC-SI only.**

---

**Usage**

Check, format, or repair all directories and files from on an internal or external storage device and re-establish the file system.

---

**Example**

The following command formats the PCMCIA card located in slot 1 on the SMC (ASR 5000):

```
filesystem format /pcmcia1
```
filesystem synchronize

Use this command to synchronize the file systems of active and standby storage devices on management cards or VPC-DI Control Function (CF) virtual machines.

**Product**
All

**Privilege**
Security Administrator, Administrator, Operator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name# 
```

**Syntax**

For the ASR 5000:

```
filesystem synchronize [ /flash | /pcmcia1 | all ] [ checkonly ] [ from card_num | to card_num ] [-noconfirm]
```

For the ASR 5500:

```
filesystem synchronize [ /flash | /usb1 | all ] [ checkonly ] [ from card_num | to card_num ] [-noconfirm]
```

For VPC:

```
filesystem synchronize [ /flash | /usb1 | /usb2 | cdrom1 | all ] [ checkonly ] [ from card_num | to card_num ] [-noconfirm]
```

The following devices are supported based on platform type:
- */flash* – ASR 5x00, VPC
- */hd-raid* – ASR 5x00, VPC
- */pcmcia1* – ASR 5000 only
- */usb1* – ASR 5500, VPC (if configured via hypervisor)
- */usb2* – VPC (if configured via hypervisor)
- */cdrom1* – VPC (if configured via hypervisor)
- */all* – Selects all file systems

**checkonly**

Checks for file system corruption; does not modify file systems.

```
[ from card_num | to card_num ]
```

Copies files from a source card to a destination card specified by slot numbers.
-noconfirm

Executes the command without displaying “are you sure” prompts.

Usage

Synchronize the file systems between active and standby storage devices.

Example

The following command all file systems on system management cards:

```
filesystem synchronize all
```

The following command sequence appears when `filesystem synchronize /flash` is run after `save configuration /flash/FILENAME-redundant` is executed and a change has been made to the configuration:

```
filesystem synchronize /flash
2 to be updated on card 2
    /flash/oam.cfg
    /flash/service.cfg
0 to be updated (but are newer) on card 2
0 to be deleted on card 2
Are you sure? [Yes|No]:
```

You must confirm the synchronization before it will be initiated.
If “No files to update” appears, you are returned to the CLI prompt.
get context-list

Generates an XML-formatted list of all currently configured contexts within the system.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

get context-list [ | { grep grep_options | more } ]

| { grep grep_options | more }

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage

Generates a list of all currently configured contexts in XML format. The output can be copied and pasted into compatible applications.

Example

```
get context-list
```
get ip

Generates an XML-formatted display of IPv4-based information.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

```
configure
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
get ip { access-list | arp [vrf name] | bgp neighbors | interface [vrf name] | ospf { interface | neighbor | vrf name | route [vrf name] | vrf } [ | { grep grep_options | more } ] }
```

- **access-list**
  Generates an XML-formatted display of all IPv4 Access Control Lists (ACLs).

- **arp**
  Generates an XML-formatted display of all Allocation Retention Priorities (ARPs) or the ARPs for the named Virtual Routing and Forwarding (VRF) table.

- **bgp neighbors**
  Generates an XML-formatted display of all Border Gateway Protocol (BGP) neighbors.

- **interface [vrf name]**
  Generates an XML-formatted display of all interfaces or for only those associated with a specified VRF table (optional).

- **ospf { interface | neighbor | vrf name }**
  Generates an XML-formatted display of all Open Shortest Path First (OSPF) routing information.

  - **interface**: Displays interface information for OSPF.
  - **neighbor**: Displays summarized information about all known OSPF neighbors.
  - **vrf name**: Displays information for the named VRF table.

- **route [vrf name]**
  Generates an XML-formatted display of all IPv4-based routes or for only those associated with a specified VRF table (optional).
**vrf**

Generates an XML-formatted display of all VRF tables.

```
| { grep grep_options | more }
```

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of `grep` and `more`, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter.

**Usage**

Generates a display of IPv4-based information in XML format. The output can be copied and pasted into compatible applications.

**Example**

```
get ip access-list
```
get ipv6

Generates an XML-formatted display of IPv6-based information.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[l]ocal]host_name(config)#

Syntax

get ip { access-list | interface [vrf name] | ospf { interface | neighbor } | route [vrf name] } [ | { grep grep_options | more } ]

access-list
Generates an XML-formatted display of all IPv6 Access Control Lists (ACLs).

interface [vrf name]
Generates an XML-formatted display of all IPv6 interfaces or for only those associated with a specified VRF table (optional).

ospf { interface | neighbor }
Generates an XML-formatted display of all Open Shortest Path First version 3 (OSPFv3) routing information.

• interface: Displays interface information for OSPFv3.
• neighbor: Displays summarized information about all known OSPFv3 neighbors.

route [vrf name]
Generates an XML-formatted display of IPv6 routes or for only those associated with a specified VRF table (optional).

| { grep grep_options | more }

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage
Generates a display of IPv6-based information in XML format. The output can be copied and pasted into compatible applications.
Example

```
get ipv6 access-list
```
get port info

Generates an XML-formatted display for all physical ports or a specific port in the system.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration

configure
Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax
get port info [slot/port] [ | { grep grep_options | more } ]

slot/port
Generates an XML-formatted display of information for the port specified by its chassis slot and card port number.

| { grep grep_options | more }
Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage
Generates a display of IP-based information in XML format. The output can be copied and pasted into compatible applications.

Example

get ip port
gtpc test echo

Tests the ability of a GGSN service to exchange GTP-C echo request messages with the specified SGSN(s).

Product
GGSN

Privilege
Security Administrator, Administrator, Operator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

```
gtpc test echo src-address gn_address { all | sgsn-address ip_address }
```

<table>
<thead>
<tr>
<th>src-address</th>
<th>gn_address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the IP address of a Gn interface configured on the system in IPv4 dotted-decimal notation.</td>
<td></td>
</tr>
</tbody>
</table>

**Important:** The IP address of the system’s Gn interface must be bound to a configured GGSN service prior to executing this command.

<table>
<thead>
<tr>
<th>all</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies that GTP-C echo requests will be sent to all SGSNs that currently have sessions with the GGSN service.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>sgsn-address</th>
<th>ip_address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies that GTP-C echo requests will be sent to a SGSN specified by an IP address in IPv4 dotted-decimal notation.</td>
<td></td>
</tr>
</tbody>
</table>

Usage

This command tests the GGSN’s ability to exchange GPRS Tunneling Protocol control plane (GTP-C) packets with the specified SGSNs. This command is useful for troubleshooting and/or monitoring. This command must be executed from within the context in which the GGSN service is configured. Refer also to the `gtpu test` command.

**Important:** In StarOS v14.0 and later, this command has been replaced by the `egtpc test echo` command.

Example

The following command issues GTP-C echo packets from a GGSN service bound to address 192.168.157.32 to an SGSN with an address of 192.168.157.2:

```
gtpc test echo src-address 192.168.157.32 sgsn-address 192.168.157.2
```
**gtpp interim now**

Check points current GTPP accounting messages and identifies which types of interim CDRs are to be generated and sent to the external charging/storage servers (for example, a CFG or a GSS). The impact of this command is immediate.

**Product**

- GGSN
- SGSN
- SGW

**Privilege**

Security Administrator, Administrator, Operator

**Mode**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
gtpp interim now [ active-charging egcdr | apn apn_name | callid call_id | cdr-types { gcdr | mcdr | scdr } | dhcp-server ip_address | gprs-service svc_name | ggsn-address ggsn_ip_addr | ggsn-service svc_name | imsi imsi [ ip-address sub_address [ username name ] ] | ip-address sub-address | nsapi nsapi [ ip-address sub-address [ username name ] ] | ip-pool pool_name | mcc mcc_number mnc mnc_number | msisdn msisdn_num | sgsn-address ip_address | sgsn-service svc_name | username name ] +
```

**active-charging**

This feature is specific to the GGSN and is documented separately.

---

**apn apn_name**

Initiates GTPP interim accounting for all PDP contexts accessing the APN specified as an alphanumeric string of 1 through 62 characters that is case sensitive.

---

**callid call_id**

Identifies a specific call id as an 8-digit hexadecimal number.

---

**cdr-types { mcdr | scdr }**

Specifies the CDR types to be generated by the SGSN:

- **gcdr** - Instructs the GGSN to only generate G-CDRs.
- **mcdr** - Instructs the SGSN to only generate M-CDRs
- **scdr** - Instructs the SGSN to only generate S-CDRs.

This keyword is specific to the SGSN.

---

**dhcp-server ip_address**

Identifies the DHCP server where the IP address (defined with the **ip address** keyword) was allocated by the IP address of the DHCP server entered using IPv4 dotted-decimal notation.
**ggsn-address ggsn_ip_addr**

Specifies the IP address of the interface to the GGSN using IPv4 dotted-decimal notation. This keyword is specific to the GGSN.

**ggsn-service svc_name**

Initiates GTPP interim accounting for all PDP contexts currently being facilitated by the GGSN service specified as an alphanumeric string of 1 through 63 characters that is case sensitive. This keyword is specific to the GGSN.

**gprs-service svc_name**

Initiates GTPP interim accounting for all PDP contexts currently being facilitated by an existing GPRS service specified as an alphanumeric string of 1 through 63 characters that is case sensitive. This keyword is specific to the SGSN.

**imsi { imsi [ ip-address sub_address [ username name ] ] | nsapi nsapi [ ip-address sub-address [ username name ] ] | username name ]**

Initiates GTPP interim accounting for a specific International Mobile Subscriber Identity (IMSI) number. The request could be further filtered using any of the following keywords:

- **ip-address**: Interim accounting will be performed for the IP address specified by `sub_address`. The command can be further filtered by specifying a specific username with that address.

- **nsapi**: Interim accounting will be performed for a Network Service Access Point Identifier (NSAPI) specified as an integer from 5 to 15. The command can be further filtered by specifying a specific ip address and/or a username with that address, or just a specific username.

**ip-address sub_address [ username name ]**

Initiates GTPP interim accounting for the IP address of the subscriber specified in IPv4 dotted-decimal notation. The command can be further filtered by specifying a username with that address. The name is the subscriber's name and can be a sequence of characters and/or wildcard characters ('$' and '*') from 1 to 127 characters. The * wildcard matches multiple characters and the $ wildcard matches a single character. If you do not want the wildcard characters interpreted as wildcard enclose them in single quotes ('). For example; *$'.

**ip-pool pool_name**

Initiates GTPP interim accounting for all PDP contexts that were allocated IP addresses from an existing pool specified as an alphanumeric string of 1 through 31 characters that is case sensitive. This keyword is applicable to the GGSN only.

**mcc mcc_number mnc mnc_number**

- **mcc_number**: Specifies the mobile country code (MCC) portion of the PLMN identifier and can be configured to any 3-digit integer value between 100 and 999.

- **mnc_number**: Specifies the mobile network code (MNC) portion of the PLMN identifier and can be configured to any 2- or 3-digit integer between 00 and 999.

**msisdn msisdn_num**

Configures the SGSN to include the Mobile Subscribers Integrated Services Digital Network identifier in generated CDRs (M-CDRs and/or the S-CDRs). This keyword is applicable for SGSN only.
GTPp interim now

**msisdn_number** must be followed by a valid MSISDN number, consisting of 1 to 15 digits.

**sgsn-address** *ip_address*

Initiates GTPP interim accounting for all PDP contexts currently being facilitated by the SGSN specified by an IP address in IPv4 dotted-decimal notation. This keyword is specific to the GGSN.

**sgsn-service** *svc_name*

Initiates GTPP interim accounting for all PDP contexts currently being facilitated by an existing SGSN service specified an alphanumeric string of 1 through 63 characters that is case sensitive. This keyword is specific to the SGSN.

**username** *name*

Initiates GTPP interim accounting for all PDP contexts for the subscriber name specified as an alphanumeric string of 1 through 127 characters that is case sensitive.

More than one of the above keywords can be entered within a single command.

**Usage**

This command causes GTPP accounting CDRs to immediately be generated for all active sessions that are in the current context. If executed within the local context, CDRs will be generated for all active sessions regardless of context. This command generates only certain types of CDRs including GCDRs, SGWCDRs, and SCDRs.

The sending of the CDRs is paced so as not to overload the accounting server.

**Example**

The following command causes CDRs to immediately be generated:

```
gtpp interim now
```
gtpp interim now active-charging egcdr

Check points current GTPP accounting messages for active charging immediately.

Product
GGSN

Privilege
Security Administrator, Administrator, Operator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

```
gtpp interim now active-charging egcdr [ callid call_id | imsi imsi | msid msid | rulebase rbase_name | session-id sess_id | username name ]
```

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>callid</td>
<td>Initiates GTPP interim accounting for a session for the call ID specified as an 8-digit hexadecimal number.</td>
</tr>
<tr>
<td>imsi</td>
<td>Initiates GTPP interim accounting for a International Mobile Subscriber Identity (IMSI) number. specified as a sequence of hexadecimal digits and wildcard characters - $ matches a single character and * matches multiple characters</td>
</tr>
<tr>
<td>msid</td>
<td>Initiates GTPP interim accounting for a Mobile Station Identifier (MSID) number specified as a sequence of up to 24 digits and wildcard characters - $ matches a single character and * matches multiple characters</td>
</tr>
<tr>
<td>rulebase</td>
<td>Initiates GTPP interim accounting for sessions that use the named active charging rulebase specified as an alphanumeric string of 1 through 24 characters.</td>
</tr>
<tr>
<td>session-id</td>
<td>Initiates GTPP interim accounting for a current active charging session.</td>
</tr>
</tbody>
</table>

Usage

This command causes GTPP accounting eG-CDRs to immediately be generated for active charging sessions that meet the specified criteria. The sending of the CDRs is paced so as not to overload the accounting server.

username name

Initiates GTPP interim accounting for all PDP contexts for the subscriber name specified as an alphanumeric string of 1 through 127 characters that is case sensitive.
Example

The following command causes eG-CDRs to immediately be generated for active charging sessions using the rulebase named rulebase1:

```
gtpp interim now active-charging egcdr rulebase rulebase1
```
gtpp storage-server commit

Causes the GTPP storage server to archive all buffered packets.

Product
GGSN
P-GW
SAEGW

Privilege
Security Administrator, Administrator, Operator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

`gtpp storage-server commit now [ group name group_name ]`

**Usage**

This command sends a request to the GTPP Storage Server to archive all buffered packets. It also deletes all CDRs that have been acknowledged by the charging gateway function (CGF). The deleted CDRs are saved in a separate file.

Note that this command must be executed from within the context in which the GTPP Storage Server is configured.

Refer to the `gtpp storage-server` command in the *Context Configuration Mode Commands* chapter for more information.
**gtpp storage-server streaming start**

This command enables to start streaming of the copied CDR files from active chassis when the ICSR switchover occurs.

**Product**
- GGSN
- P-GW
- S-GW
- SGSN

**Privilege**
- Security Administrator, Administrator, Operator

**Mode**
- Exec

The following prompt is displayed in the Exec mode:

```
[local] host_name#
```

**Syntax**

```
gtpp storage-server streaming start [ group name group_name ]
```

**group name group_name**

Specifies the name of a GTTP group configured in the current context as an alphanumeric string of 1 through 63 characters.

Note that, if the group name is not specified, then all the GTTP groups in the current context will be considered. If the group name is specified, then only the group provided in this CLI command will be considered.

**Usage**

This command is used to resynchronize the CDRs left on local HDD with the active GTTP' streaming feed to transfer the CDRs from active chassis to IT mediation device during ICSR switchover.

Note that this CLI command must be executed from within the context in which the GTTP Storage Server is configured.

In the event of ICSR switchover, to transfer the copied CDRs from active chassis to IT mediation device, follows these steps:

1. Manually copy files from old active chassis to new active chassis.
2. Issue this CLI command “gtpp storage-server streaming start” to start streaming of the copied files from active chassis.
3. If the streaming is in progress, then wait till the current file is fully streamed out. After the current file is fully streamed out, then rebuild the file list (to get the copied CDR files) and start streaming based on the timestamp.
4. If the streaming is not in progress then rebuild the file list (to get the copied CDR files) and start streaming.
gtpp test

Tests communication with configured charging gateway function (CGF) servers or a GTPP Storage-Server.

Product
GGSN
P-GW
SAEGW

Privilege
Operator, Config-Administrator, Administrator

Mode
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

```
gtpp test { accounting { all | cgf-server cgf_address | group name group_name } | storage-server [ address ip-addr port udp-port | group name group_name ] }
```

- **all**
  Tests all CGFs configured within the given context.

- **cgf-server cgf_address**
  Tests a CGF configured within the given context and specified by the IP address of the CGF entered using IPv4 dotted-decimal notation.

- **group name group_name**
  Tests the storage server for an existing group name specified as an alphanumeric string of 1 through 63 characters.

- **storage-server [ address ip-address port udp-port]**
  Tests the connectivity and provides round trip time for the echo request sent to the GTPP Storage-Server configured in the requested context. The IP address of the GSS is entered using IPv4 dotted-decimal notation and the UPD port is the one defined for the GTPP Storage Server.

Usage

This command is used to verify the configuration of and test the system’s ability to communicate with one or all configured GSS/CGFs for monitoring or troubleshooting purposes.
When executed, this command causes the system to send GTPP echo packets to the specified GSS/CGF(s).
The command’s response will display whether the GSS/CGF is active or unreachable.

Example

The following command tests communication with a CGF having an IP address of 192.168.1.5:
gtpp test accounting cgf-server 192.168.1.5

The following command tests communication with a GSS configured in requested context

gtpp test storage-server

The following command verify communication with a GSS, having IP address 192.156.12.10 and port 50000, without configuring it in a context

gtpp test storage-server address 192.156.12.10 port 50000
gtpu test echo

Tests the ability of a GGSN/P-GW/SAEGW/SGSN/S-GW service to exchange GTP-U echo request messages with specified peer(s).

Product

GGSN
P-GW
SAEGW
SGSN
S-GW

Privilege

Operator, Config-Administrator, Administrator

Mode

Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

StarOS v12.x and earlier:

```
gtpu test echo src-address gn_address { all | sgsn-address ip_address }
```

StarOS v14.0 and later:

```
gtpu test echo gtpu-service service_name { all | peer-address ip_address } [ gtpu-version { 0 | 1 } ]
```

```
src-address gn_address
```

Specifies the IP address of a Gn interface configured on the system using IPv4 dotted-decimal notation.

⚠️ Important: The IP address of the system’s Gn interface must be bound to a configured GGSN service prior to executing this command.

---

**all**

Sends GTP-U echo requests to all SGSNs that currently have sessions with the GGSN service.

**sgsn-address ip_address**

Sends GTP-U echo requests to an SGSN specified by its IP address in IPv4 dotted-decimal notation.

**gtpu-service service_name**

Specifies an existing GTP-U service.

*service_name* is an alphanumeric string of 1 through 63 characters.
**gtpu test echo**

```
all
```

Sends GTP-U echo requests to first 100 peers that currently have sessions with the GTP-U service.

---

**Important:** If this keyword is selected, additional confirmation is required after the following message, “Warning: Due to possibility of huge number of connected peers, considering system performance impacts, issue echo request to only 100 peers”.

```
peer-address ip_address
```

Specifies that GTP-U echo requests will be sent to a specific peer. 
**ip_address** must be entered using IPv4 dotted-decimal notation or IPV6 colon-separated-hexadecimal notation.

```
gtpu-version { 0 | 1 }
```

Optional. Specifies the GTP-U version in which the test echo will be sent. 0 Specifies GTP-U version 0, and 1 specifies GTP-U version 1.

- If the GTP-U version of the peer is unknown, the GGSN/P-GW/SAEGW/SGSN/S-GW will use the user-configured GTP-U version.
- If the GTPU version of peer node is already known, the test echo is sent in the known GTP-U version.
- If the GTP-U version is not configured, and the peer version is unknown, the test echo is sent in GTP-U version 0.

---

**Usage**

This command tests the GGSN/P-GW/SAEGW/SGSN/S-GW’s ability to exchange GPRS Tunneling Protocol user plane (GTP-U) packets with the specified SGSNs/peer(s). This command is useful for troubleshooting and/or monitoring. 
Refer also to the **gtpc test** command.

**Example**

The following command issues GTP-U echo packets from a GGSN service bound to address 192.168.157.43 to an SGSN with an address of 192.168.1.52:

```
gtpu test echo src-address 192.168.157.43 sgsn-address 192.168.1.52
```

The following command issues GTP-U echo packets from a GTP-U service named **gtpu_1** to the first 100 connected peers:

```
gtpu test echo gtpu-service gtpu_1 all
```
gtpv0 test echo

Tests the ability of a GGSN service to exchange GTPv0 echo request messages with the specified SGSN(s).

Product
GGSN

Privilege
Security Administrator, Administrator, Operator

Mode
Exec

The following prompt is displayed in the Exec mode:
[local]host_name#

Syntax

```bash
gtpv0 test echo src-address gn_address { all | sgsn-address ip_address }
```

- **src-address gn_address**
  Specifies the IP address of a Gn interface configured on the system using IPv4 dotted-decimal notation.

> **Important**: The IP address of the system’s Gn interface must be bound to a configured GGSN service prior to executing this command.

- **all**
  Sends GTPv0 echo requests to all SGSNs that currently have sessions with the GGSN service.

- **sgsn-address ip_address**
  Sends GTPv0 echo requests to an SGSN specified by its IP address in IPv4 dotted-decimal notation.

Usage

This command tests the GGSN’s ability to exchange GPRS Tunneling Protocol version 0 (GTPv0) packets with the specified SGSNs which can be useful troubleshooting and/or monitoring.

This command must be executed from within the context in which the GGSN service is configured.

Refer also to the `gtpc-test` and `gtpu test` commands.

> **Important**: In StarOS v14.0 and later, this command has been replaced by the `egtpc test echo` command.

Example

The following command issues GTPv0 echo packets from a GGSN service bound to address 192.168.1.33 to an SGSN with an address of 192.168.1.42:

```bash
gtpv0 test echo src-address 192.168.1.33 sgsn-address 192.168.1.42
```
hd raid

Performs RAID management operations on the platform hard disk drives.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

For the ASR 5000:

```
hd raid { check | create | insert | overwrite | remove select } local1 | remote1 } [ -force ] [ -noconfirm ]
```

For the ASR 5500:

```
hd raid { check | create | insert | overwrite | remove select } hd_num [ -force ] [ -noconfirm ]
```

---

**check**

Starts a background check on RAID disks unless the RAID is running in degraded mode.

---

**create local1 | remote1**

On the ASR 5000, creates a new RAID that could run in degraded mode on the specified drive:

- `local1` specifies the RAID is to be established on the primary SMC.
- `remote1` specifies the RAID is to be established on the backup SMC.

---

**create hd_num**

On the ASR 5500, creates a new RAID that could run in degraded mode on the hard drive array of a specific FSC.

- `hd_num` specifies the RAID is to be established on the FSC in slot numbers 13 through 18 (hd13, hd14, ..., hd18).

---

**insert local1 | remote1**

On the ASR 5000, inserts the specified disk to the running RAID causing it to recover from degraded mode.

- `local1` specifies the primary SMC is to be inserted into the RAID.
- `remote1` specifies the backup SMC is to be inserted into the RAID.

---

**insert hd_num**

On the ASR 5500, inserts the specified FSC disk array into the running RAID causing it to recover from degraded mode.
hd_num specifies the RAID is to be established on the FSC in slot numbers 13 through 18 (hd13, hd14, ... hd18).

**insert** { | local1 | local2 }

On VPC, inserts the specified vHD into the running RAID causing it to recover from degraded mode.

**overwrite** local1 | remotel

On the ASR 5000, overwrites the specified disk and adds it to the current running RAID to construct a fully mirrored array.

local1 specifies the primary SMC is to be added to the current RAID. remotel specifies the backup SMC is to be added to the current RAID.

**overwrite** hd_num

On the ASR 5000, overwrites the specified FSC disk array and adds it to the current running RAID to construct a fully mirrored array.

hd_num specifies the RAID is to be established on the FSC in slot numbers 13 through 18 (hd13, hd14, ... hd18).

**overwrite** { | local1 | local2 }

On VPC, overwrites the specified vHD and adds it to the current running RAID to construct a fully mirrored array.

**remove** local1 | remotel

On the ASR 5000, removes the specified disk from the running RAID causing it to run in degraded mode or to fail.

local1: specifies the primary SMC is to be removed from the RAID. remotel: specifies the backup SMC is to be removed from the RAID.

**remove** hd_num

On the ASR 5500, removes the specified FSC disk array from the running RAID causing it to run in degraded mode or to fail.

hd_num specifies the RAID is to be established on the FSC in slot numbers 13 through 18 (hd13, hd14, ... hd18).

**remove** { | local1 | local2 }

On the VPC, removes the specified vHD from the running RAID causing it to run in degraded mode or to fail.

**select** local1 | remotel

On the ASR 5000, selects the specified disk to assemble a RAID when two unrelated RAID disks are present in the system. The resulting RAID runs in degraded mode.

local1: specifies the primary SMC is to assemble the RAID. remotel: specifies the backup SMC is to assemble the RAID.

**select** hd_num

On the ASR 5500, selects the specified FSC disk array to assemble a RAID when two or more unrelated RAID disks are present in the system. The resulting RAID runs in degraded mode.
hd_num specifies the RAID is to be established on the FSC in slot numbers 13 through 18 (hd13, hd14, ... hd18).

-noconfirm
Executes the command without displaying “are you sure” prompts.

-force
Executes the command and overrides warnings.

Usage
All commands need confirmation unless the -noconfirm is included in the command. If the result will bring down a running RAID, you have to force the command using -force. RAID commands are needed to intervene in the following situations:
• the hard disk controller task can not determine the correct operation,
• administrator action is required by policy
• the administrator wants to wipe out an unused disk.

In an automated system, the policies created with this CLI address the possibility of a manually partitioned disk, a disk resulting from a different version of software, a partially constructed disk, or the case of two unrelated disks in the system.

To reduce administrator intervention, a set of policies can be configured to set the default action using the commands in the HD RAID configuration mode. These commands are described in the HD Storage Policy Configuration Mode Commands chapter of this guide.

Example
The following instructs the system to setup a RAID on the primary ASR 5000 SMC hard drive.

    hd raid create local1 -force
**host**

Used to resolve the IP address or logical host name information via a DNS query.

**Product**

All

**Privilege**

Security Administrator, Administrator, Operator

**Mode**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
host { host_name | host_ip_address }
```

- **host_name**
  - Specifies the logical host name for which the IP address is to be displayed (via DNS lookup).
  - This is an alphanumeric string of 1 through 127 characters.

- **host_ip_address**
  - Specifies the IP address for which the associated logical host name(s) are to be displayed (via reverse DNS lookup) using IPv4 dotted-decimal notation.

**Usage**

Verify DNS information which affects connections and packet routing.

**Example**

The following commands will resolve the host information for `remoteABC` and `10.2.3.4` respectively.

```
host remoteABC
host 10.2.3.4
```
install plugin

Unpacks the contents of a patch kit for a specific plugin module. This function is associated with the patch process for accommodating dynamic software upgrades.

Product
ADC

Privilege
Security Administrator, Administrator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

install plugin plugin_name patch_file_name

plugin_name
Specifies the name of a plugin that has been already copied onto the system as an alphanumeric string of 1 through 16 characters.

patch_file_name
Specifies the file name of the patch (.tgz extension) that was copied onto the system. Ensure that the full file path is copied.

Usage
Unpacks the contents of a patch kit intended for a specific plugin module. After unpacking the patch you must configure the plugin using the plugin command in the Global Configuration mode. For additional information, refer to the Plugin Configuration Mode Commands chapter.

Example
To unpack the plugin module named p2p with the patch file name libp2p-1.2.0.tgz onto the system enter the following command:

install plugin p2p libp2p-1.2.0.tgz
interface

Configures the system to generate gratuitous ARP (G-ARP) requests in case of a failure during an inter-node online upgrade. If the chassis is not active, an error message displays.

Product
All

Privilege
Security Administrator, Administrator, Operator, or Inspector with li-administrator permissions

Mode
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

interface name send gratuitous-arp ip-address

Usage
This command generates a G-ARP for the IP address specified and sends it over the interface.

Example
The following generate a G-ARP for IP address 192.168.100.10.

    interface interface_1 send gratuitous-arp 192.168.100.10
lawful-intercept

Refer to the *Lawful Intercept Configuration Guide* for a description of this command.
lawful-intercept packet-cable

Refer to the Lawful Intercept Configuration Guide for a description of this command.
lawful-intercept ssdf

Refer to the *Lawful Intercept Guide* for a description of this command.
link-aggregation port switch to

When a link aggregation group (LAG) contains two sets of ports with each connecting to a different Ethernet switch, this command allows you to change the status of the active distributing ports. (ASR 5x00 only)

Default: none.

Product
All

Privilege
Security Administrator, Administrator, Operator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

link-aggregation port switch to slot# / port#

slot#
Identifies the physical chassis slot where the line card or MIO card is installed.

port#
Identifies the physical port on the line card or MIO card to automatically switch to.

Usage

This command is subject to the following restrictions:
- slot#/port# must support LAG.
- slot#/port# must be configured with LAG.
- slot#/port# must not be actively distributing.
- slot#/port# must have negotiated a partner while in standard mode.
- slot#/port#’s partner must have a priority equal to or greater than itself.
- slot#/port#’s partner bundle must have bandwidth in standard mode equal to or greater than itself.
- Switching to slot#/port# must not violate preference within hold-time in standard mode.

Example

link-aggregation port switch to 17/2

link-aggregation port switch to 5/12
logging active

Enables or disables logging for active internal log files.

Product

All

Privilege

Security Administrator, Administrator, Operator

Mode

Exec

The following prompt is displayed in the Exec mode:

[local] host_name#

Syntax

logging active [ copy runtime filters ] [ event-verbosity event_level ] [ pdu-data format ] [ pdu-verbosity pdu_level ]

no logging active

no

Indicates the internal logging is to be disabled.

copy runtime filters

Copies the runtime filters and uses that copy to filter the current logging session.

event-verbosity event_level

Specifies the level of verboseness to use in logging of events as one of:

- min: Displays minimal information about the event. Information includes event name, facility, event ID, severity level, date, and time.
- concise: Displays detailed information about the event, but does not provide the event source within the system.
- full: Displays detailed information about event, including source information, identifying where within the system the event was generated.

pdu-data format

Specifies output format for packet data units when logged as one of:

- none: raw format (unformatted).
- hex: hexadecimal format.
- hex-ascii: hexadecimal and ASCII similar to a main-frame dump.

pdu-verbosity pdu_level

Specifies the level of verboseness to use in logging of packet data units as an integer from 1 through 5, where 5 is the most detailed.
Usage

Adjust the active logging levels when excessive log file sizes are being generated or, conversely, not enough information is being sent to the active log files for adequate troubleshooting support. The no keyword is used to disable internal logging.

Important: A maximum of 50,000 events may be stored in each log. Enabling more events for logging may cause the log to be filled in a much shorter time period. This may reduce the effectiveness of the log data as a shorter time period of event data may make troubleshooting more difficult.

Important: Once a log has reached the 50,000 event limit the oldest events will be discarded as new log entries are created.

Example

The following sets the active logging for events to the maximum.

```
logging active event-verbosity full
```

The following command sets the active logging for packet data units to level 3 and sets the output format to the main-frame style hex-ascii.

```
logging active pdu-data hex-ascii pdu-verbosity 3
```

The following disables internal logging.

```
no logging active
```
logging filter

Sets the logging filtering options for all or individual facilities.

**Product**
All

**Privilege**
Security Administrator, Administrator, Operator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
logging filter active facility facility level severity_level [ critical-info | no-critical-info ]
```

- **active**
  Indicates only active processes are to have logging options set.

- **facility facility**
  Specifies the facility to modify the filtering of logged information. Valid facilities for this command are:
  - **a10**: A10 interface facility
  - **a11**: A11 interface facility
  - **a11mgr**: A11 Manager facility
  - **aaa-client**: Authentication, Authorization and Accounting (AAA) client facility
  - **aaamgr**: AAA manager logging facility
  - **aaaproxy**: AAA Proxy facility
  - **aal2**: ATM Adaptation Layer 2 (AAL2) protocol logging facility
  - **acl-log**: Access Control List (ACL) logging facility
  - **acsctrl**: Active Charging Service (ACS) Controller facility
  - **acsmgr**: ACS Manager facility
  - **afctrl**: Fabric Controller facility [ASR 5500 only]
  - **afmgr**: Fabric Manager logging facility [ASR 5500 only]
  - **alarmctrl**: Alarm Controller facility
  - **alcap**: Access Link Control Application Part (ALCAP) protocol logging facility
  - **alcapmgr**: ALCAP manager logging facility
  - **all**: All facilities
  - **asngwmg**: Access Service Network (ASN) Gateway Manager facility
  - **asnpmgr**: ASN Paging Controller Manager facility
- **bfd**: Bidirectional Forwarding Detection (BFD) protocol logging facility
- **bgp**: Border Gateway Protocol (BGP) facility
- **bindmux**: IPCF BindMux-Demux Manager logging facility
- **bngmgr**: Broadband Network Gateway (BNG) Demux Manager logging facility
- **bssap+**: Base Station Sub-system Application Part+ protocol facility for the login interface between the SGSN and the MSC/VLR (2.5G and 3G)
- **bssgp**: Base Station Sub-system GPRS Protocol logging facility handles exchange information between the SGSN and the BSS (2.5G only)
- **callhome**: Call Home application logging facility
- **cap**: CAMEL Application Part (CAP) logging facility for protocol used in prepaid applications (2.5G and 3G)
- **cbsmgr**: Cell Broadcasting Service (CBS) logging facility [HNBGW]
- **cdf**: Charging Data Function (CDF) logging facility
- **cgw**: Converged Access Gateway (CGW) logging facility
- **cli**: Command Line Interface (CLI) logging facility
- **cmp**: Certificate Management Protocol (IPSec) logging facility
- **connectedapps**: SecGW ASR 9000 oneP communication protocol
- **connproxy**: Controller Proxy logging facility
- **credit-control**: Credit Control (CC) facility
- **csf**: IMS/MMD Call Session Control Function (CSCF)
- **csfcpmgr**: CSCFCPMGR logging facility
- **csfmgr**: SIP CSCF Manager facility
- **cscfnpdb**: CSCF Number Portability Database (NPDB) logging facility
- **csfrtcp**: IMS/MMD CSCF RTCP log facility
- **csfrtp**: IMS/MMD CSCF RTP log facility
- **cscfttmgr**: SIP CSCF Tunnel and Transport Manager facility
- **csp**: Card/Slot/Port controller facility
- **css**: Content Service Selection (CSS) facility
- **css-sig**: CSS RADIUS Signaling facility
- **cx-diameter**: Cx Diameter Messages facility [CSCF <--> HSS]
- **dcardctrl**: IPSec Daughter Card Controller logging facility
- **dcardmgr**: IPSec Daughter Card Manager logging facility
- **demuxmgr**: Demux Manager API facility
- **dgmbmgr**: Diameter Gmb Application Manager logging facility
- **dhcp**: Dynamic Host Configuration Protocol (DHCP) logging facility
- **dhcpv6**: DHCPv6
- **dhost**: Distributed Host logging facility
- **diabase**: Diabase messages facility
• **diameter**: Diameter endpoint logging facility
• **diameter-acct**: Diameter Accounting
• **diameter-auth**: Diameter Authentication
• **diameter-dns**: Diameter DNS subsystem
• **diameter-ecs**: ACS Diameter signaling facility
• **diameter-hdd**: Diameter Horizontal Directional Drilling (HDD) Interface facility
• **diameter-svc**: Diameter Service
• **diamproxy**: DiaProxy logging facility
• **dpath**: IPSec Data Path facility
• **drvctrl**: Driver Controller facility
• **doulosuemgr**: Doulos (IMS-IPSec-Tool) user equipment manager
• **eap-diameter**: Extensible Authentication Protocol (EAP) IP Security facility
• **eap-ipsec**: Extensible Authentication Protocol (EAP) IPsec facility
• **eap-sta-s6a-s13-s6b-diameter**: EAP/STA/S6A/S13/S6B Diameter messages facility
• **eecs-cs**: ACSMGR <=> Session Manager Signalling Interface facility
• **egtpc**: eGTP-C logging facility
• **egtpmgr**: enhanced GPRS Tunneling Protocol (eGTP) manager logging facility
• **egtpu**: eGTP-U logging facility
• **epdg**: evolved Packet Data (ePDG) gateway logging facility
• **event-notif**: Event Notification Interface logging facility
• **evlog**: Event log facility
• **famgr**: Foreign Agent manager logging facility
• **firewall**: Firewall logging facility
• **fng**: Femto Network Gateway (FNG) logging facility
• **gbmgr**: SGSN Gb Interface Manager facility
• **gmm**:  
  • For 2.5G: Logs the GPRS Mobility Management (GMM) layer (above LLC layer)  
  • For 3G: Logs the access application layer (above the RANAP layer)
• **gprs-app**: GPRS Application logging facility
• **gprs-ns**: GPRS Network Service Protocol (layer between SGSN and the BSS) logging facility
• **gq-rx-tx-diameter**: Gq/Rx/Tx Diameter messages facility
• **gss-gcdr**: GTPP Storage Server GCDR facility
• **gtpc**: GTP-C protocol logging facility
• **gtpcmgr**: GTP-C protocol manager logging facility
• **gtp**: GTP-prime protocol logging facility
• **gtpu**: GTP-U protocol logging facility
• **gtpumgr**: GTP-U Demux manager
• **gx-ty-diameter**: Gx/Ty Diameter messages facility
• **gy-diameter**: Gy Diameter messages facility
• **h248p**: H.248 port manager facility
• **hamgr**: Home Agent manager logging facility
• **hat**: High Availability Task (HAT) process facility
• **hdctrl**: HD Controller logging facility
• **henhapp**: Home Evolved NodeB (HENB) App facility
• **henbgw**: HENB-GW facility
• **henbgw-p**: HENB-GW Public Warning System logging facility
• **henbgw-sctp-acs**: HENB-GW access Stream Control Transmission Protocol (SCTP) facility
• **henbgw-sctp-n**: HENBGW network SCTP facility
• **henbgwdemux**: HENBGW Demux facility
• **henbgwmgr**: HENB-GW Manager facility
• **hnb-g**: HNB-GW (3G Femto GW) logging facility
• **hnbmgr**: HNB-GW Demux Manager logging facility
• **hss-peer-service**: Home Subscriber Server (HSS) Peer Service facility
• **igmp**: Internet Group Management Protocol (IGMP)
• **ikev2**: Internet Key Exchange version 2 (IKEv2)
• **ims-authorizat**: IP Multimedia Subsystem (IMS) Authorization Service facility
• **ims-sh**: HSS Diameter Sh Interface Service facility
• **imsimgr**: SGSN IMSI Manager facility
• **imsue**: IMS User Equipment (IMSUE) facility
• **ip-arp**: IP Address Resolution Protocol facility
• **ip-interface**: IP interface facility
• **ip-route**: IP route facility
• **ipms**: Intelligent Packet Monitoring System (IPMS) logging facility
• **ipne**: IP Network Enabler (IPNE) facility
• **ipsec**: IP Security logging facility
• **ips**: IP Service Gateway interface logging facility
• **ipsgm**: IP Services Gateway facility
• **ips**: IP Pool Sharing Protocol logging facility
• **kvstore**: Key/Value Store (KVSTORE) Store facility
• **l2tp-control**: Layer 2 Tunneling Precool (L2TP) control logging facility
• **l2tp-data**: L2TP data logging facility
• **l2tpdemux**: L2TP Demux Manager logging facility
• **l2tpmgr**: L2TP Manager logging facility
• **lagmgr**: Link Aggregation Group (LAG) manager logging facility
• **lcs**: Location Services (LCS) logging facility
• **ldap**: Lightweight Directory Access Protocol (LDAP) messages logging facility
• **li**: Refer to the *Lawful Intercept Interface Reference* for a description of this command.
• **linkmgr**: SGSN/BSS SS7 Link Manager logging facility (2.5G only)
• **llc**: Logical Link Control (LLC) Protocol logging facility; for SGSN: logs the LLC layer between the GMM and the BSSGP layers for logical links between the MS and the SGSN
• **local-policy**: Local Policy Service facility
• **location-service**: Location Services facility
• **m3ua**: M3UA Protocol logging facility
• **magmgr**: Mobile Access Gateway manager logging facility
• **map**: Mobile Application Part (MAP) protocol logging facility
• **megadmmgr**: MegaDiameter Manager (SLF Service) logging facility
• **mme-app**: Mobility Management Entity (MME) Application logging facility
• **mme-misc**: MME miscellaneous logging facility
• **mmedemux**: MME Demux Manager logging facility
• **mmemgr**: MME Manager facility
• **mmgr**: Master Manager logging facility
• **mobile-ip**: Mobile IP processes
• **mobile-ip-data**: Mobile IP data facility
• **mobile-ipv6**: Mobile IPv6 logging facility
• **mpls**: Multiprotocol Label Switching (MPLS) protocol logging facility
• **mrme**: Multi Radio Mobility Entity (MRME) logging facility
• **mseg-app**: Mobile Services Edge Gateway (MSEG) application logging facility (This option is not supported in this release.)
• **mseg-gtpc**: MSEG GTP-C application logging facility (This option is not supported in this release.)
• **mseg-gtpu**: MSEG GTP-U application logging facility (This option is not supported in this release.)
• **msegmgr**: MSEG Demux Manager logging facility (This option is not supported in this release.)
• **mtp2**: Message Transfer Part 2 (MTP2) Service logging facility
• **mtp3**: Message Transfer Part 3 (MTP3) Protocol logging facility
• **multicast-proxy**: Multicast Proxy logging facility
• **nas**: Non-Access Stratum (NAS) protocol logging facility [MME 4G]
• **netwstrg**: Network Storage facility
• **npuctrl**: Network Processor Unit Control facility
• **npudrv**: Network Processor Unit Driver facility [ASR 5500 only]
• **npumgr**: Network Processor Unit Manager facility
• **npumgr-acl**: NPUMGR ACL logging facility
• **npumgr-driv**: NPUMGR DRV logging facility
• `npumgr-flow`: NPUMGR FLOW logging facility
• `npumgr-fwd`: NPUMGR FWD logging facility
• `npumgr-init`: NPUMGR INIT logging facility
• `npumgr-lc`: NPUMGR LC logging facility
• `npumgr-port`: NPUMGR PORT logging facility
• `npumgr-recovery`: NPUMGR RECOVERY logging facility
• `npumgr-rrri`: NPUMGR RRI (Reverse Route Injection) logging facility
• `npumgr-vpn`: NPUMGR VPN logging facility
• `npusim`: NPUSIM logging facility [ASR 5500 only]
• `ntfy-intf`: Notification Interface logging facility [Release 12.0 and earlier versions only]
• `ocsp`: Online Certificate Status Protocol logging facility.
• `orbs`: Object Request Broker System logging facility
• `ospf`: OSPF protocol logging facility
• `ospfv3`: OSPFv3 protocol logging facility
• `p2p`: Peer-to-Peer Detection logging facility
• `pagingmgr`: PAGINGMGR logging facility
• `pccmgr`: Intelligent Policy Control Function (IPCF) Policy Charging and Control (PCC) Manager library
• `pdg`: Packet Data Gateway (PDG) logging facility
• `pdgdmgr`: PDG Demux Manager logging facility
• `pdf`: Packet Data Interworking Function (PDIF) logging facility
• `pgw`: Packet Data Network Gateway (PGW) logging facility
• `pmm-app`: Packet Mobility Management (PMM) application logging facility
• `ppp`: Point-To-Point Protocol (PPP) link and packet facilities
• `pppoa`: PPP over Ethernet logging facility
• `push`: VPNMGR CDR push logging facility
• `radius-acct`: RADIUS accounting logging facility
• `radius-auth`: RADIUS authentication logging facility
• `radius-coa`: RADIUS change of authorization and radius disconnect
• `ranap`: Radio Access Network Application Part (RANAP) Protocol facility logging info flow between SGSN and RNS (3G)
• `rc`: Recovery Control Task logging facility
• `rd`: Redirect Task logging facility
• `resmgr`: Resource Manager logging facility
• `rf-diameter`: Diameter RF interface messages facility
• `rip`: Routing Information Protocol (RIP) logging facility [RIP is not supported at this time.]
• `rlf`: Rate Limiting Function (RLF) logging facility
- **rohc**: Robust Header Compression (RoHC) facility
- **rsvp**: Reservation Protocol logging facility
- **rua**: RANAP User Adaptation (RUA) [3G Femto GW - RUA messages] logging facility
- **s1ap**: S1 Application Protocol (S1AP) Protocol logging facility
- **sabp**: Service Area Broadcast Protocol (SABP) logging facility
- **saegw**: System Architecture Evolution (SAE) Gateway facility
- **scpp**: Signalling Connection Control Part (SCCP) Protocol logging (connection-oriented messages between RANAP and TCAP layers).
- **set**: Shared Configuration Task logging facility
- **sctp**: Stream Control Transmission Protocol (SCTP) Protocol logging facility
- **sef ecs**: Severely Errored Frames (SEF) APIs printing facility
- **sess-gr**: SM GR facility
- **sessctrl**: Session Controller logging facility
- **sessmgr**: Session Manager logging facility
- **sesstrc**: session trace logging facility
- **sft**: Switch Fabric Task logging facility
- **sgs**: SGs interface protocol logging facility
- **sgsn-app**: SGSN-APP logging various SGSN “glue” interfaces (for example, between PMM, MAP, GPRS-FSM, SMS).
- **sgsn-failures**: SGSN call failures (attach/activate rejects) logging facility (2.5G)
- **sgsn-gtpc**: SGSN GTP-C Protocol logging control messages between the SGSN and the GGSN
- **sgsn-gtpu**: SGSN GTP-U Protocol logging user data messages between the SGSN and GGSN
- **sgsn-mbms-bearer**: SGSN Multimedia Broadcast/Multicast Service (MBMS) Bearer app (SMGR) logging facility
- **sgsn-misc**: Used by stack manager to log binding and removing between layers
- **sgsn-system**: SGSN System Components logging facility (used infrequently)
- **sgsn-test**: SGSN Tests logging facility; used infrequently
- **sgtpcmgr**: SGSN GTP-C Manager logging information exchange through SGTPC and the GGSN
- **sgw**: Serving Gateway facility
- **sh-diameter**: Sh Diameter messages facility
- **sitmain**: System Initialization Task main logging facility
- **sm-app**: SM Protocol logging facility
- **sms**: Short Message Service (SMS) logging messages between the MS and the SMSC
- **sndcp**: Sub Network Dependent Convergence Protocol (SNDCP) logging facility
- **snmp**: SNMP logging facility
- **sprmgr**: IPCF Subscriber Policy Register (SPR) manager logging facility
- **srdb**: Static Rating Database
- **srr**: Service Redundancy Protocol (SRP) logging facility
logging filter

- **sscfnni**: Service-Specific Coordination Function for Signaling at the Network Node Interface (SSCF-NNI) logging facility
- **sscop**: Service-Specific Connection-Oriented Protocol (SSCOP) logging facility
- **ssh-ipsec**: Secure Shell (SSH) IP Security logging facility
- **ssl**: Secure Socket Layer (SSL) message logging facility
- **stat**: Statistics logging facility
- **supserv**: Supplementary Services logging facility [H.323]
- **system**: System logging facility
- **tacacsplus**: TACACS+ Protocol logging facility
- **tcap**: TCAP Protocol logging facility
- **testctrl**: Test Controller logging facility
- **testmgr**: Test Manager logging facility
- **threshold**: threshold logging facility
- **ttg**: Tunnel Termination Gateway (TTG) logging facility
- **tucl**: TCP/UDP Convergence Layer (TUCL) logging facility
- **udr**: User Data Record (UDR) facility (used with the Charging Service)
- **user-data**: User data logging facility
- **user-l3tunnel**: User Layer 3 tunnel logging facility
- **user tcp-stack**: User TCP Stack
- **vim**: Voice Instant Messaging (VIM) logging facility
- **vinfo**: VINFO logging facility
- **vmgctrl**: Virtual Media Gateway (VMG) controller facility
- **vmgctrl**: VMG Content Manager facility
- **vpn**: Virtual Private Network logging facility
- **wimax-data**: WiMAX DATA
- **wimax-r6**: WiMAX R6
- **wsg**: Wireless Security Gateway (ASR 9000 Security Gateway)

```markdown
level severity_level
```

Specifies the level of information to be logged from the following list which is ordered from highest to lowest:

- **critical** - display critical events
- **error** - display error events and all events with a higher severity level
- **warning** - display warning events and all events with a higher severity level
- **unusual** - display unusual events and all events with a higher severity level
- **info** - display info events and all events with a higher severity level
- **trace** - display trace events and all events with a higher severity level
- **debug** - display all events
critical-info | no-critical-info

critical-info: Specifies that events with a category attribute of critical information are to be displayed. Examples of these types of events can be seen at bootup when system processes and tasks are being initiated. This is the default setting.

no-critical-info: Specifies that events with a category attribute of critical information are not to be displayed.

Usage

Apply filters for logged data to collect only that data which is of interest.

Important: A maximum of 50,000 events may be stored in each log. Enabling more events for logging may cause the log to be filled in a much shorter time period. This may reduce the effectiveness of the log data as a shorter time period of event data may make troubleshooting more difficult.

Important: Once a log has reached the 50,000 event limit the oldest events will be discarded as new log entries are created.

Caution: Issuing this command could negatively impact system performance depending on the amount of system activity at the time of execution and/or the type of facility(ies) being logged.

Example

The following are selected examples used to illustrate the various options. Not all facilities will be explicitly shown as each follows the same syntax for options.

The following sets the level to log only warning information for all facilities.

    logging filter active facility all level warning

The following enables the logging of critical information for the SNMP facility while setting the level to error.

    logging filter active facility snmp level error critical-info
logging trace

Enables or disables the logging of trace information for specific calls, mobiles, or network addresses.

**Product**
All

**Privilege**
Security Administrator, Administrator, Operator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
[ no ] logging trace { callid call_id | ipaddr ip_address | msid ms_id | username user_name }
```

**no**
Indicates the logging of trace information is to be disabled.

```
callid call_id | ipaddr ip_address | msid ms_id | username user_name
```

- **callid call_id**: Specifies the exact call instance ID which is to have trace data logged as a 4-byte hexadecimal number.
- **ipaddr ip_address**: Specifies the IP address in IPv4 dotted-decimal notation for which trace information is to be logged.
- **msid ms_id**: Specifies the mobile subscriber ID for which trace information is to be logged as 7 to 16 digits of an IMSI, MIN, or RMI.
- **username user_name**: Specifies a previously configured user who is to have trace information logged.

**Usage**

A trace log is useful in troubleshooting subscriber problems as well as for system verification by using a test subscriber. The *no* keyword is used to stop the logging of trace information.

**Important**: A maximum of 50,000 events may be stored in each log. Enabling more events for logging may cause the log to be filled in a much shorter time period. This may reduce the effectiveness of the log data as a shorter time period of event data may make troubleshooting more difficult.

**Important**: Once a log has reached the 50,000 event limit the oldest events will be discarded as new log entries are created.

**Caution**: Issuing this command could negatively impact system performance depending on the number of subscribers connected and the amount of data being passed.
Example

The following commands enables/disables trace information for user user1.

```
logging trace username user1

no logging trace username user1
```

The following commands will enable/disable trace information logging for the user assigned IP address 10.2.3.4.

```
logging trace ipaddr 10.2.3.4

no logging trace ipaddr 10.2.3.4
```

The following enables/disables logging of trace information for call ID fe80AA12.

```
logging trace callid fe80AA12

no logging trace callid fe80AA12
```
logs checkpoint

Performs check pointing operations on log data. Check pointing identifies logged data as previously viewed or marked. Check pointing results in only the log information since the last check point being displayed; check pointed log data is not available for viewing.

Individual logs may have up to 50,000 events in the active log. Check pointing the logs will then result in at most 50,000 events being in the inactive log files. This gives a maximum of 100,000 events in total which are available for each facility logged.

Product
All

Privilege
Security Administrator, Administrator, Operator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax
logs checkpoint

Usage
Check point log data to a set the log contents to a well know point prior to special activities taking place. This command may also be a part of periodic regular maintenance to manage log data.

The check pointing of logs moves the current log data to the inactive logs. Only the most recently check pointed data is retained in the inactive logs. A subsequent check pointing of the logs will result in the prior check pointed inactive log data being cleared and replaced with the newly check pointed data.

The check pointing of log data moves the active log data to be retained as the inactive log data. This results in the active log data, if displayed, having no data earlier than the point in time when the check pointing occurred.

Important: Check pointing of logs should be done periodically to avoid the logs becoming full. Logs which have 50,000 events logged will discard the oldest events first when new events are to be logged.

Example

logs checkpoint
**Isp-ping**

Checks Multi Protocol Label Switching (MPLS) label switch path (LSP) connectivity for the specified IPv4 forwarding equivalence class (FEC). It must be followed by an IPv4 FEC prefix.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec
The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
Isp-ping ip_prefix_FEC [ count ping_packets ] [ | verbose ] [ | grep grep_options ]
```

Where:

- `ip_prefix_FEC`
  Specifies an IP prefix FEC with or without subnet mask entered using IPv4 dotted-decimal CIDR notation.

- `count ping_packets`
  Sets the number of ping packets to be sent as an integer from 1 through 16. Default: 4.

**Important:** The timeout interval for the packets is 5 seconds by default.

- `verbose`
  Sets the verbose (detailed) output mode.

- `grep grep_options`
  Pipes (sends) the output of this command to the `grep` command.

**Usage**

This command is used to verify the MPLS LSP connectivity for the specified FEC.

**Example**

Following are the examples for using this command with all possible options for IPv4 address 13.13.13.1 and mask 32 (CIDR notation):

```
Isp-ping 13.13.13.1/32
```

```
Isp-ping 13.13.13.1/32 count 15
```

```
Isp-ping 13.13.13.1/32 verbose
```
**lsp-traceroute**

Discovers MPLS LSP routes that packets actually take when traveling to their destinations. It must be followed by an IPv4 or IPv6 FEC prefix.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
lsp-traceroute ip_prefix_FEC [ maxttl time_to_live ] [ | verbose ] [ | grep grep_options ]
```

**ip_prefix_FEC**

Specifies the destination IP address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal with or without mask (CIDR notation).

**maxttl time_to_live**

Sets the maximum time to live in hops. TTL is an integer from 1 through 255. Default: 30.

**verbose**

Sets the verbose (detailed) output mode.

**grep grep_options**

Pipes (sends) the output of this command to the grep command.

**Usage**

This command is used or the router to discover the MPLS LSP routes through which the packets will travel to their IPv4 or IPv6 destinations.

**Example**

The following command specifies the destination IP address 13.13.13.13 for which the MPLS routes will be discovered for packets to traverse:

```
lsp-traceroute 13.13.13.13/32
```
mkdir

Creates a new directory in the local file system or in remote locations as specified.

Product

All

Privilege

Security Administrator, Administrator

Mode

Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

```plaintext
mkdir filepath
```

filepath

Specifies the directory path to create. The path must be formatted as follows:

For the ASR 5000:

```
[ file: ]{ /flash | /pcmcia1 | /hd-raid }[ /directory ]/file_name
```

**Important:** Use of the ASR 5000 SMC hard drive is not supported in this release.

For the ASR 5500:

```
[ file: ]{ /flash | /usb1 | /hd-raid }[ /directory ]/file_name
```

**Important:** Do not use the following characters when entering a string for the field names below: “/” (forward slash), “:” (colon) or “@” (at sign).

`directory` is the directory name

`filename` is the actual file of interest

Usage

Create new directories as part of periodic maintenance activities to better organize stored files.

Example

The following creates the directory `/flash/pub` in the local flash storage.

```plaintext
mkdir /flash/pub
```
**mme disconnect**

Performs a graceful/ungraceful disconnection of an SCTP peer.

**Product**
MME

**Privilege**
Security Administrator, Administrator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

**Syntax**

```
mme disconnect s1-peer peer_ID  [ graceful ]  [ -noconfirm ]
```

- **s1-peer peer-ID**
  Specifies the eNodeB peer ID which has to be disconnected. `peer-ID` is an integer from 1 through 4294967295.

- **graceful**
  Specifies that the SCTP connection to the S1 peer will be terminated with a complete handshake. By default (without this keyword), SCTP connections are aborted.

- **-noconfirm**
  Executes the command without any additional prompts or confirmation from the user.

**Usage**

Use this command to disconnect the SCTP connection to the specified peer eNodeB. This command can be used to remove stale eNodeB connections from the MME, even when no active SCTP connection exists.

**Example**

The following gracefully disconnects the SCTP connection with the eNodeB with a peer ID of 22315734:

```
mme disconnect s1-peer 22315734 graceful -noconfirm
```
mme offload

Initiates or stops the offload of UEs associated with a specified MME service.

Product
MME

Privilege
Security Administrator, Administrator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]\host_name#

Syntax

The following command syntax is available in Release 12.2 and earlier.

mme offload mme-service mme_svc_name \{ start mme-init-release-timeout seconds paging-init-timeout seconds | stop \}

The following command syntax is available in Release 14.0 and higher.

mme offload mme-service mme_svc_name \{ time-duration minutes offload-percentage percent \[ disable-implicit-detach \] | stop \} \[ -noconfirm \]

Syntax Reference

mme-service name

Specifies the name of an existing MME service from which UEs will be offloaded as an alphanumeric string of 1 through 63 characters.

start mme-init-release-timeout seconds paging-init-timeout seconds

These keywords are available in Release 12.2 and earlier.

Sets the timeout for the initial release procedure and the paging procedure.

start mme-init-release-timeout seconds: Configures the timeout (in seconds) for triggering the IDLE MODE ENTRY procedure for UEs that are in the ECM_CONNECTED state as an integer from 1 to 120. The cause of the IDLE MODE ENTRY will be “Load balancing TAU required”.

paging-init-timeout seconds: Configures the timeout (in seconds) for triggering the PAGING procedure for UEs in the ECM_IDLE state as an integer from 1 to 120. After returning the UEs to the ECM_CONNECTED state, the IDLE MODE ENTRY procedure is triggered with the “Load balancing TAU required” cause.

time-duration minutes offload-percentage percent

time-duration specifies the maximum allowed time for the UE offload procedure to complete. minutes can be any value 1 through 1000 minutes.

offload-percentage specifies the percentage of total subscribers on this mme-service to offload. percent can be any value 0 through 100.
disable-implicit-detach
By default, if the UE context is not transferred to another MME within 5 minutes, the UE will be implicitly detached. This option disables this implicit detach timer.

stop
Ends the offload process.

-noconfirm
Executes the command without any additional prompts or confirmation from the user.

Usage
Use this command to initiate or stop the offloading of UEs associated with a specified MME service.
Prior to initiating this command, you can set the relative-capacity command in the MME Service Configuration Mode to zero (0). This prevents this MME from accepting any new calls, and redirects them to other MMEs in the pool while existing UEs on this MME are removed.

Important: Emergency attached UEs in Connected or Idle mode are not considered for offloading.

Example
This example applies to Release 12.2 and earlier.
The following command sets the trigger to start off-loading UEs from a service named mme3 at 60 seconds and the paging trigger at 90 seconds:

mme offload mme-service mme3 start mme-init-release-timeout 60 paging-init-timeout 90

Example
This example applies to Release 14.0 and higher.
The following example command rebalances (offloads) 30 percent of all UEs from the specified mme-service (to other mme-services in the MME pool) over the course of 10 minutes.

mme offload mme-service mme_svc time-duration 10 offload-percentage 30 -noconfirm
**mme paging cache clear**

Enables the operator to clear the paging cache for either a specific SessMgr instance or for all SessMg.rs.

**Product**
MME.

**Privilege**
Security Administrator, Administrator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name# 
```

**Syntax**

```
mme paging cache clear { all | instance sessmgr_instance }
```

- **all**
  Instructs the MME to clear the paging cache for all Session Managers.

- **instance sessmgr_instance**
  Enter an integer from 0 to 4294967295 to specify a single Session Manager.

**Usage**

This command clears the cache. It is important to clear the cache after the mme paging cache size is set to zero (0) to stop caching. This clear command needs to be used to reset the cache after caching is stopped.

**Example**

Use the following command to clear the paging cache for all SessMg.rs:

```
mme paging cache clear all
```
mme relocate-ue imsi

This command enables the operator to detach a UE from the current MME and cause it to reattach to another MME in the pool.

**Product**

MME

**Privilege**

Security Administrator, Administrator

**Mode**

Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

**Syntax**

```plaintext
mme relocate-ue imsi imsi new-guti mme-group-id grp_id mme-code mme_code m-tmsi mtmsi
```

**imsi imsi**

Specifies the Mobile Station Identifier of the UE to be relocated. This UE must be registered or connected to this MME.

**new-guti mme-group-id group_id**

The group to which the target MME belongs.

- `grp_id`:
  - Beginning with Releases 16.5, 17.4, and 18.2 and forward, the valid range for mme group id value is from 0 through 65536.
  - Previous releases, the valid range for mme group id value is from 32768 through 65536.

**mme-code mme_code**

The target MME to which this UE should be attached.

- `mme_code`: The unique identifier for the target MME; must be value from 0 through 255.

**m-tmsi mtmsi**

The new GUTI MME-TMSI for this UE.

- `mtmsi`: A value from 0 through 4294967295.

**Usage**

MME uses this configuration to relocate UEs to a different MME using IMSI, mme-group-id, mme-code and m-tmsi.
mme reset

Sends an S1 RESET message to a designated eNodeB to reset all UE-associated S1 connections.

**Product**
MME

**Privilege**
Security Administrator, Administrator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
mme reset s1-peer peer_ID
```

```
s1-peer peer-ID
```

Specifies an existing eNodeB peer ID to which the REST message is to be sent as an integer from 1 through 4294967295.

**Usage**

Use this command to send an S1 RESET message to a designated eNodeB to reset all UE-associated S1 connections.

The S1 peer ID for an eNodeB can be identified by executing the `show mme-service enodeb-association` command available in this mode. The peer ID is presented in the “Peerid” field.

**Example**

The following command initiates the sending of an S1-peer reset message to an eNodeB with a peer ID of 22315734:

```
mme reset s1-peer 22315734
```
monitor interface

Enables monitoring of traffic on a particular interface.

**Product**
All

**Privilege**
Security Administrator, Administrator, Operator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
monitor interface if_name
```

*if_name*

Specifies the name of the interface to be monitored as an alphanumeric string of 1 through 79 characters.

**Usage**

Use this command to monitor the traffic on a specified interface.

**Example**

This command monitors the traffic on the interface named *if1001*:

```
monitor interface if1001
```
monitor protocol

Enters the system’s protocol monitoring utility.

Product
All

Privilege
Security Administrator, Administrator, Operator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local] host_name#

Syntax

monitor protocol

Usage
Useful for troubleshooting, this command provides a tool for monitoring protocol transactions between the system and other network nodes including the mobile station(s).

The following protocols can be monitored:
- SNMP
- RADIUS Authentication
- RADIUS Accounting
- A11 (R-P Interface) (PDSN only)
- Mobile IPv4
- A11MGR
- PPP
- A10
- User L3 (User Layer 3 protocols)
- USERTCP STACK
- L2TP
- L2TPMGR
- L2TP Data
- GTPC
- GTPCMGR
- GTPU
- GTPP
Important: If the hard disk drive (HDD) is used for CDR storage, the CDR option must be used and not GTPP option (27).

- DHCP (GGSN only)
- CDR
- DHCPV6
- RADIUS COA
- MIP Tunnel
- L3 Tunnel (Layer 3 Tunnel Protocols)
- CSS Data
- CSS Signaling

Important: In StarOS 9.0 and later releases the CSS Data Signaling option is not supported.

- EC Diameter (Diameter Enhanced Charging)
- SIP (IMS)
- IPSec IKE Inter-Node
- IPSec IKE Subscriber
- IPSG RADIUS Signal
- ROHC (Robust Header Compression)
- WiMAX R6
- WiMAX Data
- SRP
- BCMCS SERV AUTH
- RSVP
- Mobile IPv6
- ASNGWMGR
- STUN
- SCTP: Enabling this option will display the SCTP protocol message packets on HNB-GW node.
- M3UA
- SCCP
- TCAP
- MAP
- RANAP
- GMM
- GPRS-NS
- BSSGP
- CAP
- SSCOP
- SSCFNNI
- MTP3
- LLC
- SNDCP
- BSSAP+
- SMS
- PHS-Control (Payload Header Compression)
- PHS-Data
- DNS Client
- MTP2
- HNBAP: Enabling this option will display the HNB Application Part (HNBAP) protocol packets.
- RUA: Enabling this option will display the RANAP User Adaptation (RUA) protocol packets.
- EGTPC
- App Specific Diameter: Enabling this option will display the following sub-options —
  - 1 - DIABASE (OFF)
  - 2 - DIAMETER Gy (OFF)
  - 3 - DIAMETER Gx/Ty/Gxx (OFF)
  - 4 - DIAMETER Gq/Rx/Tx (OFF)
  - 5 - DIAMETER Cx (OFF)
  - 6 - DIAMETER Sh (OFF)
  - 7 - DIAMETER Rf (OFF)
  - 8 - DIAMETER EAP/STa/S6a/S6d/S6b/S13/SWm (OFF)
  - 9 - DIAMETER HDD (OFF)
- PHS-EAPOL
- ICAP
- Micro-Tunnel
- ALCAP: Enabling this option will display the Access Link Control Application Part (ALCAP) protocol message packets on HNB-GW node.
- SSL
- S1-AP
- NAS
- LDAP
- SGS
- AAL2: Enabling this option will display the ATM Adaptation Layer 2 (AAL2) protocol message packets on HNB-GW node.
Once the protocol has been selected by entering its associated number, the utility monitors and displays every relative protocol message transaction.

Protocol monitoring is performed on a context-by-context-basis. Therefore, the messages displayed are only those that are transmitted/received within the system context from which the utility was executed.

For additional information on using the monitor utility, refer to the System Administration Guide.

⚠️ **Caution:** Protocol monitoring can be intrusive to subscriber sessions and could impact system performance. Therefore, it should only be used as a troubleshooting tool.

**Example**

The following command opens the protocol monitoring utility for SIP (IMS) = 37:

```
monitor protocol 37
```
monitor subscriber

Enables the system’s subscriber monitoring utility. Available keywords vary based on the licenses installed on the system.

Product
All

Privilege
Security Administrator, Administrator, Operator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

`monitor subscriber [ asn-peer-address bs_peer_address | callid call_id fng-peer-address ipv4_address | imei imei_value | imsi imsi_value | ipaddr ip_address | ipv6addr ipv6_address | ipsg-peer-address ipsg_peer_address | msid ms_id | msisdn msisdn | next-call | pcf pcf_address | pdif-peer-address pdif_peer_address | peer-fa peer_fa_address | peer-lac lac_peer_address | sgsn-address sgsn_address | type { lrttt | asngw | asnpc | closedrp | evdorev0 | evdoreva | interrogating-cscf | ggsn [ Next-Call By APN ] | ha | ipsg | lns | mme | pdif | proxy-cscf | rfc3261-proxy | serving-cscf } next-call | type bcmcs { next-call | next-service-request } | username user_name | Next-Call By APN ]`

---

`asn-peer-address bs_peer_address`

Specifies the peer ASN Base Station IP address in IPv4 address in dotted-decimal notation.

---

`callid call_id`

Specifies the call identification number assigned to the subscriber session by the system to be monitored as a 4-byte hexadecimal number.

---

`fng-peer-address ipv4_address`

Specifies the specific FNG WLAN IP address in IPv4 dotted-decimal notation.

---

`imei imei_value`

International Mobile Equipment Identification (IMEI). Must be followed by 8 digits of TAC (Type Allocation Code) and 6 digits of SNR (Serial Number). Only the first 14 digit of IMEI/IMEISV is used to find the equipment ID.

---

`imsi imsi_value`

Specifies the International Mobile Subscriber Identity (IMSI) of the subscriber session to be monitored an integer from 1 though 15 characters.

---

`ipaddr ip_address`

Specifies the IP address of the subscriber session to be monitored in IPv4 dotted-decimal notation.
**ipv6addr ipv6_address**
Specifies the IPv6 address of the subscriber session to be monitored in IPv6 colon-separated-hexadecimal notation.

**ipsg-peer-address ipsg_peer_address**
Specifies the peer IPSG IP address. Must be followed by an IPv4 address in dotted-decimal notation.

**msid ms_id**
Specifies the mobile subscriber identification number to be monitored as 7 to 16 digits of an IMSI, MIN, or RMI.

**msisdn msisdn**
Specifies the Mobile Subscriber ISDN number to be monitored as 7 to 16 digits of an IMSI, MIN, or RMI.

**next-call**
Specifies that the system will monitor the next incoming subscriber session. Entering this keyword will display the available options of protocols to select. For a list of supported protocols with this keyword, refer to the `monitor protocol` command.

**pcf pcf_address**
Specifies the PCF IP address in IPv4 dotted-decimal notation.

**pdif-peer-address pdif_peer_address**
Specifies the peer PDIF IP address in IPv4 dotted-decimal notation.

**peer-fa peer_fa_address**
Specifies the peer FA IP address in IPv4 dotted-decimal notation.

**peer-lac lac_peer_address**
Specifies the peer LAC IP address in IPv4 dotted-decimal notation.

**sgsn-address sgsn_address**
Specifies the SGSN IP address in IPv4 dotted-decimal notation.

**type { 1xrtt | asngw | asnpc | bcmcs | next-call | next-service-request }**
**evdorev0 | evdoreva | | fng | interrogating-cscf | ggsn | Next-Call By APN | ha | ipsg | ins | mme | openrp | pdif | pgw | proxy-cscf | rfc3261-proxy | saegw | serving-cscf | next-call [ apn apn ]**
Allows monitoring for specific subscriber types established in the system when next call occurs.

- **1xrtt**: Displays logs for cdma2000 1xRTT call session subscriber
- **asngw**: Displays logs for ASN-GW call session subscriber
- **asnpc**: Displays logs for ASN PC/LR call session subscriber
- **bcmcs**: Displays logs for Broadcast and Multicast Service
- **evdorev0**: Displays logs for cdma2000 EVDO Rev0 call session subscriber
On some page is a list of commands under the header "Exec Mode Commands (D-S)". The list includes:

- **evdoreva**: Displays logs for cdma2000 EVDO RevA call session subscriber
- **fng**: Displays logs for the FNG session subscriber
- **interrogating-cscf**: Displays logs for Interrogating CSCF subscriber
- **ggsn**: Displays logs for UMTS GGSN call session subscriber
- **Next-Call By APN**: Display logs for next call on APN basis, where APN name can be any Gi or Gn APN
- **ha**: Displays logs for Home Agent call session subscriber
- **ipsg**: Displays logs for IPSG call session subscriber
- **lns**: Displays logs for LNS call session subscriber
- **mme**: Displays logs for MME session subscribers.
- **pgw**: Displays logs for P-GW call session subscriber
- **pdif**: Displays logs for PDIF call session subscriber
- **proxy-cscf**: Displays logs for Proxy CSCF subscriber
- **rfc3261-proxy-cscf**: Displays logs for non-ims-proxy (RFC-3261 proxy) subscriber
- **saegw**: Displays logs for SAEGW call session subscriber
- **serving-cscf**: Displays logs for Serving CSCF subscriber

**username user_name**

Specifies the username of an existing subscriber to be monitored.

**Usage**

The monitor subscriber utility provides a useful tool for monitoring information about and the activity of either a single subscriber or all subscribers with active sessions within a given context.

**Caution**: The **monitor subscriber** command is intended for system debugging only. This command is complementary to external tracing systems and not meant as a replacement for ongoing external system monitoring.

The following items can be monitored:

- Control events
- Data events
- Event ID information
- Inbound events
- Outbound events
- Protocols (identical to those monitored by command)

Once the criteria has been selected, the utility will monitor and display every relative piece of information on the subscriber(s).

For additional information on using the monitor utility, refer to the *System Administration Guide*.
Important: Option Y for performing multi-call traces is only supported for use with the GGSN. This option is available when monitoring is performed using the “Next-Call” option. It allows you monitor up to 11 primary PDP contexts for a single subscriber.

Subscriber monitoring is performed on a context-by-context-basis. Therefore, the information displayed will be only that which is collected within the system context from which the utility was executed.

Caution: Subscriber monitoring can be intrusive to subscriber sessions and could impact system performance; therefore, it should only be used as a troubleshooting tool.

Example

The following command enables monitoring for user user1.

```
monitor subscriber username user1
```

The following command will enable monitoring for the user assigned IP address 10.2.3.4.

```
monitor subscriber ip-address 10.2.3.4
```

The following enables monitoring for call ID FE80AA12.

```
monitor subscriber callid fe80aa12
```
newcall policy

Configures new call policies for busy-out conditions.

Product

ASN-GW
ASN PC/LR
ePDG
GGSN
HA
HNB-GW
IPCF
LNS
MME
P-CSCF
PDSN
P-GW
SAEGW
S-GW
SGSN

Privilege

Security Administrator, Administrator, Operator

Mode

Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

newcall policy { asngw-service | asnpc-service | ePDG-service | sgsn-service } { all | name service_name } reject

newcall policy csf-service { all | name service_name } { redirect target_ip_address [ weight weight_num ] [ target_ipaddr2 [ weight weight_num ] ... target_ipaddr16 [ weight weight_num ] | reject }

newcall policy { fa-service | lma-service | lns-service | mipv6ha-service } { all | name service_name } reject

newcall policy ggsn-service { apn name apn_name | all | name service_name } reject

newcall policy { ha-service | pdsn-service } { all | name service_name } { redirect target_ip_address [ weight weight_num ] [ target_ipaddr2 [ weight weight_num ] ... target_ipaddr16 [ weight weight_num ] | reject }

Cisco ASR 5x00 Command Line Interface Reference
newcall policy hnbgw-service { all | name service_name } reject
newcall policy mme-service { all | name service_name } reject
newcall policy { pcc-af-service | pcc-policy-service } { all | name service_name } reject
newcall policy pgw-service { all | name service_name } reject
newcall policy saegw-service { all | name service_name } reject
newcall policy sgw-service { all | name service_name } reject
no newcall policy { asngw-service | asnpc-service | epDG-Service } { all | name service_name }
no newcall policy { fa-service | ggsn-service | ha-service | lma-service | lns-service | mipv6ha-service | psdn-service | psdnservice } { all | name service_name }
no newcall policy ggsn-service { apn apn_name | all | name service_name } reject
no newcall policy { ha-service | psdn-service } { all | name service_name } redirect
target_ip_address [ weight weight_num ] [ target_ip_address2 [ weight weight_num ] ... target_ip_address16 [ weight weight_num ]
no newcall policy hnbgw-service { all | name service_name }
no newcall policy mme-service { all | name service_name }
no newcall policy { pcc-af-service | pcc-policy-service } { all | name service_name }
no newcall policy pgw-service { all | name service_name }
no newcall policy saegw-service { all | name service_name }
no newcall policy sgw-service { all | name service_name }

no
Disables the new call policy for all or specified service of a service type.

no newcall policy { ha-service | psdn-service } { all | name service_name } redirect
target_ip_address [ weight weight_num ] [ target_ip_address2 [ weight weight_num ] ... target_ip_address16 [ weight weight_num ]
Deletes up to 16 IP addresses from the redirect policy. The IP addresses must be expressed in IPv4 dotted-decimal notation

newcall policy { asngw-service | asnpc-service | epDG-service } { all | name service_name } reject
Creates a new call policy to reject the calls based on the specified ASN-GW or ASN PC/LR service name or all services of this type.

asngw-service: Specifies the type of service as ASN GW for which new call policy is configured.
asnpc-service: Specifies the type of service as ASN PC/LR for which new call policy is configured.epDG-service: Specifies the type of service as ePDG for which new call policy is configured.
newcall policy { cscf-service | fa-service | lma-service | lns-service | mipv6ha-service | mme-service | pdsn-service | pdsn closedrp-service } { all | name service_name } reject

Creates a new call policy that rejects calls based on the specified access point name.

cscf-service | fa-service | ha-service | lma-service | lns-service | mipv6ha-service | mme-service | pdsn-service | pdsn closedrp-service

Specifies the type of service for which to configure a new call policy. The following services are supported:

- **cscf-service**: A Call/Session Control Function service
- **fa-service**: A Foreign Agent service
- **ha-service**: A Home Agent service
- **lma-service**: A Local Mobility Anchor (LMA) service
- **lns-service**: An L2TP Network Server service
- **mipv6ha-service**: A Mobile IPv6 Home Agent service
- **pdsn-service**: A Packet Data Serving Node service

{ all | name service_name }

Specifies a filter for the new call policy. Whether the new call policy will be applied to all configured services or a specific one.

- **all**: Specifies that the new call policy will be applied to all instances of the selected service type.
- **name: service_name**: Specifies the name of a specific instance of the selected service type as an alphanumeric string of 1 through 63 characters that is case sensitive.

redirect target_ip_address [ weight weight_num ] [ target_ip_address2 [ weight weight_num ] ... target_ip_address16 [ weight weight_num ]

Configures the busy-out action. When a redirect policy is invoked, the service rejects new sessions and provides the IP address of an alternate destination. This command can be issued multiple times. target_ip_address# is the IP address of an alternate destination expressed in IPv4 dotted-decimal notation. Up to 16 IP addresses can be specified either in one command or by issuing the redirect command multiple times. If you try to add more than 16 IP addresses to the redirect policy the CLI issues an error message. If you specify an IP address and weight that already exists in the redirect policy the new values override the existing values.

- **weight weight_num**: When multiple addresses are specified, they are selected in a weighted round-robin scheme. Entries with higher weights are more likely to be chosen. If a weight is not specified the entry is automatically assigned a weight of 1. weight_num must be an integer from 1 through 10.

Depending on the type of service that the policy is applied to, the following reason codes are reported as part of the reply:

- **ha service**: 88H (Registration Denied - unknown home agent address)
- **pdsn service**: 88H (Registration Denied - unknown PDSN address)
### Exec Mode Commands (D-S)

**Important:** The redirect option is not supported for use with FA and GGSN services.

```
newcall policy hnbgw-service { all | name service_name } reject
```

Creates a new call policy to reject the calls in a specified HNB-GW service name instance or all HNB-GW services on the system.

- **name service_name**: Specifies the name of the HNB-GW service for which new call policy is configured.
- **reject**: Specifies that the policy rejects all new incoming calls. Depending on the type of service that the policy is applied to, the reason codes are reported as part of the reply to indicate the rejection. For HNB-GW service rejection code is 81H (Registration Denied - administratively prohibited).

```
newcall policy mme-service { all | name service_name } reject
```

Creates a new call policy to reject the calls based on the specified MME service name or all MME services on the system.

- **name service_name**: Specifies the name of the MME service for which new call policy is configured.
- **reject**: Specifies that the policy rejects new incoming calls. Depending on the type of service that the policy is applied to, the reason codes are reported as part of the reply to indicate the rejection. For MME service rejection code is 81H (Registration Denied - administratively prohibited).

```
newcall policy { pcc-af-service | pcc-policy-service | pcc-quota-service} { all | name service_name } reject
```

Creates a new call policy to reject the calls for PCC services on the system for any of the following PCC services:

- **pcc-af-service name service_name**: Specifies the Policy and Charging Control-Application Function (PCC-AF) service for which new call policy is to be configured on the system.
  - **name service_name**: Specifies the name of an existing PCC-AF service for which new call policy is configured.
- **pcc-policy-service name service_name**: Specifies the Policy and Charging Control-Policy (PCC-Policy) service for which new call policy is to be configure on the system.

**Important:** When `newcall policy` is set to reject for the FA service, the Busy Bit is set in the Agent Advertisement. Any further RRQs will be rejected with this code value.

```
rej
```

Specifies that the policy rejects new incoming calls. Depending on the type of service that the policy is applied to, the following reason codes are reported as part of the reply to indicate the rejection:

- **asngw service**: 81H (Registration Denied - administratively prohibited)
- **fa service**: 41H (administratively prohibited)

```
rej
```

**Important:** The redirect option is not supported for use with FA and GGSN services.
**newcall policy**

```markdown
name service_name: Specifies the name of an existing PCC-Policy service for which new call policy is configured.

reject: Specifies that the policy rejects new incoming calls. Depending on the type of service that the policy is applied to, the reason codes are reported as part of the reply to indicate the rejection. For PCC services rejection code is 81H (Registration Denied - administratively prohibited).
```

### newcall policy pgw-service { all | name service_name } reject

Creates a new call policy to reject the calls based on the specified P-GW service name or all P-GW services (and any SAEGW service associated with the P-GW service) in this context.

- **all**: Rejects all P-GW services on the system. Specifies that the new call policy will be applied to all instances of the P-GW service, and any associated SAEGW service, in this context.
- **name service_name**: Specifies the name of the P-GW service, and any SAEGW service associated with this P-GW service, for which new call policy is configured.
- **reject**: Specifies that the policy rejects new incoming calls. Depending on the type of service that the policy is applied to, the reason codes are reported as part of the reply to indicate the rejection.

### newcall policy saegw-service { all | name service_name } reject

Creates a new call policy to reject the calls based on the specified SAEGW service name or all SAEGW services on the system.

- **name service_name**: Specifies the name of the SAEGW service for which new call policy is configured.
- **reject**: Specifies that the policy rejects new incoming calls. Depending on the type of service that the policy is applied to, the reason codes are reported as part of the reply to indicate the rejection.

### newcall policy sgw-service { all | name service_name } reject

Creates a new call policy to reject the calls based on the specified S-GW service name or all S-GW services on the system.

- **name service_name**: Specifies the name of the S-GW service for which new call policy is configured.
- **reject**: Specifies that the policy rejects new incoming calls. Depending on the type of service that the policy is applied to, the reason codes are reported as part of the reply to indicate the rejection.

### Usage

This command is used to busy-out specific system services prior to planned maintenance or for troubleshooting. This is required when operator find out that the system is somehow overloaded, or needs some kind of maintenances or so.

### Example

The following command creates a new call policy to re-direct all new calls for all PDSN services to a device having an IP address of 192.168.1.23:

```
newcall policy pdsn-service all redirect 192.168.1.23
```

The following command creates a new call policy to reject all new calls for a GGSN service called `ggsn1`:

```
newcall policy ggsn-service name ggsn1 reject
```

The following command creates a new call policy to reject all new calls for an MME service called `MME1`:

```
newcall policy mme-service name MME1 reject
```

The following command creates a new call policy to reject all new calls for an HNB-GW service called `hnbgw1`:
newcall policy hnbw-service name hnbwl reject

The following command creates a new call policy to reject all new calls for a PCC Policy service called pcrf1:

newcall policy pcc-policy-service name pcrf1 reject
password change

Provides a mechanism for local-user administrative users to change their passwords.

Product
All

Privilege
All local-user administrative levels except as noted below

Mode
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

password change [ local-user name ]

local-user name
Specifies the name of an existing local-user administrative user for which to change the password as an alphanumeric string of 3 through 144 characters that is case sensitive.

Important: This keyword is only available to local-users with an authorization level of security-administrator.

Usage
This command provides a mechanism for local-user administrative users to change their passwords. In addition, it also provides a mechanism for security-administrator local-users to change the password for other local-user accounts.
If the local-user keyword is not entered, the system prompts the user for their current password and for the new password. New passwords take effect at the next login. Users that have had their password changed by a security-administrator are prompted to change their passwords at their next login.
New passwords must meet the criteria dictated by the local-user password command options in the Global Configuration Mode.

Important: The system does not allow the changing of passwords unless the time limit specified by the local-user password min-change-interval has been reached.

Example
The following command, executed by a security-administrator, resets the password for a local-user name operator12:

    password change local-user operator12
patch plugin

Copies a patch intended for a specific plugin module onto the system. This function is associated with the patch process for accommodating dynamic software upgrades.

Product
ADC

Privilege
Security Administrator, Administrator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

`patch plugin plugin_name filepath certificate filepath`

*plugin_name*
Specifies the name of an existing plugin that will be copied onto the system as an alphanumerical string of 1 through 16 characters.

*certificate*
Specifies the name of a certificate associated with the plugin that will be copied onto the system as an alphanumerical string of 1 through 16 characters.

*filepath*
Specifies the location of the file to copy. The path must be formatted as follows:

For the ASR 5000:

```
[ file: ]{ /flash | /pcmcia1 | /hd }[ /directory ]/file_name
```

**Important**: Use of the ASR 5000 SMC hard drive is not supported in this release.

For the ASR 5500:

```
[ file: ]{ /flash | /usb1 | /hd }[ /directory ]/file_name
```

**Important**: Do not use the following characters when entering a string for the field names below: “/” (forward slash), “:” (colon) or “@” (at sign).

*directory* is the directory name.
*filename* is the actual file of interest.
Usage
Use this command to verify and copy a patch onto the system. After the patch has been copied onto the system, you must run the `install plugin` command to unpack the kit and validate its contents.

Example
To copy the plugin module named `p2p` onto the system enter the following command:

```
patch plugin p2p http://192.168.1.2/tmp/libp2p-1.2.0.tgz certificate http://192.168.1.2/tmp/1.2.0.cert
```

When the patch has been successfully copied the following message appears:

```
New patch for plugin p2p available for installation
```
ping

Verifies ability to communicate with a remote node in the network by passing data packets between and measuring the response. This is accomplished by sending IPv4 Internet Control Message Protocol (ICMP) echo request packets to the target node (pinging) and waiting for an ICMP response.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Important: Inspector privileges are granted for all variables except count. To initiate a ping count, you must have a minimum privilege level of Operator.

Syntax

ping { hostname | ip_address } [ broadcast ] [ count num_packets ] [ pattern packet_pattern ] [ size octet_count ] [ src { src_host_name | src_host_ip_address } ]

hostname
Sends ICMP echo request packets to the remote node specified the node’s name (up to 127 alphanumeric characters) or assigned IPv4 address in dotted-decimal notation.

ip_address
IPv4 address of host to be pinged in dotted-decimal notation.

broadcast
Sends ping packets to broadcast addresses.

count num_packets
Specifies the number of packets to send to the remote host for verification as an integer from 1 through 10000. Default: 5

pattern packet_pattern
Specifies a pattern to use to fill the internet control message protocol packets in hexadecimal format with a value in the range of 0x0000 through 0xFFFF. By default each octet of the packet is encoded with the octet number of the packet.

size octet_count
Specifies the number of bytes in each IP datagram as an integer from 40 through 18432. Default: 56
**src host_ip_address**

Specifies the source IP address in IPv4 dotted-decimal notation. Default: originating system’s IP address

---

### Usage

This command is useful in verifying network routing and if a remote node is able to respond at the IPv4 layer.

The following command is the most basic and will report the results of trying to communicate with remote node `remoteABC`.

```
ping remoteABC
```

The following command verifies communication with the remote node `10.2.3.4` using `1000` packets.

```
ping 10.2.3.4 count 1000
```

The following command verifies communication with remote node `remoteABC` while making it appears as though the source is remote node with IP address `10.2.3.4`.

```
ping remoteABC src 10.2.3.4
```

---

**Important:** The responses from the remote host to the ping packets will be rerouted to the host specified as the source.
ping6

Verifies ability to communicate with a remote node in the network by passing data packets between and measuring the response. This is accomplished by sending IPv6 Internet Control Message Protocol (ICMP) echo request packets to the target node (pinging) and waiting for an ICMP response.

**Product**
All

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
ping6 { hostname | ipv6_address } [ count num ] [ flood ] [ pattern val ] [ size val ] [ src ip_address ] [ interface string ] [ vrf vrf_name
```

**host_name**
Name of the host to be pinged.

**ipv6_address**
IPv6 address of host to be pinged in colon-separated-hexadecimal notation.

**count num**
Sets the number of ping packets to be sent as an integer from 1 through 10000.

**flood**
Configures ping6 to send packets as quickly as possible, or 100 per second, whichever is faster.

**pattern val**
Specifies the hexadecimal pattern to fill ICMP packets as a hexadecimal number from 0x0 through 0xffff

**size val**
Specifies the size of ICMP datagram (in bytes) as an integer from 40 through 18432. Default: 56.

**src ip_address**
Specifies the source IP address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation. Default: originating system’s IP address

**vrf name**
Specifies the name of an existing VFR as an alphanumeric string of 1 through 63 characters.
**Usage**

This command is useful in verifying network routing and if a remote node is able to respond at the IPv6 layer.

**Example**

Use this command to ping the IPv6 address 2001:0db8:85a3:0000:0000:8a2e:0370:7334

```plaintext
ping6 2001:0db8:85a3:0000:0000:8a2e:0370:7334
```
**port switch to**

Performs a manual switchover to an available redundant/standby line card, SPIO port, or MIO port.

Default: none.

**Product**

All

**Privilege**

Security Administrator, Administrator, Operator

**Mode**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name# 
```

**Syntax**

```
port switch to slot#/por# 
```

---

**Usage**

This command is used to specify the redundant port on a Line Card (LC) or MIO. When port redundancy is enabled, if an external network device or cable failure occurs that causes a link down failure on the port, then the redundant port is used.

---

**Important:** This command is not supported on all platforms.

**Example**

```
port switch to 17/1
```

```
port switch to 6/11
```
ppp echo-test

Sends link control protocol (LCP) keep-alive echo packet to the peer point-to-point protocol (PPP) connection to verify proper communication between PPP connections, and awaits a response.

Product
PDSN
GGSN

Privilege
Security Administrator, Administrator, Operator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

ppp echo-test { callid call_id | imsi imsi_id | ipaddr ip_address | msid ms_id | username user_name } [ num_packets ] [ | { grep grep_options | more } ]

**callid call_id**
Specifies the call instance ID for which the PPP link must be verified as a 4-byte hexadecimal number.

**imsi imsi_id**
Specifies the International Mobile Subscriber Identifier (IMSI) for which the PPP link must be verified.

**ipaddr ip_address**
Specifies the IP address for which the PPP link must be verified in IPv4 dotted-decimal notation.

**msid ms_id**
Specifies the mobile subscriber ID for which the PPP link must be verified as 7 to 16 digits of an MIN, or RMI.

**username user_name**
Specifies an existing user for which the PPP link must be verified as an alphanumeric string of 1 through 127 characters.

**num_packets**
Specifies the number of test packets to generate an integer from 1 through 1000000. Default: 1

**grep grep_options | more**
Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command’s Output* section of the Command Line Interface Overview chapter in Command Line Interface Reference.
Usage

Use this command to verify the point-to-point protocol communications. This command sends LCP keep-alive echo packet to the peer PPP connection to verify proper communication between PPP connections. `ppp echo-test` command waits for LCP echo response for configured numbers of tries, if response is not received it will retry configured no of times with an interval of 5 seconds. This command accepts the parameters call ID, IMSI, IP address, MSID, and user name to specify which active PPP session to consider. `ppp echo-test` command makes the dormant session active.

⚠️ Caution: Issuing this command could negatively impact system performance depending on the number of subscribers using the same name and/or if the number of packets used in the test is large.

LCP includes Echo-Request and Echo-Reply codes in order to provide a Data Link Layer loopback mechanism for use in exercising both directions of the link. This is useful as an aid in debugging, link quality determination, performance testing, and for numerous other functions. Upon reception of an Echo-Request in the LCP Opened state, an Echo-Reply is transmitted.

Example

The following command tests the PPP link to user user1.

```
ppp echo-test username user1
```

The following command tests the PPP link to the user assigned IP address 10.2.3.4.

```
ppp echo-test ipaddr 10.2.3.4
```

The following tests the PPP link associated with call ID fe80aa12.

```
ppp echo-test callid fe80aa12
```
radius interim accounting now

Check points current RADIUS accounting messages immediately.

**Product**
- PDSN
- GGSN
- ASN-GW

**Privilege**
- Security Administrator, Administrator, Operator

**Mode**
- Exec
  
  The following prompt is displayed in the Exec mode:

  
  ![local]host_name#

**Syntax**

```
radius interim accounting now
```

**Usage**

The interim command may be part of a regiment of periodic activities to maintain the chassis. This command may also be useful in preparation for system monitoring or troubleshooting to set the list of messages to be displayed at a well known time.
radius test

Verifies the RADIUS servers functions for accounting and authentication.

Product
PDSN
GGSN
ASN-GW

Privilege
Security Administrator, Administrator, Operator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

radius test { accounting | admin authentication | authentication | probe authentication server ip_addr port port_no [ username username password password ] } { all | [ on ] | off } | radius group group_name user_name | server server_name port server_port } user_name password

accounting
Tests accounting server functionality.

admin authentication name_admin admin_password
Tests the RADIUS admin authentication.
name_admin: Specifies he name of the administrator as an alphanumeric string of 1 through 127 characters.
admin_password: Specifies the password for the administrator as an alphanumeric string of 1 through 63 characters.

authentication
Tests authentication server functionality.

all | radius group group_name user_name | server server_name port server_port
all: Tests all configured servers.
server server_name port server_port: Tests only the server specified by server_name and server_port. The server must have been previously configured.

radius group group_name user_name: Tests all configured authentication servers in a specific RADIUS group for a specific user. Must be followed by the RADIUS group name and user name.
group_name is an alphanumeric string of 1 through 63 characters that specifies the name of server group configured in the specific context for authentication/accounting.
on/off
Allows the user to turn RADIUS test accounting on or off.
user_name
Specifies the RADIUS user who is to be verified. The user must have been previously configured.

password
Specifies the RADIUS user who is to have authentication verified. password is only applicable when the authentication keyword is specified.

Usage
Test the RADIUS accounting for troubleshooting the system for specific users or to verify all the system RADIUS accounting functions.

Example
The following verifies all RADIUS servers.

```
radius test accounting all
radius test authentication all
```

The following verifies the RADIUS accounting and authentication for user user1 for the sampleServer.

```
radius test accounting server sampleServer port 5000 user1
radius test authentication server sampleServer port 5000 user1 dummyPwd
```

The following commands will verify the RADIUS accounting and authentication for RADIUS server group star1 for the current context:

```
radius test accounting server sampleServer port 5000 user1
radius test authentication server sampleServer port 5000 user1 dummyPwd
radius test authentication all
```

The following verifies the RADIUS authentication server group star1 for user user1.

```
radius test authentication radius group star1 user1
```
reload

Invokes a full system reboot. All processes are terminated and the system initiates a hardware reset (reboot). This command is identical to the `shutdown` command.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec
The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
reload [ -noconfirm ]
```

- `-noconfirm`
  
  Executes the command without any additional prompts or confirmation from the user.

**Usage**

The system performs a hardware reset and reloads the highest priority boot image and configuration file specified in the boot.sys file. Refer to the `boot system priority` command in the Global Configuration Mode for additional information on configuring boot images, configuration files and priorities.

⚠️ **Important:** To avoid the abrupt termination of subscriber sessions, it is recommended that a new call policy be configured and executed prior to invoking the `reload` command. This policy sets busy-out conditions for the system and allows active sessions to terminate gracefully. Refer to the `newcall` command in the Exec Mode for additional information.

⚠️ **Caution:** Issuing this command causes the system to become unavailable for session processing until the reboot process is complete.

**Example**

The following command performs a hardware reset on the system:

```
reload
```
rename

Changes the name of an existing local file.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

rename from_filepath to_filepath [ -noconfirm ]

from_filepath

Specifies the path to the file/directory to be renamed. The path must be formatted according to the following format:

For the ASR 5000:

[ file:]{/flash | /pcmcia 1 | /hd-raid }[/directory ]/file_name

For the ASR 5500:

[ file:]{/flash | /usb 1 | /hd-raid }[/directory ]/file_name

Important: Use of the SMC hard drive is not supported in this release.

Important: Do not use the following characters when entering a string for the field names below: “/” (forward slash), “:” (colon) or “@” (at sign).

directory is the directory name
filename is the actual file of interest

to_filepath

Specifies the path to the file/directory to be renamed. The path must be formatted according to the following format:

For the ASR 5000:

[ file:]{/flash | /pcmcia 1 | /hd }[/directory ]/file_name

For the ASR 5500:
rename [ file: ]{ /flash | /usb1 | /hd } [ /directory ]/file_name

**Important:** Use of the SMC hard drive is not supported in this release.

directory is the directory name
filename is the actual file of interest

-noconfirm
Executes the command without any additional prompt and confirmation from the user.

**Caution:** Extreme caution should be taken when using the -noconfirm option. The paths to the source and the destination should be verified prior to performing the command.

**Usage**
Rename files as part of regular system maintenance in conjunction with the delete command.

**Example**
The following renames the directory /pub in the local PCMCIA1 device.

rename /pcmcia1/pub /pcmcia1/pub_old

The following renames the directory /pub in the local USB device.

rename /usb1/pub /usb1/pub_old
reset alcap-service

Resets a named Access Link Control Application Part (ALCAP) protocol service. ALCAP is the protocol used for the control plane of the UMTS transport layer. It manages and multiplexes users into ATM AAL2 virtual connections.

**Product**
All

**Privilege**
Security Administrator, Administrator, Operator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

**Syntax**

```
reset alcap-service srvc_name aal2 node node_name aal2-path { path_name | all }
```

- **srvc_name**
  Specifies the name of an existing ALCAP service as an alphanumeric string of 1 through 63 characters.

- **aal2 node node_name**
  Specifies the name of an existing ATM Adaptation Layer 2 (AAL2) node as an alphanumeric string of 1 through 64 characters.

**Usage**

Reset a named ALCAP service for a specified AAL2 node.

**Example**

The following command resets the ALCAP service *alcap_01* for the AAL2 node *aal2_1001*, all paths:

```
reset alcap-service alcap_01 aal2-node aal2_1001 aal2-path all
```
reveal disabled commands

Enables or disables the input of commands for features that do not have license keys installed. The output of the command `show cli` indicates when this feature is enabled. This command effects the current CLI session only and is disabled by default.

**Product**
All

**Privilege**
Security Administrator, Administrator, Operator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
[ no ] reveal disabled commands
```

- **no**
  
  Does not show disabled commands.

**Usage**

When this command is enabled and a disabled command is entered, a message is displayed that informs you that the required feature is not enabled and also lists the name of the feature that you need to support the command.

When this command is disabled and a disabled command is entered, the CLI does not acknowledge the existence of the command and displays a message that the keyword is unrecognized.

**Example**

The following command sets the CLI to accept disabled commands and display the required feature for the current CLI session with the following command:

```
reveal disabled commands
```

The following command sets the CLI to reject disabled commands and return an error message for the current CLI session:

```
no reveal disabled commands
```
rlogin

Attempts to connect to a remote host.

Product
All

Privilege
Security Administrator, Administrator, Operator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

rlogin { host_name | host_ip_address } [ user user_name ]

host_name | host_ip_address
Identifies the remote node with which to attempt connection.
host_name: Specifies the remote node using the node’s logical host name which must be resolved via DNS lookup.
host_ip_address: Specifies the remote node using its assigned IP address in IPv4 dotted-decimal notation.

user user_name
Specifies a user name attempting connection as an alphanumeric string of 1 through 1023 characters.

Usage

Connect to remote network elements using rlogin.

**Important:** rlogin is not a secure method of connecting to a remote host. ssh should be used whenever possible for security reasons.

Example

The following connects to remote host remoteABC as user user1.

```
rlogin remoteABC user user1
```

The following connects to remote host 10.2.3.4 without any default user.

```
rlogin 10.2.3.4
```
rmdir

Removes (deletes) a local directory.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
rmdir path [ force ]
```

**path**

Specifies the directory path to remove. The must be formatted according as follows:

For the ASR 5000:

```
[ file: ]{ /flash | /pcmcia1 | /hd-raid }[ /directory ]/file_name
```

For the ASR 5500:

```
[ file: ]{ /flash | /usb1 | /hd-raid }[ /directory ]/file_name
```

**Important:** Do not use the following characters when entering a string for the field names below: “/” (forward slash), “:” (colon) or “@” (at sign).

- directory is the directory name
- filename is the actual file of interest

**force**

Over-rides any warnings to force deletion of the directory and any files contained therein.

**Important:** Use of the `force` keyword should be done with care to ensure the directory is specified accurately as there is no method to recover a directory which has been removed.

**Usage**

Remove old directories as part of regular maintenance.

**Example**

The following removes the local directory `/pcmcia/pub`.

```
rmdir /pcmcia/pub
```
rollback module

Loads a specified software plugin module from the Version Priority List (VPL) with the next higher priority number. This function is associated with the patch process for accommodating dynamic software upgrades.

**Product**
ADC

**Privilege**
Security Administrator, Administrator

**Mode**
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

**Syntax**

```
rollback module plugin_name
```

**Usage**

Specifies the name of an existing plugin module that you want to downgrade as an alphanumeric string of 1 through 16 characters. If the named module is not known to the system, an error message is displayed.

**Example**

To load the next plugin module named p2p enter the following command:

```
rollback module p2p
```
rotate-hd-file

Rotates the Diameter files stored on the hard disk drive.

Product

HSGW
P-GW
SAEGW
S-GW

Privilege

Security Administrator, Administrator

Mode

Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

rotate-hd-file diameter [ name policy_name ]

day name policy_name

Specifies the hd-storage policy name of an existing HD Storage Policy as an alphanumeric string of 0 through 63 characters.

Usage

Use this command to manually rotate the Diameter HD stored files.

Example

The following command rotates Diameter files that were stored using the HD storage policy named CDR1:

    rotate-hd-file diameter name CDR1
**save configuration**

Saves the configuration of current contexts to a local or remote location. The configuration contains the sequence of CLI commands that define system parameters and ends with the `.cfg` extension.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Mode**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
save configuration url [ obsolete-encryption | showsecrets | verbose ] [ -redundant ] [ -noconfirm ]
```

**url**

Default: saves to the location of the active configuration currently loaded. Specifies the location in which to store the configuration file. `url` may refer to a local or a remote file and must be entered in the following format:

For the ASR 5000:

```
```

```
tftp:// { host [ : port# ] } [ /directory ] /file_name
```

```
```

For the ASR 5500:

```
```

```
tftp:// { host [ : port# ] } [ /directory ] /file_name
```

```
```

**Important:** Do not use the following characters when entering a string for the field names below: “/” (forward slash), “:” (colon) or “@” (at sign).

- `directory` is the directory name.
- `filename` is the actual file of interest.
- `username` is the user to be authenticated.
- `password` is the password to use for authentication.
- `host` is the IP address or host name of the server.
**Important:** *host* can only be used if the *networkconfig* parameter is configured for DHCP and the DHCP server returns a valid nameserver.

The following file transfer protocols are supported on all platforms to save the configuration to a destination on the network (off box):

- `tftp` – Trivial File Transfer Protocol [no username/password required]
- `ftp` – File Transfer Protocol [username/password required]
- `sftp` – SSH File Transfer Protocol [SSH username/password required]

`port#` is the logical port number that the communication protocol is to use.

```plaintext
[ obsolete-encryption | showsecrets | verbose ]
```

Specifies options when saving the configuration file.

- **obsolete-encryption**: Saves the configuration with encrypted values generated via an obsolete encryption method. This option may be required to preserve a configuration for a possible downgrade.
- **showsecrets**: Saves the CLI configuration file with all passwords in plain text, rather than their default encrypted format.
- **verbose**: Saves as much information as possible, including default values. If this option is not specified, the configuration will not include default values.

**-redundant**

Saves the configuration file to the local device on the management card, defined by the *url* variable, and then automatically copies that same file to the like device on the standby management card, if available.

The management card can be any of the following:

- ASR 5000 – System Management Card (SMC) [/flash or pcmcia1]
- ASR 5500 – Management Input/Output (MIO) card [/flash, usb1, usb2]

Use the **-redundant** keyword if you have only made changes to the configuration, but not to the boot order or after installing a new boot image. Changes to the boot order or installing a new image requires file synchronization via the `filesystem synchronize` command.

**Important**: This keyword will only work for local devices that are located on both the active and standby management cards. Otherwise, a failure message is displayed. When saving the file to an external network (non-local) device, the system disregards this keyword.

**Important**: This keyword does not synchronize the local file system. If you have added, modified, or deleted other files or directories to or from a local device for the active management card, then you must synchronize the local file system on both cards.

**-noconfirm**

Executes the command without any additional prompt and confirmation from the user.

**Caution**: Exercise caution when using the **-noconfirm** option as this will overwrite data if the URL targets an existing file.
save configuration

Usage
Backup the current configuration as part of periodic maintenance activities for emergency recovery.

Important: Saving a configuration does not save the boot options as configured via the Global Configuration mode boot commands.

Example
The following saves the configuration data to the local file /flash/pub/juneconfig.cfg with no confirmation from the user:

save configuration /flash/pub/juneconfig.cfg -noconfirm

The following saves the configuration data to remote host remoteABC at /pub/juneconfig.cfg:

save configuration tftp://remoteABC/pub/juneconfig.cfg
save logs

Saves the current log file to a local or remote location.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

save logs { url } [ active ] [ inactive ] [ callid call_id ] [ event-verbosity evt_verbosity ] [ facility facility ] [ level severity_level ] [ pdu-data pdu_format ] [ pdu-verbosity pdu_verbosity ] [ since from_date_time [ until to_date_time ] ] [ | { grep grep_options | more } ]

url

Specifies the location to store the log file(s). url may refer to a local or a remote file and must be entered in the following format.

For the ASR 5000:


tftp:// { host [ : port# ] } [ /directory ] /file_name


Important: Use of the SMC hard drive is not supported in this release.

For the ASR 5500:


tftp:// { host [ : port# ] } [ /directory ] /file_name


Important: Do not use the following characters when entering a string for the field names below: “/” (forward slash), “:” (colon) or “@” (at sign).
directory is the directory name.
filename is the actual file of interest.
username is the user to be authenticated.
password is the password to use for authentication.
host is the IP address or host name of the server.

**Important:** hostname can only be used if the networkconfig parameter is configured for DHCP and the DHCP server returns a valid nameserver.

port# is the logical port number that the communication protocol is to use.

**active**
Saves data from active logs.

**inactive**
Saves data from inactive logs.

**callid** call_id
Specifies a call ID for which log information is to be saved as a 4-byte hexadecimal number.

**event-verbosity** evt_verboseness
Specifies the level of verboseness to use in displaying of event data as one of:
- **min**: Logs minimal information about the event. Information includes event name, facility, event ID, severity level, date, and time.
- **concise**: Logs detailed information about the event, but does not provide the event source within the system.
- **full**: Logs detailed information about event, including source information, identifying where within the system the event was generated.

**facility** facility
Specifies the facility to modify the filtering of logged information. Valid facilities for this command are:
- **a10**: A10 interface facility
- **a11**: A11 interface facility
- **a11mgr**: A11 Manager facility
- **aaa-client**: Authentication, Authorization and Accounting (AAA) client facility
- **aaamgr**: AAA manager logging facility
- **aaaprox**: AAA Proxy facility
- **aal2**: ATM Adaptation Layer 2 (AAL2) protocol logging facility
- **acl-log**: Access Control List (ACL) logging facility
- **acsctrl**: Active Charging Service (ACS) Controller facility
- **acsmgr**: ACS Manager facility
- **afctrl**: Fabric Controller facility [ASR 5500 only]
- **afmng**: Fabric Manager logging facility [ASR 5500 only]
• alarmctrl: Alarm Controller facility
• alcap: Access Link Control Application Part (ALCAP) protocol logging facility
• alcapmgr: ALCAP manager logging facility
• all: All facilities
• asngwmgr: Access Service Network (ASN) Gateway Manager facility
• asnpcmgr: ASN Paging Controller Manager facility
• bfd: Bidirectional Forwarding Detection (BFD) protocol logging facility
• bgp: Border Gateway Protocol (BGP) facility
• bindmux: IPCF BindMux-Demux Manager logging facility
• bngmgr: Broadband Network Gateway (BNG) Demux Manager logging facility
• bssap+: Base Station Sub-system Application Part+ protocol facility for the login interface between the SGSN and the MSC/VLR (2.5G and 3G)
• bssgp: Base Station Sub-system GPRS Protocol logging facility handles exchange information between the SGSN and the BSS (2.5G only)
• callhome: Call Home application logging facility
• cap: CAMEL Application Part (CAP) logging facility for protocol used in prepaid applications (2.5G and 3G)
• cbsmgr: Cell Broadcasting Service (CBS) logging facility [HNBGW]
• cdf: Charging Data Function (CDF) logging facility
• cgw: Converged Access Gateway (CGW) logging facility
• cli: Command Line Interface (CLI) logging facility
• cmp: Certificate Management Protocol (IPSec) logging facility
• connectedapps: SecGW ASR 9000 oneP communication protocol
• connproxy: Controller Proxy logging facility
• credit-control: Credit Control (CC) facility
• cscf: IMS/MMD Call Session Control Function (CSCF)
• cscfcpmgr: CSCFCPMGR logging facility
• cscfmgr: SIP CSCF Manager facility
• cscfnpdb: CSCF Number Portability Database (NPDB) logging facility
• cscfrtcp: IMS/MMD CSCF RTCP log facility
• cscfrtp: IMS/MMD CSCF RTP log facility
• cscfttmgr: SIP CSCF Tunnel and Transport Manager facility
• csp: Card/Slot/Port controller facility
• css: Content Service Selection (CSS) facility
• css-sig: CSS RADIUS Signaling facility
• cx-diameter: Cx Diameter Messages facility [CSCF <--> HSS]
• dcardctrl: IPSec Daughter Card Controller logging facility
• dcardmgr: IPSec Daughter Card Manager logging facility
• **demuxmgr**: Demux Manager API facility
• **dgmbmgr**: Diameter Gmb Application Manager logging facility
• **dhcp**: Dynamic Host Configuration Protocol (DHCP) logging facility
• **dhcpv6**: DHCPv6
• **dhost**: Distributed Host logging facility
• **diabase**: Diabase messages facility
• **diameter**: Diameter endpoint logging facility
• **diameter-acct**: Diameter Accounting
• **diameter-auth**: Diameter Authentication
• **diameter-dns**: Diameter DNS subsystem
• **diameter-ecs**: ACS Diameter signaling facility
• **diameter-hdd**: Diameter Horizontal Directional Drilling (HDD) Interface facility
• **diameter-svc**: Diameter Service
• **diamproxy**: DiamProxy logging facility
• **dpath**: IPSec Data Path facility
• **drvctrl**: Driver Controller facility
• **doulosuemgr**: Doulus (IMS-IPSec-Tool) user equipment manager
• **eap-diameter**: Extensible Authentication Protocol (EAP) IP Security facility
• **eap-ipsec**: Extensible Authentication Protocol (EAP) IPSec facility
• **eap-sta-s6a-s13-s6b-diameter**: EAP/STA/S6A/S13/S6B Diameter messages facility
• **ecs-css**: ACSMGR <-> Session Manager Signalling Interface facility
• **egtpc**: eGTP-C logging facility
• **egtpmgr**: enhanced GPRS Tunneling Protocol (eGTP) manager logging facility
• **egtpu**: eGTP-U logging facility
• **epdg**: evolved Packet Data (ePDG) gateway logging facility
• **event-notif**: Event Notification Interface logging facility
• **evlog**: Event log facility
• **famgr**: Foreign Agent manager logging facility
• **firewall**: Firewall logging facility
• **fng**: Femto Network Gateway (FNG) logging facility
• **gbmgr**: SGSN Gb Interface Manager facility
• **gmm**:
  • For 2.5G: Logs the GPRS Mobility Management (GMM) layer (above LLC layer)
  • For 3G: Logs the access application layer (above the RANAP layer)
• **gprs-app**: GPRS Application logging facility
• **gprs-ns**: GPRS Network Service Protocol (layer between SGSN and the BSS) logging facility
• **gq-rx-tx-diameter**: Gq/Rx/Tx Diameter messages facility
• **gss-gcdr**: GTPP Storage Server GCDR facility
• **gtpc**: GTP-C protocol logging facility
• **gtpcmgr**: GTP-C protocol manager logging facility
• **gtp**: GTP-prime protocol logging facility
• **gtpu**: GTP-U protocol logging facility
• **gtpumgr**: GTP-U Demux manager
• **gx-ty-diameter**: Gx/Ty Diameter messages facility
• **gy-diameter**: Gy Diameter messages facility
• **h248prt**: H.248 port manager facility
• **hamgr**: Home Agent manager logging facility
• **hat**: High Availability Task (HAT) process facility
• **hdctrl**: HD Controller logging facility
• **henbapp**: Home Evolved NodeB (HENB) App facility
• **henbgw**: HENB-GW facility
• **henbgw-pws**: HENB-GW Public Warning System logging facility
• **henbgw-sctp-acb**: HENB-GW access Stream Control Transmission Protocol (SCTP) facility
• **henbgw-sctp-nw**: HENBGW network SCTP facility
• **henbgwdemux**: HENB-GW Demux facility
• **henbgwmanager**: HENB-GW Manager facility
• **hnb-gw**: HNB-GW (3G Femto GW) logging facility
• **hnbmgr**: HNB-GW Demux Manager logging facility
• **hss-peer-service**: Home Subscriber Server (HSS) Peer Service facility
• **igmp**: Internet Group Management Protocol (IGMP)
• **ikev2**: Internet Key Exchange version 2 (IKEv2)
• **ims-authorizatn**: IP Multimedia Subsystem (IMS) Authorization Service facility
• **ims-sh**: HSS Diameter Sh Interface Service facility
• **imsimgr**: SGSN IMSI Manager facility
• **imsue**: IMS User Equipment (IMSUE) facility
• **ip-arp**: IP Address Resolution Protocol facility
• **ip-interface**: IP interface facility
• **ip-route**: IP route facility
• **ipms**: Intelligent Packet Monitoring System (IPMS) logging facility
• **ipne**: IP Network Enabler (IPNE) facility
• **ips**: IP Security logging facility
• **ipsg**: IP Service Gateway interface logging facility
• **ipsgmgr**: IP Services Gateway facility
• **ipsp**: IP Pool Sharing Protocol logging facility
save logs

- **kvstore**: Key/Value Store (KVSTORE) Store facility
- **l2tp-control**: Layer 2 Tunneling Precool (L2TP) control logging facility
- **l2tp-data**: L2TP data logging facility
- **l2tpdemux**: L2TP Demux Manager logging facility
- **l2tpmgr**: L2TP Manager logging facility
- **lagmgr**: Link Aggregation Group (LAG) manager logging facility
- **lcs**: Location Services (LCS) logging facility
- **ldap**: Lightweight Directory Access Protocol (LDAP) messages logging facility
- **li**: Refer to the *Lawful Intercept Interface Reference* for a description of this command.
- **linkmgr**: SGSN/BSS SS7 Link Manager logging facility (2.5G only)
- **llc**: Logical Link Control (LLC) Protocol logging facility; for SGSN: logs the LLC layer between the GMM and the BSSGP layers for logical links between the MS and the SGSN
- **local-policy**: Local Policy Service facility
- **location-service**: Location Services facility
- **m3ua**: M3UA Protocol logging facility
- **magmgr**: Mobile Access Gateway manager logging facility
- **map**: Mobile Application Part (MAP) protocol logging facility
- **megadiammgr**: MegaDiameter Manager (SLF Service) logging facility
- **mme-app**: Mobility Management Entity (MME) Application logging facility
- **mme-misc**: MME miscellaneous logging facility
- **mmedemux**: MME Demux Manager logging facility
- **mmemgr**: MME Manager facility
- **mmgr**: Master Manager logging facility
- **mobile-ip**: Mobile IP processes
- **mobile-ip-data**: Mobile IP data facility
- **mobile-ipv6**: Mobile IPv6 logging facility
- **mpls**: Multiprotocol Label Switching (MPLS) protocol logging facility
- **mrmr**: Multi Radio Mobility Entity (MRME) logging facility
- **mseg-app**: Mobile Services Edge Gateway (MSEG) application logging facility (This option is not supported in this release.)
- **mseg-gtpc**: MSEG GTP-C application logging facility (This option is not supported in this release.)
- **mseg-gtpu**: MSEG GTP-U application logging facility (This option is not supported in this release.)
- **msegmgr**: MSEG Demux Manager logging facility (This option is not supported in this release.)
- **mtp2**: Message Transfer Part 2 (MTP2) Service logging facility
- **mtp3**: Message Transfer Part 3 (MTP3) Protocol logging facility
- **multicast-proxy**: Multicast Proxy logging facility
- **nas**: Non-Access Stratum (NAS) protocol logging facility [MME 4G]
• **netwstrg**: Network Storage facility
• **npuctrl**: Network Processor Unit Control facility
• **npudrv**: Network Processor Unit Driver facility [ASR 5500 only]
• **npumgr**: Network Processor Unit Manager facility
• **npumgr-act**: NPUMGR ACL logging facility
• **npumgr-drvo**: NPUMGR DRV logging facility
• **npumgr-flow**: NPUMGR FLOW logging facility
• **npumgr-fwd**: NPUMGR FWD logging facility
• **npumgr-init**: NPUMGR INIT logging facility
• **npumgr-lc**: NPUMGR LC logging facility
• **npumgr-port**: NPUMGR PORT logging facility
• **npumgr-recovery**: NPUMGR RECOVERY logging facility
• **npumgr-rrri**: NPUMGR RRI (Reverse Route Injection) logging facility
• **npumgr-vpn**: NPUMGR VPN logging facility
• **npusim**: NPUSIM logging facility [ASR 5500 only]
• **ntfy-intf**: Notification Interface logging facility [Release 12.0 and earlier versions only]
• **ocsp**: Online Certificate Status Protocol logging facility.
• **orbs**: Object Request Broker System logging facility
• **ospf**: OSPF protocol logging facility
• **ospfv3**: OSPFv3 protocol logging facility
• **p2p**: Peer-to-Peer Detection logging facility
• **pagingmgr**: PAGINGMGR logging facility
• **pcemgr**: Intelligent Policy Control Function (IPCF) Policy Charging and Control (PCC) Manager library
• **pdg**: Packet Data Gateway (PDG) logging facility
• **pdgdmgr**: PDG Demux Manager logging facility
• **pdif**: Packet Data Interworking Function (PDIF) logging facility
• **pgw**: Packet Data Network Gateway (PGW) logging facility
• **pmm-app**: Packet Mobility Management (PMM) application logging facility
• **ppp**: Point-To-Point Protocol (PPP) link and packet facilities
• **pppoe**: PPP over Ethernet logging facility
• **push**: VPNMGR CDR push logging facility
• **radius-acct**: RADIUS accounting logging facility
• **radius-auth**: RADIUS authentication logging facility
• **radius-coa**: RADIUS change of authorization and radius disconnect
• **ranap**: Radio Access Network Application Part (RANAP) Protocol facility logging info flow between SGSN and RNS (3G)
• **rct**: Recovery Control Task logging facility
• **rdt**: Redirect Task logging facility
• **resmgr**: Resource Manager logging facility
• **rf-diameter**: Diameter Rf interface messages facility
• **rip**: Routing Information Protocol (RIP) logging facility [RIP is not supported at this time.]
• **rlf**: Rate Limiting Function (RLF) logging facility
• **rohc**: Robust Header Compression (RoHC) facility
• **rsvp**: Reservation Protocol logging facility
• **rua**: RANAP User Adaptation (RUA) [3G Femto GW - RUA messages] logging facility
• **s1ap**: S1 Application Protocol (S1AP) Protocol logging facility
• **sabp**: Service Area Broadcast Protocol (SABP) logging facility
• **saegw**: System Architecture Evolution (SAE) Gateway facility
• **sccp**: Signalling Connection Control Part (SCCP) Protocol logging (connection-oriented messages between RANAP and TCAP layers).
• **sct**: Shared Configuration Task logging facility
• **sctp**: Stream Control Transmission Protocol (SCTP) Protocol logging facility
• **sef_ecs**: Severely Errored Frames (SEF) APIs printing facility
• **sess-gr**: SM GR facility
• **sessctrl**: Session Controller logging facility
• **sessmgr**: Session Manager logging facility
• **sesstrc**: session trace logging facility
• **sft**: Switch Fabric Task logging facility
• **sgs**: SGs interface protocol logging facility
• **sgsn-app**: SGSN-APP logging various SGSN “glue” interfaces (for example, between PMM, MAP, GPRS-FSM, SMS).
• **sgsn-failures**: SGSN call failures (attach/activate rejects) logging facility (2.5G)
• **sgsn-gtpc**: SGSN GTP-C Protocol logging control messages between the SGSN and the GGSN
• **sgsn-gtpu**: SGSN GTP-U Protocol logging user data messages between the SGSN and GGSN
• **sgsn-mbms-bearer**: SGSN Multimedia Broadcast/Multicast Service (MBMS) Bearer app (SMGR) logging facility
• **sgsn-misc**: Used by stack manager to log binding and removing between layers
• **sgsn-system**: SGSN System Components logging facility (used infrequently)
• **sgsn-test**: SGSN Tests logging facility; used infrequently
• **sgtpcmgr**: SGSN GTP-C Manager logging information exchange through SGTPC and the GGSN
• **sgw**: Serving Gateway facility
• **sh-diameter**: Sh Diameter messages facility
• **sitmain**: System Initialization Task main logging facility
• **sm-app**: SM Protocol logging facility
• **sms**: Short Message Service (SMS) logging messages between the MS and the SMSC
• **sndcp**: Sub Network Dependent Convergence Protocol (SNDCP) logging facility
• **snmp**: SNMP logging facility
• **sprmgr**: IPCF Subscriber Policy Register (SPR) manager logging facility
• **srdb**: Static Rating Database
• **srp**: Service Redundancy Protocol (SRP) logging facility
• **sscfnni**: Service-Specific Coordination Function for Signaling at the Network Node Interface (SSCF-NNI) logging facility
• **sscop**: Service-Specific Connection-Oriented Protocol (SSCOP) logging facility
• **ssh-ipsec**: Secure Shell (SSH) IP Security logging facility
• **ssl**: Secure Socket Layer (SSL) message logging facility
• **stat**: Statistics logging facility
• **supserv**: Supplementary Services logging facility [H.323]
• **system**: System logging facility
• **tacacplus**: TACACS+ Protocol logging facility
• **tcap**: TCAP Protocol logging facility
• **testctrl**: Test Controller logging facility
• **testmgr**: Test Manager logging facility
• **threshold**: threshold logging facility
• **ttg**: Tunnel Termination Gateway (TTG) logging facility
• **tucl**: TCP/UDP Convergence Layer (TUCL) logging facility
• **udr**: User Data Record (UDR) facility (used with the Charging Service)
• **user-data**: User data logging facility
• **user-l3tunnel**: User Layer 3 tunnel logging facility
• **userTCP-stack**: User TCP Stack
• **vim**: Voice Instant Messaging (VIM) logging facility
• **vinfo**: VINFO logging facility
• **vmgctrl**: Virtual Media Gateway (VMG) controller facility
• **vmgctrl**: VMG Content Manager facility
• **vpn**: Virtual Private Network logging facility
• **wimax-data**: WiMAX DATA
• **wimax-r6**: WiMAX R6
• **wsg**: Wireless Security Gateway (ASR 9000 Security Gateway)

**level severity_level**

Specifies the level of information to be logged from the following list which is ordered from highest to lowest:
• **critical**: Logs critical events
save logs

- **error**: Logs error events and all events with a higher severity level
- **warning**: Logs warning events and all events with a higher severity level
- **unusual**: Logs unusual events and all events with a higher severity level
- **info**: Logs info events and all events with a higher severity level
- **trace**: Logs trace events and all events with a higher severity level
- **debug**: Logs all events

**pdu-data pdu_format**
Specifies output format for the display of packet data units as one of:
- **none**: raw format (unformatted).
- **hex**: hexadecimal format.
- **hex-ascii**: hexadecimal and ASCII similar to a main-frame dump.

**pdu-verbosity pdu_verboseness**
Specifies the level of verboseness to use in displaying of packet data units as a value from 1 to 5, where 5 is the most detailed.

**since from_date_time [ until to_date_time ]**
Default: no limit.
- **since from_date_time**: Saves only the log information which has been collected more recently than from_date_time.
- **until to_date_time**: Saves no log information more recent than to_date_time. Defaults to current time when omitted.
- **from_date_time** and **to_date_time** must be formatted as YYYY:MM:DD:HH:mm or YYYY:MM:DD:HH:mm:ss. Where:
  - **YYYY** = 4-digit year
  - **MM** = 2-digit month in the range 01 through 12
  - **DD** = 2-digit day in the range 01 through 31
  - **HH** = 2-digit hour in the range 00 through 23
  - **mm** = 2-digit minute in the range 00 through 59
  - **ss** = 2 digit second in the range 00 through 59
- **to_date_time** must be a time which is more recent than from_date_time.
Using the **until** keyword allows for a time range of log information; using only the **since** keyword will display all information up to the current time.

**grep grep_options | more**
Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in Command Line Interface Reference.

**Usage**
Backup the current log file as part of periodic maintenance activities.
Example

The following saves the log to the local file `/flash/pub/junelogs.logs` with no confirmation from the user:

```
save logs /flash/pub/junelogs.logs -noconfirm
```

The following saves the configuration data to remote host `remoteABC` as `/pub/junelogs.logs`:

```
save logs tftp://remoteABC/pub/junelogs.logs
```
session trace

Enable or disables the subscriber session trace functionality based on a specified subscriber device or ID on one or all instance of session on a specified UMTS/EPS network element. It also clears/resets the statistics collected for subscriber session trace on a system.

Product
GGSN
MME
P-GW
SAEGW
S-GW

Privilege
Operator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

session trace { reset statistics | subscriber network-element { mme | pgw | sgw | ggsn saegw [func-pgw | func-sgw] { imei id | imsi id | interface { all | interface } } trace-ref id collection-entity ip_address

no session trace subscriber network-element [ mme | pgw | sgw | ggsn ] [ trace-ref id ]

Caution: This is a system wide command that affects all statistical data.

Identifies the network element that, in turn, identifies the interfaces where the session trace is to occur. Specific interfaces can be specified using the interface keyword described below.

ggsn: Specifies that the session trace is to occur on one or all interfaces on the GGSN.
mme: Specifies that the session trace is to occur on one or all interfaces on the MME.
pgw: Specifies that the session trace is to occur on one or all interfaces on the P-GW.
sgw: Specifies that the session trace is to occur on one or all interfaces on the S-GW.
**imei id**

Specifies the International Mobile Equipment Identification number of the subscriber UE. *id* must be the 8-digit TAC (Type Allocation Code) and 6-digit serial number. Only the first 14 digits of the IMEI/IMEISV are used to find the equipment ID.

**imsi id**

Specifies the International Mobile Subscriber Identification (IMSI). *id* must be the 3-digit MCC (Mobile Country Code), 2- or 3-digit MNC (Mobile Network Code), and the MSIN (Mobile Subscriber Identification Number). The total should not exceed 15 digits.

**interface { all | interface }**

Specifies the interfaces where the session trace application will collect data.

- **all**: Specifies all interfaces associated with the selected network element
- **interface**: Specifies the interface type where the session trace application will collect trace data. The following interfaces are applicable for each network element type:
  - **GGSN**:
    - **gi**: Specifies that the interface where the trace will be performed is the Gi interface between the GGSN and RADIUS server.
    - **gmb**: Specifies that the interface where the trace will be performed is the Gmb interface between the GGSN and BM-SC.
    - **gn**: Specifies that the interface where the trace will be performed is the Gn interface between the GGSN and the SGSN.
    - **gx**: Specifies that the interface where the trace will be performed is the Gx interface between the GGSN and PCRF.
  - **MME**:
    - **s1mme**: Specifies that the interface where the trace will be performed is the S1-MME interface between the MME and the eNodeB.
    - **s3**: Specifies that the interface where the trace will be performed is the S3 interface between the MME and an SGSN.
    - **s6a**: Specifies that the interface where the trace will be performed is the S6a interface between the MME and the HSS.
    - **s10**: Specifies that the interface where the trace will be performed is the S10 interface between the MME and another MME.
    - **s11**: Specifies that the interface where the trace will be performed is the S11 interface between the MME and the S-GW.
  - **P-GW**:
    - **gx**: Specifies that the interface where the trace will be performed is the Gx interface between the P-GW and the PCRF.
    - **s2a**: Specifies that the interface where the trace will be performed is the S2a interface between the P-GW and the HSGW.
    - **s2b**: Specifies that the interface where the trace will be performed is the S2b interface between the P-GW and an ePDG.
    - **s2c**: Specifies that the interface where the trace will be performed is the S2c interface between the P-GW and a trusted, non-3GPP access device.
• **s5**: Specifies that the interface where the trace will be performed is the S5 interface between the P-GW and the S-GW.

• **s6b**: Specifies that the interface where the trace will be performed is the S6b interface between the P-GW and the 3GPP AAA server.

• **s8b**: Specifies that the interface where the trace will be performed is the S8b interface between the P-GW and the S-GW.

• **sgi**: Specifies that the interface where the trace will be performed is the SGi interface between the P-GW and the PDN.

**S-GW:**

• **gxc**: Specifies that the interface where the trace will be performed is the Gxc interface between the S-GW and the PCRF.

• **s11**: Specifies that the interface where the trace will be performed is the S11 interface between the S-GW and the MME.

• **s4**: Specifies that the interface where the trace will be performed is the S4 interface between the S-GW and an SGSN.

• **s5**: Specifies that the interface where the trace will be performed is the S5 interface between the S-GW and the P-GW.

• **s8b**: Specifies that the interface where the trace will be performed is the S8b interface between the S-GW and the P-GW.

```
trace-ref id
```

Specifies the trace reference for the trace being initiated. *id* must be the MCC (3 digits), followed by the MNC (3 digits), then the trace ID number (3-byte octet string).

```
collection-entity ip_address
```

Specifies the IP address of the collection entity where session trace data is pushed in IPv4 dotted-decimal notation.

**Usage**

Use this command to initiate a session trace for a specified subscriber device or ID on one or all interfaces on a specified network element.

**Important:** Session trace configuration is performed in the *Global Configuration Mode* using the `session trace` command. Refer to the *Global Configuration Mode Commands* chapter for more information.

**Example**

The following command initiates a session trace on a P-GW S5 interface for a subscriber with an IMSI of 322233123456789 and sets the trace reference as 322233987654 and the collection entity IP address as 10.2.3.4:

```none
session trace subscriber network-element pgw imsi 322233123456789
interface s5 trace-ref 322233987654 collection-entity 10.2.3.4
```

The following command initiates a session trace on an MME S6a interface for a subscriber with an IMSI of 322233123456789 and sets the trace reference as 322233987654 and the collection entity IP address as 10.2.3.4:

```none
session trace subscriber network-element mme imsi 322233123456789
interface s6a trace-ref 322233987654 collection-entity 10.2.3.4
```
The following command initiates a session trace on a Gn interface on GGSN between GGSN and SGSN for a subscriber with an IMSI of 322233123456789 and sets the trace reference as 322233987654 and the collection entity IP address as 10.2.3.4:

```
session trace subscriber network-element mme imsi 322233123456789
interface s6a trace-ref 322233987654 collection-entity 10.2.3.4
```

The following command initiates a session trace on a Gn interface on GGSN between GGSN and SGSN for a subscriber with an IMSI of 322233123456789 and sets the trace reference as 322233987654 and the collection entity IP address as 10.2.3.4:

```
session trace subscriber network-element ggsn imsi 322233123456789
interface gn trace-ref 322233987654 collection-entity 10.2.3.4
```
session trace signaling

Enable or disables the subscriber session trace functionality based on signaling information on one or all instance of session on a specified UMTS/EPS network element. It also clears/resets the statistics collected for subscriber session trace on a system.

Product
GGSN
P-GW

Privilege
Operator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local] host_name#

Syntax

[no] session trace signaling network-element {ggsn | pgw}

no
Disables the entire session trace based on signaling information for a specific network element and/or trace reference.

session trace signaling network-element {pgw | ggsn}
Identifies the network element that where the session trace based on signaling information for a subscriber session is to occur. Specific network element GPRS/EPS can be specified for this session trace.

ggsn: Specifies that the session trace based on signaling is to occur on one or all interfaces on the GGSN.
pgw: Specifies that the session trace based on signaling is to occur on one or all interfaces on the P-GW.

Usage
Use this command to initiate a session trace for a specified subscriber based on signaling information on a specified network element.

Important: Session trace configuration is performed in the Global Configuration Mode using the session trace command. Refer to the Global Configuration Mode Commands chapter for more information.

Example
The following command initiates a session trace on a GGSN for a subscriber based on signaling information.

    session trace signaling network-element ggsn
**session trace random**

Enable or disables the subscriber session trace functionality based on a the random trace on the network element. If enabled, the subscriber selection will be based on random logic all instance of session on a specified UMTS/EPS network element. It also clears/resets the statistics collected for subscriber session trace on a system.

**Product**
- GGSN
- P-GW

**Privilege**
- Operator

**Mode**
- Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
[no] session trace random random_num network-element {ggsn | pgw} [interface {all | interface}]
```

- **[no]** Disables the entire random subscriber session trace or for a specific network element and/or interface.

- **session trace random random_num}**
  Configures the number of random subscriber sessions where the session trace is to occur. `random_num` is an integer between 1 to 1000 identified the number of subscribers to be selected by random logic.

- **network-element {ggsn | pgw}**
  Identifies the network element that, in turn, identifies the interfaces where the random session trace is to occur. Specific interfaces can be specified using the interface keyword described below.
  - **ggsn**: Specifies that the random session trace is to occur on one or all interfaces on the GGSN.
  - **pgw**: Specifies that the random session trace is to occur on one or all interfaces on the P-GW.

- **interface { all | interface }**
  Specifies the interfaces where the random session trace application will collect data.
  - **all**: Specifies all interfaces associated with the selected network element
  - **interface**: Specifies the interface type where the random session trace application will collect trace data.

  The following interfaces are applicable for the network element type:
  - **GGSN**:
    - **gi**: Specifies that the interface where the trace will be performed is the Gi interface between the GGSN and RADIUS server.
    - **gmb**: Specifies that the interface where the trace will be performed is the Gmb interface between the GGSN and BM-SC.
**gn**: Specifies that the interface where the trace will be performed is the Gn interface between the GGSN and the SGSN.

**gx**: Specifies that the interface where the trace will be performed is the Gx interface between the GGSN and PCRF.

**P-GW**:

- **gx**: Specifies that the interface where the trace will be performed is the Gx interface between the P-GW and the PCRF.
- **s2a**: Specifies that the interface where the trace will be performed is the S2a interface between the P-GW and the HSGW.
- **s2b**: Specifies that the interface where the trace will be performed is the S2b interface between the P-GW and an ePDG.
- **s2c**: Specifies that the interface where the trace will be performed is the S2c interface between the P-GW and a trusted, non-3GPP access device.
- **s5**: Specifies that the interface where the trace will be performed is the S5 interface between the P-GW and the S-GW.
- **s6b**: Specifies that the interface where the trace will be performed is the S6b interface between the P-GW and the 3GPP AAA server.
- **s8b**: Specifies that the interface where the trace will be performed is the S8b interface between the P-GW and the S-GW.
- **sgi**: Specifies that the interface where the trace will be performed is the SGi interface between the P-GW and the PDN.

### Usage

Use this command to initiate the session trace for a specified subscriber sessions selected on random logic on one or all interfaces on a specified network element.

**Important**: Session trace configuration is performed in the Global Configuration Mode using the `session trace` command. Refer to the Global Configuration Mode Commands chapter for more information.

### Example

The following command initiates a session trace on a GGSN Gx interface for 1000 subscriber session selected on random logic:

```
session trace random 1000 network-element ggsn interface gx
```
**setup**

Enters the system setup wizard which guides the user through a series of questions regarding the system basic configuration options, such as initial context-level administrative users, host name, etc.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
setup
```

**Usage**

The setup wizard provides a user friendly interface for initial system configuration.

**Important:** If the configuration script generated by the setup wizard is applied when an existing configuration is in use, the options which are common to both are updated and all remaining options are left unchanged.

**Example**

```
setup
```
sgs offload

Enables or disables offloading of UEs associated with a VLR which has become unavailable. This enables the MME to preemptively move subscribers away from a VLR which is scheduled to be put in maintenance mode.

**Product**
MME

**Privilege**
Security Administrator, Administrator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local] host_name#
```

**Syntax**

```
sgs offload sgs-service sgs_svc_name vlr vlr_name { start time-duration minutes | stop } [ -noconfirm ]
```

**sgs-service sgs_svc_name**

Specifies the SGs service to which the VLR belongs. 

*sgs_svc_name* specifies the name of a pre-configured SGs service. For more information on the SGs service, refer to the *sgs-service* command in the Context Configuration Mode Commands chapter and refer to the MME SGs Service Configuration Mode Commands chapter.

**vlr vlr_name**

Specifies the VLR service which must have its UEs offloaded. 

*vlr_name* specifies the name for a pre-configured VLR and must be an alphanumeric string of 1 through 63 characters. For more information, refer to the *vlr* command in the MME SGs Service Configuration Mode Commands chapter.

**start time-duration minutes**

Specifies that the UE offloading should be started for the specified the VLR. 

*time-duration* defines the period in minutes over which all qualifying subscribers will be offloaded. 

*minutes* must be an integer from 0 to 3000.

A value of 0 enables only Passive VLR Offloading, where the MME marks all affected sessions with the “VLR Offload” flag. During the next UE activity, the MME requires each UE to perform a combined TAU/LAU. This flag is not affected by the removal of the “offload” state by the operator. Even though the VLR state may later change from “offloaded” to “not-offloaded”, the subscriber’s state will not change to “not-offloaded”.

A value of 1-3000 enables Active VLR Offloading and Passive VLR Offloading. The MME splits this time-duration into n intervals, 5 seconds apart. A maximum of 50 subscribers will be actively detached per interval. For example, a setting of 120 minutes with 60000 subscribers would process all subscribers in 100 minutes. Any subscribers remaining at the expiry of the time-duration will not be detached.

**Note:** For Release 12.2, only Passive VLR Offloading is supported. While the *time-duration* value is not used in Release 12.2 or earlier, it is required for completion of the *start* command.
Exec Mode Commands (D-S)

sgs offload

stop
Specifies that the offload state should no longer be set for the specified VLR.

-noconfirm
Indicates that the command is to execute without additional prompt and confirmation from the user.

Usage
This command enables the MME to preemptively move subscribers away from a VLR which is scheduled to be put in maintenance mode. When this offload command is set on the MME, all sessions matching this VLR are marked with an “offload” flag. If the time-duration keyword is set to 1-3000, sessions are also detached and required to reattach.
The behavior of SGs with respect to “Location Updates” towards the MSC is similar to the behavior when the “VLR Reliable” flag is set to “false”. In other words, for offloaded subscribers, normal Combined TAs (without IMSI Attach) and periodic TAs will trigger a LU towards the MSC.
When issuing the command, the MME notifies the operator if this is the last available VLR in a pool.
More than one VLR may be offloaded at the same time.
VLR Offloading and MME offloading cannot be performed at the same time.

Important: This is a licensed feature and is unavailable unless the proper license is installed.

Related Commands:
- To display VLR offload information and statistics for a specified SGs service name, refer to the show sgs-service offload-status service-name sgs_svc_name command.
- To clear the counters displayed by the previous command, issue the clear sgs-service statistics service-name sgs_svc_name command.

Example
The following command starts offloading the subscribers associated with vlr1 over the next 60 minutes.

sgs offload sgs-service sgs1 vlr vlr1 start time-duration 60 -noconfirm
s gs vlr-failure

This command configures the MME to monitor all VLRs and perform a controlled release (detach) of affected UEs when any VLR becomes unavailable.

Product
MME

Privilege
Security Administrator, Administrator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

[no] sgs vlr-failure sgs-service sgs_svc_name duration minutes backoff-timer seconds [ -noconfirm ]

---

no

Resets the command to its default setting of disabled.

sgs-service sgs_svc_name

Specifies the SGs service to which the VLR belongs.

sgs_svc_name specifies the name of a pre-configured SGs service.

duration minutes

Specifies the amount of time in minutes during which all qualifying UEs will be detached.

The MME splits this duration into \( n \) intervals, 5 seconds apart. A maximum of 50 subscribers are processed per interval. For example, a setting of 2 minutes with 100 subscribers would result in the MME processing all subscribers in the first 2 intervals (10 seconds). Any subscribers remaining at the expiry of the duration will not be processed.

minutes must be an integer from 1 through 3000.

backoff-timer seconds

Specifies the period of time the MME will wait following the detection of a VLR condition before starting the controlled release of affected UEs.

seconds must be an integer from 1 to 3000.

-noconfirm

Indicates that the command is to execute without additional prompt and confirmation from the user.
Usage

When this command is issued, the MME monitors the availability of all VLRs. If one or more VLRs become unavailable, the MME performs a controlled release (EPS IMSI detach) for all UEs associated with that VLR. If another VLR is available, the MME sends a combined TA/LA Update with IMSI attach. This command remains active until it is disabled with the `no sgs vlr-failure` command.

Important: This is a licensed feature and is unavailable unless the proper licensed is installed.

Related Commands:

- To display VLR failure information and statistics, refer to the `show sgs-service vlr-status full` command.

Example

The following enables the monitoring and automatic detach of UEs when any VLR becomes unavailable. The MME will wait 2 minutes (120 seconds) after detecting a VLR condition before starting the controlled release of the affected UEs. The MME will process the UEs over a span of 60 minutes.

```
sgs vlr-failure sgs-service sg1 duration 60 backoff-timer 120 -noconfirm
```
**sgs vlr-recover**

This command enables active recovery of Circuit Switched Fall Back (SMS-only) UEs when a failed VLR becomes responsive again.

**Product**
MME

**Privilege**
Security Administrator, Administrator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local] host_name#
```

**Syntax**

```
[no] sgs vlr-recover sgs-service sgs_svc_name duration minutes backoff-timer seconds [ -noconfirm ]
```

- **no**
  Resets the command to its default setting of disabled.

- **sgs-service sgs_svc_name**
  Specifies the SGs service to which the VLR belongs.
  `sgs_svc_name` specifies the name for a pre-configured SGs service.

- **duration minutes**
  Specifies the amount of time in minutes over which all qualifying UEs will be recovered.
  The MME splits this duration into $n$ intervals, 5 seconds apart. A maximum of 50 subscribers will be processed per interval. For example, a setting of 2 minutes with 100 subscribers would result in the MME processing all subscribers in the first 2 intervals (10) seconds. Any subscribers remaining at the expiry of the duration will not be processed.
  `duration` must be an integer from 1 through 3000.

- **backoff-timer seconds**
  Specifies the period of time the MME will wait following the detection of a recovered VLR before starting the VLR recovery actions.
  `seconds` must be an integer from 1 to 3000.

- **-noconfirm**
  Indicates that the command is to execute without additional prompt and confirmation from the user.
Usage

When this command is issued, the MME monitors the availability of all VLRs. If a failed VLRs become available again, the MME attempts to recover CSFB (SMS-only) UEs that failed while the VLR was unavailable with an EPS Detach.

Important: This is a licensed feature and is unavailable unless the proper license is installed.

Related Commands:

- To display VLR recovery information and statistics, refer to the `show sgs-service vlr-status full` command.

Example

The following enables the active recovery of Circuit Switched Fall Back (SMS-only) UEs when a failed VLR becomes responsive again. The MME will wait 2 minutes (120 seconds) after detecting a recovered VLR before starting the recovery of the affected UEs. The MME will process the UEs over a span of 60 minutes.

```
sgs vlr-recover sgs-service sgsl duration 60 backoff-timer 120 -noconfirm
```
**sgsn clear-detached-subscriptions**

Clears subscription data belonging to a subscriber who has already detached.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
sgsn clear-detached-subscriptions imsi imsi
```

**Usage**

This command can be issued on either a 2G or 3G SGSN to clear subscription data (including subscription information, and information for P-TMSI allocated, received authorization vectors, and NGAF flag values). This command is only effective if the subscriber has already detached.

After the data is purged, the SGSN sends an appropriate message to the HLR.

**Related Commands:**
- To clear subscription data for subscribers that are currently attached, refer to the `admin-disconnect-behavior clear-subscription` commands described in the chapters for **GPRS Service Configuration Mode** or the **SGSN Service Configuration Mode**.

**Example**

```
sgsn clear-detached-subscriptions imsi 040501414199978
```
sgsn imsimgr

Initiates an audit for managing the SGSN’s IMSI manager’s (IMSIMgr) IMSI table.

**Important:** These commands are used primarily for troubleshooting purposes and are intended for the use of specially trained service representatives.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
sgsn imsimgr { add-record imsi sessmgr instance sessmgr# | audit-with sessmgr { all | instance sessmgr# } | remove-record imsi }
```

**add-record imsi**

Adds a record for an IMSI to the IMSI manager’s table and associates a specific session manager (SessMgr) with the IMSI.

*imsi:* Enter up to 15 digits. An IMSI consists of the 3-digit MCC (mobile country code) + the 2- or 3-digit MNC (mobile network code) + the MSIN (mobile station identification number) for the remaining 10 or 9 digits (depending on the length of the MNC).

**audit-with**

Initiates an IMSI audit with all SessMgrs or a Session Manager (SessMgr) instance specified.

**remove-record imsi**

Deletes a specific IMSI from the IMSI table.

*imsi:* Enter up to 15 digits. An IMSI consists of the 3-digit MCC (mobile country code) + the 2- or 3-digit MNC (mobile network code) + the MSIN (mobile station identification number) for the remaining 10 or 9 digits (depending on the length of the MNC).

**sessmgr instance sessmgr#**

For releases prior to 14.0, this keyword specifies a Session Manager (SessMgr) instance associated with the IMSI as an integer from 0 through 4095.

For releases 14.0 and later, this keyword specifies a Session Manager (SessMgr) instance associated with the IMSI as an integer from 0 through 384.
Usage
Use this command to manage the IMSIMgr’s IMSI table, and to initiate an audit of one or more SessMgrs with the IMSIMgr so that the IMSI table has the correct IMSI-SessMgr association. After this audit, any IMSI in the IMSIMGR which is not found in any Sessmgr is deleted and similarly any missing entries at the IMSIMgr are created.

Example
Delete IMSI 044133255524211 from the audit table:

        sgsn imsimgr remove-record 044133255524211
**sgsn offload**

Instructs the SGSN to begin the offloading procedure and actually starts and stops the offloading of subscribers which is part of the SGSN Gb (2G) or Iu (3G) Flex load redistribution functionality.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
```

---

**gprs-service svc_name**

Specifies a unique alphanumeric string of 1 through 63 characters that identifies a GPRS service that has already been defined for the 2G SGSN configuration.

---

**sgsn-service svc_name**

Specifies a unique alphanumeric string of 1 through 63 characters that identifies an SGSN service that has already been defined for the 3G SGSN configuration.

---

**activating**

Instructs the SGSN to off load any subscribers sending an “activate request” message.

---

**connecting**

Instructs the SGSN to off load any subscribers sending either an Attach Request or a RAU Request message. Including this keyword without adding the target-nri and target-count keywords activates local offloading.

---

**imsi imsi**

Identifies a subscriber by the international mobile subscriber ID (IMSI) which consists of the 3-digit MCC (mobile country code) + the 2- or 3-digit MNC (mobile network code) + the MSIN (mobile station identification number) for the remaining 10 or 9 digits (depending on the length of the MNC).

*imsi*- enter an integer comprising up to 15 digits.
**sgsn offload**

Sets the local NRI. Including this keyword in the configuration instructs the SGSN to check the P-TMSI and use the SGSN matching the configured NRI value to off load subscribers.

---

**Important:** `nri-value` and `target-nri` are mutually exclusive.

`nri-value` is an integer from 1 through 63 that identifies a specific, already defined, SGSN in a pool. (NRI defined in the service configuration.) Use of 0 (zero) value is not recommended.

**stop**

Instructs the SGSN to stop offloading subscribers from the pool area.

**target-nri target_nri**

Instructs the SGSN to begin dynamically load balancing across a network of pooled SGSNs. `target_nri` is an integer from 0 through 63 that identifies an already defined target NRI (SGSN) to which the subscribers are to be offloaded. (NRI previously defined in the service configuration.) Use of 0 (zero) value is not recommended.

**target-count target_count**

Identifies the number of subscribers to be offloaded as an integer from 0 through 4000000. Instructs the SGSN to begin target count-based offloading.

**t3312-timeout seconds**

Sets the timer (in seconds) for sending period RAUs to the MS as an integer from 2 through 60. Default: 4

---

**Usage**

Use this command to configure the offloading of subscribers which is a part of the SGSN’s load redistribution operation. This command can be used anytime an SGSN is to be taken out of service. Commands, with different NRI values, are repeated to expand/contract the radius of the offloading. Target count-based offloading and local offloading can not run simultaneously. When target count offloading is to be used, you should choose an algorithm to control offloading from the perspective of the IMSIMGR and SESSMGR. This is done with the `target-offloading` command in the SGSN-Global configuration mode.

---

**Example**

The following is a series of two commands to initiate **local offloading**.

Command 1: The following command instructs the SGSN to begin local offloading for the local NRI id 1 included in the `gprs1` GPRS service configuration:

```
sgsn offload gprs-service gprs1 connecting nri-value 1
```

Command 2: Enter this second command to add offloading for NRI 2 to the offloading already occurring for NRI 1:

```
sgsn offload gprs-service gprs1 connecting nri-value 2
```

The following is a series of commands to discontinue local offloading and to initiate **target count-based offloading**.
Command 1: The following command instructs the SGSN to discontinue local offloading for NRIs 5 included in the sgsnserv4 SGSN service configuration:

```
sgsn offload sgsn-service sgsnserv4 connecting stop nri 5
```

**Important:** The next command is an example of provision configuration for multiple NRI with a single command.

Command 2: The following command instructs the SGSN to initiate target count-based offloading for target NRI 5 to a target count of 10000 and target NRI 6 to count of 300000:

```
sgsn offload sgsn-service sgsnserv4 connecting target-nri 5 target-count 100000 target-nri 6 target-count 300000
```
sgsn op

Instructs the SGSN to begin specific operations or functions.

Product

SGSN

Privilege

Security Administrator, Administrator

Mode

Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

sgsn op { auth-ptmsi-counters imsi imsi | convert | nse { fr | ip | sgsn-involve-trace } | show | ss7-rd ss7-rd-id { destination | link | linkset | peer } }

auth-ptmsi-counters imsi imsi

Displays the authentication, P-TMSI reallocation, and P-TMSI signature reallocation counters for the specified IMSI.

imsi: Enter a unique 15-digit number associated with a mobile phone.

convert point-code pt_code variant variant

Converts SS7 point codes, according to identified variants, from dotted-decimal format to decimal format and vice versa.

point-code pt_code: Enters an SS7 point code in either dotted-decimal format or decimal format.

variant variant: Identifies the appropriate variant for the point code:

- ansi
- itu
- ttc

nse { fr operation | ip operation | sgsn-involve-trace nse-id nse-id }

Enables the operator to perform a range of live control functions (for example, reset, block, unblock) for various types of virtual connections based on the signalling type of the NSE:

fr: Identifies a Frame Relay NSE.

ip: Identifies an IP NSE.

operation: Identifies the operation to be performed for the NSE connection (if available for the selected signalling type):

- block nse-id nse-id: Blocks signal flow through all network service virtual connections (NSVC) for the specified NSE:
  
  - nse_id: an integer from 0 to 65535.

- bvc-flc-limit rate rate bvc-id bvc_id nse-id nse_id: SGSN initiates flow control at the defined percentage rate to limit the flow through the BSSGP virtual connection (BVC) for the specified NSE and optionally for a specified BVC.
• **rate**: an integer from 0 to 100.
• **bvc_id**: an integer from 0 to 65000.
• **nse_id**: an integer from 0 to 65535.

**bvc-reset bvc-id bvc_id nse-id nse_id**: SGSN initiates a BVC-Reset on the specified BVC and NSE:

• **bvc_id**: an integer from 0 through 65000.
• **nse_id**: an integer from 0 through 65535.

**nsvc nsvc_id { block | enable | disable | unblock } nse_id**: SGSN initiates NS-Block or NS-Unblock for the specified NSVC of the specified NSE:

• **nsvc_id**: an integer from 0 through 65535.
• **nse_id**: an integer from 0 through 65535.

**reset nse-id nse_id**: SGSN initiates NS-Reset for all NSVC configured in the NSE. **nse_id** is an integer from 0 through 65535.

**unblock nse-id nse_id**: SGSN initiates NS-Unblock for all NSVC configured for the specified NSE. **nse_id** is an integer from 0 through 65535.

**sgsn-invoke-trace nse-id nse_id record-type record_type trace-reference reference [ mobile-id type id_type | trace-transaction-id trace_id ]**:  

**Important**: This command can be used for troubleshooting/debugging purposes and is primarily intended for the use of specially trained service representatives.

Instructions the SGSN (1) to send the BSSGP message SGSN-INVOKE-TRACE to the BSC to initiate a BSC trace of a particular MS and (2) to define the type and triggering of the trace.

• **nse_id**: Identifies the peer NSE, enter an integer from 0 to 65535.

• **record_type**: Specifies the type of trace to be performed:
  • basic
  • handover
  • no-bss-trace
  • radio

• **trace-reference reference**: Specifies the trace reference ID as an integer from 0 to 65535.

• **mobile-id type id_type**: Select the appropriate mobile ID type for the MS that is to be traced:
  • **imei value value**: Specifies the mobile ID type as the unique International Mobile Equipment Identity.
    value: 15-digit IMEI value.
  • **imeisv value value**: Specifies the mobile ID type as the unique International Mobile Equipment Identity with the two-digit software version number.
    value: 16-digit IMEISV value.
  • **imsi value value**: Specifies the mobile ID type as a network unique International Mobile Subscriber Identity as a 15-digit IMSI value.
  • **trace-transaction-id trace_id**: Specifies the trace transaction ID as an integer from 0 through 65535.
**show plmn-list smgr-inst sessmgr#**

**Important:** This function is only available in release 8.1.

SGSN displays the configured PLMN list for the specified session manager (SessMgr):  
`sessmgr#`: Enter up to 4 digits, 0 to 4095.

**ss7-rd ss7-rd_id** { destination | link | linkset | peer }

The `ss7-rd` commands assist with troubleshooting connections between the SGSN and the peer server.

`ss7-rd_id`: Specifies the configured SS7 routing domain as an integer from 1 through 12.

- **destination audit asp-instance asp_id peer-server-id peer_id psp-instance-id psp_id**
  
  Initiates destination audit (DAUD) messages for all point codes reachable via the identified peer-server, which is in restricted/unavailable/congested state due to DRST/DUNA/SCON messages respectively from the far end.
  
  - **asp_id**: Specifies the relevant ASP configuration ID as an integer from 1 through 4.
  - **peer_id**: Specifies the relevant peer server configuration ID as an integer from 1 through 144.
  - **psp_id**: Specifies the relevant PSP configuration ID as an integer from 1 through 4.

- **link procedure linkset-id linkset_id link-id link_id**
  
  Initiates MTP3 network link management procedures for the specified link:
  
  - **activate**: Activates the deactivated link.
  - **deactivate**: Deactivates specified link.
  - **deactivate-12-only**: Deactivates the link only at the MTP3 layer.
  - **inhibit**: Inhibits the link only if it does not make any destination unreachable.
  - **uninhibit**: Uninhibits the inhibited link.
  - **linkset_id**: an integer between 1 and 144.
  - **link_id**: an integer between 1 and 16.

- **linkset-id procedure linkset-id linkset_id**
  
  Initiates MTP3 network link management procedures for all the links in the specified linkset:
  
  - **activate**: Activates the deactivated linkset.
  - **deactivate**: Deactivates the linkset.
  - **deactivate-12-only**: Deactivates the linkset only at MTP3 layer.
  - **linkset_id**: an integer between 1 and 144.

- **peer message asp-instance asp_id peer-server-id peer_id psp-instance-id psp_id**
  
  Initiates one of the following SCTP/M3UA management messages from the identified link:
  
  - **abort**: Sends an SCTP Abort message which aborts the SCTP association ungracefully.
  - **activate**: Sends an M3UA ASP Active message to activate the link.
  - **down**: Sends an M3UA ASP Down message to bring down the M3UA link.
  - **establish**: Sends an SCTP INIT message to start the SCTP association establishment.
• **inactivate**: Sends an M3UA ASP Inactive message to deactivate the link.
• **inhibit**: Inhibits the M3UA link locally when the operator wants to lockout the link.
• **terminate**: Sends SCTP Shutdown message which closes the SCTP association gracefully.
• **un-inhibit**: Uninhibits the M3UA link.
• **up**: Sends an M3UA ASP UP message to bring up the M3UA link.

• **asp_id**: Specifies a relevant ASP configuration ID as an integer from 1 through 4.
• **peer_id**: Specifies the relevant peer server configuration ID as an integer from 1 through 144.
• **psp_id**: Specifies the relevant PSP configuration ID as an integer from 1 through 4

---

**Usage**

In most cases, an operator will block/unblock/reset from the BSC-side. The `nse` commands cause the SGSN to initiate actions, usually for one of the following reasons:

• to resolve issues on the BSC-side,
• as part of an upgrade to the BSC,
• as part of link expansion,
• to resolve NSVC/BVC status mismatches observed between the SGSN and BSC.

The `sgsn-invoke-trace` command initiates the trace procedure where the BSC begins a trace record on a specified MS.

**Example**

The following command instructs the SGSN to initiate an NS-Block for all NSVC associated with Frame Relay NSE ID 2422:

```
sgsn op nse fr unblock nse-id 2422
```

Activate linkset 1 configured in SS7 routing domain 1:

```
sgsn op ss7-rd 1 linkset activate linkset-id 1
```
sgsn retry-unavailable-ggsn

Marks the GGSN as available for further activation.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
sgsn retry-unavailable-ggsn ip_address
```

*ip_address*

Specifies the IP address of a GGSN in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

**Usage**

This command allows the operator to directly inform both the session manager and the SGTPC manager that the GGSN has been removed from a blacklist and is now available for activations. This action would override the GGSN blacklist timer configuration with **ggsn-fail-retry-timer** in the SGTP service configuration mode.

**Example**

The following command indicates that the GGSN identified by its IP address is now available for activation:

```
sgsn retry-unavailable-ggsn 198.168.128.8
```
sgtpc test echo sgsn-address

Initiates SGTPC echo test procedure.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

```
sgtpc test echo sgsn-address sgsn_ip_address { all | ggsn-address ggsn_ip_address }
```

<table>
<thead>
<tr>
<th>sgsn-address</th>
<th>sgsn_ip_address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identifies the IP address of the SGSN issuing the test in IPv4 dotted-decimal notation.</td>
<td></td>
</tr>
</tbody>
</table>

| all |
| Sends GTPC echo requests to all GGSNs having current sessions with the SGTP service. |

<table>
<thead>
<tr>
<th>ggsn-address</th>
<th>ggsn_ip_address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sends a GTPC echo request to the specified GGSN whether or not the GGSN has active sessions with the SGTP service. ggsn_ip_address is entered using IPv4 dotted-decimal notation.</td>
<td></td>
</tr>
</tbody>
</table>

Usage

This command initiates a test for the GTPC echo procedure -- echo from the specified SGSN to a specified GGSN or to all GGSNs that have sessions with the SGTP service. Issue the command from the Exec Mode within the context in which the SGTP service is configured. Note that if the GGSN does not respond to the initial echo request, the echo requests will be retried for the max-retransmissions times.

Example

This SGSN with IP address of 10.1.1.1 sends an echo test to all GGSNs attached to the SGTP service:

```
sgtpc test echo sgsn-address 10.1.1.1 all
```
shutdown

Terminates all processes within the chassis. After all processes are terminated, the system initiates a hardware reset (reboot). This command is identical to the `reload` command.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Mode**

Exec

The following prompt is displayed in the Exec mode:

```
[local] host_name#
```

**Syntax**

```
shutdown [ -noconfirm ]
```

- `-noconfirm`
  
  Executes the command without any additional prompts or confirmation from the user.

**Usage**

The system performs a hardware reset and reloads the highest priority boot image and configuration file specified in the boot.sys file. Refer to the `boot system priority` command in the Global Configuration Mode for additional information on configuring boot images, configuration files and priorities.

**Important:** To avoid the abrupt termination of subscriber sessions, it is recommended that a new call policy be configured and executed prior to invoking the `shutdown` command. This policy sets busy-out conditions for the system and allows active sessions to terminate gracefully. Refer to the `newcall` command in the Exec Mode for additional information.

**Caution:** Issuing this command causes the system to become unavailable for session processing until the reboot process is complete.

**Example**

The following command performs a hardware reset on the system:

```
shutdown
```
sleep

Pauses the command line interface (CLI).

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

```
sleep seconds
```

Specifications the number of seconds to pause as an integer from 1 through 3600.

Usage
Sleep is a command delay which is only useful when creating command line interface scripts such as predefined configuration files/scripts.

Example
The following will cause the CLI to pause for 30 seconds.

```
sleep 30
```
srp initiate-switchover

Changes the device status on the primary and backup systems configured for Interchassis Session Recovery (ICSR) support employing Service Redundancy Protocol (SRP).

**Product**

All products that support ICSR

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Mode**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
srp initiate-switchover [ force | post-processing-timeout | reset-route-modifier | timeout seconds ] [ -noconfirm ]
```

---

**force**

Switchover by force, without any validating checks.

---

**post-processing-timeout**

Specifies the timeout value (in seconds) to initiate the post-switchover process as an integer from 0 through 3600.

---

**reset-route-modifier**

During a switchover, resets the route-modifier to the initial value.

---

**timeout seconds**

Specifies the number of seconds before a forced switchover occurs as an integer from 0 through 65535. Default: 300

---

**-noconfirm**

Executes the command without any additional prompt and confirmation from the user.

---

**Usage**

This command executes a forced switchover from active to inactive. The command must be executed on the active system and switches the active system to the inactive state and the inactive system to an active state.

---

**Example**

The following initiates a switchover in 30 seconds.

```
srp initiate-switchover timeout 30
```
srp reset-auth-probe-fail

Resets Service Redundancy Protocol (SRP) authentication probe monitor failure information.

**Product**
All products that support Interchassis Session Recovery (ICSR)

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
srp reset-auth-probe-fail
```

**Usage**

This command resets the auth probe monitor failure information to 0.
srp reset-diameter-fail

Resets Service Redundancy Protocol (SRP) Diameter monitor failure information.

**Product**
All products that support Interchassis Session Recovery (ICSR)

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

**Syntax**

```
srp reset-diameter-fail
```

**Usage**
This command resets the Diameter monitor failure information to 0.
**srp terminate-post-process**

forcibly terminates post-switchover processing by primary and backup systems configured for Interchassis Session Recovery (ICSR) support employing Service Redundancy Protocol (SRP).

**Product**
All products that support ICSR

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
srp terminate-post-process [ -noconfirm ]
```

- **-noconfirm**
  
  Executes the command without any additional prompt and confirmation from the user.

**Usage**

Use this command to force the termination of post-switchover process.

**Example**

```
srp terminate-post-process
```
srp validate-configuration

Initiates a configuration validation check from the active chassis via Service Redundancy Protocol (SRP).

**Product**
All products that support Interchassis Session Recovery (ICSR)

**Privilege**
Security Administrator, Administrator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
srp validate-configuration
```

**Usage**
Validates the configuration for an active chassis.
**srp validate-switchover**

Validates both active and standby systems are ready for a planned Service Redundancy Protocol (SRP) switchover.

**Product**
All products that support Interchassis Session Recovery (ICSR)

**Privilege**
Security Administrator, Administrator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
srp validate-switchover
```

**Usage**
Validates that both active and standby systems are ready for a planned SRP switchover.
ssh

Connects to a remote host using a secure shell (SSH) interface.

**Product**
All

**Privilege**
Security Administrator, Administrator, Operator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
ssh { host_name | host_ip_address } [ port port_num ] [ user user_name ]
```

- `host_name | host_ip_address`
  Identifies the remote node with which to attempt connection.
  - `host_name`: specifies the remote node using its logical host name which must be resolved via DNS lookup.
  - `host_ip_address`: specifies the remote node using its assigned IP address in IPv4 dotted-decimal notation.

- `port port_num`
  Specifies a specific port for connection as an integer from 1025 through 10000.

- `user user_name`
  Specifies the user name attempting connection.

**Usage**

SSH connects to a remote network element using a secure interface.

**Example**

The following connects to remote host `remoteABC` as user `user1`.

```
ssh remoteABC user user1
```

The following connects to remote host `10.2.3.4` without any default user.

```
ssh 10.2.3.4
```

The following connects to remote host `10.2.3.4` via port `2047` without any default user.

```
ssh 10.2.3.4 port 2047
```
start crypto security-association

Initiates Internet Key Exchange (IKE) negotiations.

**Product**
- PDSN
- HA
- GGSN

**Privilege**
- Security Administrator, Administrator, Operator, Inspector

**Mode**
- Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
start crypto security-association cryptomap
```

- **cryptomap**
  Specifies the name of an existing crypto map policy to use when starting the IKE negotiations as an alphanumeric string of 1 through 127 characters.

**Usage**

Use this command to start IKE negotiations for IPSEC.

**Example**

The following command starts the IKE negotiations using the parameters set in the crypto map named cryptomap1:

```
start crypto security-association cryptomap1
```
system

Configures information about the system that will be accessible by the SNMP agent.

Product
P-GW
SAEGW

Privilege
Security Administrator, Administrator

Mode
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

```
system { carrier-id mcc mcc_num mnc mnc_num | contact name | description description | hostname name | location location }

default system { contact | description | hostname | location }

no system carrier-id
```

```
carrier-id mcc mcc_num mnc mnc_num
Specifies the system’s Carrier ID via the three-digit MCC (mobile country code) and three-digit MNC (mobile network code).

contact name
Specifies the system’s contact name as an alphanumeric string from 0 through 255 characters.

description description
Defines description text that as an alphanumeric string from 1 through 255 characters that includes text and some parameters, including:

- %version% - software version
- %build% - software build number
- %chassis% - chassis type (“asr5000”)
- %staros% - ID of the kernel revision
- %ostype% - os type
- %hostname% - system name
- %release% - release
- %kerver% - kernel version
- %machine% - machine hardware name

Default: “%ostype% %hostname% %release% %kerver% %machine%”
After replacing the parameters with values, the string will be truncated if the length is greater than 255.
```
**hostname name**

Specifies the system’s host name (name of system) as an alphanumeric string of 1 through 63 characters.

**location location**

Specifies the system’s geographic or referenced location as an alphanumeric string of 0 through 255 characters.

**default system { contact | description | hostname | location }**

Sets/restores the default value assigned for specified parameter.

**no system carrier-id**

Removes the Carrier ID established for the system.

**Usage**

Use this command to configure information about the system that is accessible by the SNMP agent.

**Example**

The following command identifies the system’s location as *boston*:

```
  system location boston
```
This section includes the commands `telnet` through `upgrade url-blacklisting database`.

The Exec Mode is the initial entry point into the command line interface system. Exec mode commands are useful in troubleshooting and basic system monitoring.

**Mode**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
**tcpdump kernel**

Runs the tcpdump packet analyzer and prints out a description of the contents of packets on a specified network interface that match the boolean expression.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Mode**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
tcpdump kernel string
```

*string*

Specifies an existing interface match string as an alphanumeric string of 0 through 80 characters.

**Usage**

Runs the tcpdump packet analyzer and prints out a description of the contents of packets on a specified network interface that match the boolean expression. This analyzer performs a sniff operation at the mcdma0 interface using the kernel BIA (Bump-in-the-API) as a filter. This allows sniffing of kernel traffic complete with midplane header.
telnent

Connects to a remote host using the terminal-remote host protocol and a hostname or IPv4 address and port number.

**Product**
All

**Privilege**
Security Administrator, Administrator, Operator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

**Syntax**

```plaintext
telnet { host_name | host_ipv4_address } [ port port_num ]
```

<table>
<thead>
<tr>
<th>host_name</th>
<th>host_ipv4_address</th>
</tr>
</thead>
</table>

Identifies the remote node with which to attempt connection.

- **host_name**: specifies the remote node using its logical host name which must be resolved via DNS lookup.
- **host_ipv4_address**: specifies the remote node using its assigned IP address entered using the IPv4 dotted-decimal notation.

<table>
<thead>
<tr>
<th>port</th>
<th>port_num</th>
</tr>
</thead>
</table>

Specifies a specific port for connect connection as an integer from 1025 through 10000.

**Usage**

Telnet to a remote node for maintenance activities and/or troubleshooting when unable to do so directly.

**Important**: **telnet** is not a secure method of connecting between two hosts. **ssh** should be used whenever possible for security reasons.

**Example**

The following connects to remote host *remoteABC*.

```plaintext
telnet remoteABC
```

The following connects to remote host *10.2.3.4 port 2047*.

```plaintext
telnet 10.2.3.4 port 2047
```
telnet6

Connects to a remote host using the terminal-remote host protocol and a hostname or an IPv6 address and port number.

**Product**
All

**Privilege**
Security Administrator, Administrator, Operator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
telnet6 { host_name | host_ipv6_address } [ port port_num ]
```

- `host_name | host_ipv6_address`
  Identifies the remote node with which to attempt connection.
  - `host_name`: specifies the remote node using its logical host name which must be resolved via DNS lookup.
  - `host_ipv6_address`: specifies the remote node using its assigned IP address entered using the IPv6 colon-separated-hexadecimal notation.

- `port port_num`
  Specifies a specific port for connect connection as an integer from 1025 through 10000.

**Usage**

Telnet to a remote node for maintenance activities and/or troubleshooting when unable to do so directly.

**Important:** `telnet6` is not a secure method of connecting between two hosts. `ssh` should be used whenever possible for security reasons.

**Example**

The following connects to host `remoteABC`.

```
telnet6 remoteABC
```

The following connects to remote host `FE80::172.30.67.89 port 2047`.

```
telnet6 FE80::172.30.67.89 port 2047
```
terminal

Sets the number of rows or columns for display output.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

```
terminal { length lines | width characters }
```

<table>
<thead>
<tr>
<th>length</th>
<th>width</th>
</tr>
</thead>
<tbody>
<tr>
<td>lines</td>
<td>characters</td>
</tr>
</tbody>
</table>

length lines: sets the terminal length in number of lines (rows) of text from 5 to 4294967295 lines or the special value of 0 (zero). The value 0 sets the terminal length to infinity.
width characters: sets the terminal width in number of characters from 5 to 512 characters.

Usage

Set the length to 0 (infinite) when collecting the output of a command line interface session which is part of a scripted interface.

Example

The following sets the length then width in two commands.

```
terminal length 66
terminal width 160
```

The following command sets the number of rows of the terminal to infinity.

```
terminal length 0
```
test alarm

Tests the alarm capabilities of the chassis.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

test alarm { audible | central-office { critical | major | minor } }

- **audible**: Tests the internal alarm on the ASR 5000 System Management Card (SMC) or the ASR 5500 System Status Card (SSC) for 10 seconds. The alarm status is returned to its prior state, such as if the audible alarm was enabled prior to the test, the alarm will again be enabled following the test.
- **central-office { critical | major | minor }**: Tests the specified central office alarm type.

Usage
Test the alarm capabilities of the chassis as periodic maintenance to verify the hardware for generation of the internal audible alarms is functional.

⚠️ **Caution**: The use of test commands could adversely affect the operation of your system. It is recommended that they only be used under the guidance and supervision of qualified support representative.

Example

test alarm audible

test alarm central-office critical

test alarm central-office major

test alarm central-office minor
test ipcf bindmux

Tests the status of the Intelligent Policy Control Function (IPCF) BindMux Manager instance and also starts or stops the BindMux Manager instance on the chassis.

**Product**
IPCF

**Privilege**
Security Administrator, Administrator, Operator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

**Syntax**

```bash
test ipcf bindmux [ start | stop ]
```

**start**

Starts the IPCF BindMux Manager on the chassis. If already an instance of IPCF BindMux Manager is running it prompts accordingly.

**stop**

Stops the IPCF BindMux Manager instance running on the chassis.

**Usage**

Use this command to test the status of IPCF BindMux Manager instance and also to start or stop the BindMux Manager instance on the chassis.

**Caution:** The use of test commands could adversely affect the operation of your system. It is recommended that they only be used under the guidance and supervision of qualified support representative.

**Example**

The following command stops the BindMux Manager instance running on the chassis:

```bash
test ipcf bindmux stop
```
test ipsec tunnel ip-pool

Tests a specified IPSec tunnel associated with an IP pool name.

**Product**
All

**Privilege**
Security Administrator, Administrator, Operator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
test ipsec tunnel ip pool pool_name destination-ip ip_address }

  pool_name destination-ip ip_address

  ip pool pool_name: Specifies the name of an existing IP pool as an alphanumeric string of 1 through 32 characters.
  destination-ip ip_address: Specifies a destination IP address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation
```

**Usage**

Use this command to test a specified IPSec tunnel.

⚠️ **Caution:** The use of test commands could adversely affect the operation of your system. It is recommended that they only be used under the guidance and supervision of qualified support representative.

**Example**

```
test ipsec tunnel ip pool pool3 destination-ip 10.2.3.4
```
test mobile tunnel

Tests for the existence of a specified mobile tunnel.

Product
All

Privilege
Security Administrator, Administrator, Operator

Mode
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

test mobile tunnel { callid call_id | imsi imsi_value | ipaddr ip_address | msid msid_num | nai nai_value }

callid call_id
Specifies the exact call instance ID which is to have trace data logged as a 4-byte hexadecimal number.

imsi imsi_value
Specifies the International Mobile Subscriber Identity (IMSI) of the subscriber session to be monitored an integer from 1 through 15 characters.

ipaddr ip_address
Specifies the IP address of the subscriber session to be monitored in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

msid msid_num
Specifies the mobile subscriber identification number to be monitored as 7 to 16 digits of an IMSI, MIN, or RMI.

nai nai_value
Specifies the mobile session Network Access Identifier as an alphanumeric string of 1 through 256 characters. The NAI is the user identity submitted by the client during network access authentication.

Usage
Use this command to test a specified mobile tunnel.

⚠️ Caution: The use of test commands could adversely affect the operation of your system. It is recommended that they only be used under the guidance and supervision of qualified support representative.
test mobile tunnel ipaddr 192.64.66.9
timestamps

Enables or disables the generation of a timestamp in response to each command entered. The timestamp does not appear in any logs as it is a CLI output only. This command affects the current CLI session only. Use the `timestamps` command in the Global Configuration Mode to change the behavior for all future CLI sessions.

**Product**

All

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Mode**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
[ no ] timestamps
```

- **no**
  
  Disables generation of timestamp output for each command entered. When omitted, the output of a timestamp for each entered command is enabled.

**Usage**

Enable timestamps when logging a CLI session on a remote terminal such that each command will have a line of text indicating the time when the command was entered.
traceroute

Collects information on the route data will take to a specified IPv4 host.

Product

All

Privilege

Security Administrator, Administrator, Operator, Inspector

Mode

Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Important: Inspector privileges are granted for all variables except count and port. To initiate a traceroute count or to target a specific port for a traceroute, you must have a minimum privilege level of Operator.

Syntax

traceroute { host_name | host_ip_address } [ count packets ] [ df ] [ maxttl max_ttl ] [ minttl min_ttl ] [ port port_num ] [ size octet_count ] [ src { src_host_name | src_host_ip_address } ] [ timeout seconds ] [ vrf vrf_name ] [ | { grep grep_options | more } ]

host_name | host_ip_address

Identifies the remote node to trace the route to.

df

Indicates the packets for the tracing of the route should not be fragmented. If a packet requires fragmenting, it is dropped and the result is the ICMP response "Unreachable, Needs Fragmentation" is received.

maxttl max_ttl

Specifies the maximum time to live for the route tracing packets as an integer from 1 through 255. max_ttl must be greater than min_ttl whether min_ttl is specified or defaulted. Default: 30

The time to live (TTL) is the number of hops through the network; it is not a measure of time.

minttl min_ttl

Specifies the minimum time to live for the route tracing packets as an integer from 1 through 255. min_ttl must be less than max_ttl whether max_ttl is specified or defaulted. Default: 1

The time to live (TTL) is the number of hops through the network; it is not a measure of time.
Traceroute is a command used to trace the route packets take as they travel from a source to a destination. It is particularly useful for debugging network problems by identifying bottlenecks in the routing of data within the network. The command allows specifying various parameters to customize its behavior.

### Parameters

- **port port_num**
  Specifies a specific port for connection as an integer from 1 through 65535. Default: 33434

- **size octet_count**
  Specifies the number of bytes for each packet as an integer from 40 through 32768. Default: 40

- **src { src_host_name | src_host_ip_address }**
  Specifies an IP address to use in the packets as the source node. Default: originating system’s IP address
  - **src_host_name**: specifies the remote node using its logical host name which must be resolved via a DNS lookup.
  - **src_host_ip_address**: specifies the remote node using its assigned IP address specified entered using IPv4 dotted-decimal notation.

- **timeout seconds**
  Specifies the maximum time (in seconds) to wait for a response from each route tracing packet as an integer from 2 through 100. Default: 5

- **vrf vrf_name**
  Specifies the name of an existing virtual routing and forwarding (VRF) context associated with this route as an alphanumeric string of 1 through 63 characters. Associates a Virtual Routing and Forwarding (VRF) context with this static ARP entry.

- **grep grep_options | more**
  Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
  For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in this guide.

### Usage

Trace an IPv4 route when troubleshooting network problems where certain nodes are having significant packet delays or packet loss. This can also be used to identify bottlenecks in the routing of data within the network.

### Example

The following command traces the route to remote host `remoteABC` and sends the output to the more command.

```
traceroute remoteABC | more
```

The following command traces the route to remote host `10.2.3.4`’s port 2047 waiting a maximum of 2 seconds for responses.

```
traceroute 10.2.3.4 port 2047 timeout 2
```
**traceroute6**

Collects information on the route data will take to a specified IPv6 host.

**Product**

All

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Mode**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Important:** Inspector privileges are granted for all variables except **count** and **port**. To initiate a traceroute count or to target a specific port for a traceroute, you must have a minimum privilege level of Operator.

**Syntax**

```
traceroute6 { host_name | host_ipv6_address } [ count packets ] [ maxttl max_ttl ] [ port port_num ] [ size octet_count ] [ src { src_host_name | src_host_ipv6_address } ] [ timeout seconds ] [ vrf vrf_name ] [ | { grep grep_options | more } ]
```

- **host_name** | **host_ipv6_address**
  - Identifies the remote node to trace the route to.
  - **host_name:** specifies the remote node using its logical host name which must be resolved via DNS lookup.
  - **host_ipv6_address:** specifies the remote node using its assigned IP address entered using the IPv6 colon-separated-hexadecimal notation.

- **count packets**
  - Specifies the number of UDP probe packets to send. Default: 3

- **maxttl max_ttl**
  - Specifies the maximum time to live for the route tracing packets as an integer from 1 through 255. **max_ttl** must be greater than **min_ttl** whether **min_ttl** is specified or defaulted. Default: 30
  - The time to live (TTL) is the number of hops through the network; it is not a measure of time.

- **port port_num**
  - Specifies a specific port for connection as an integer from 1 through 65535. Default: 33434

- **size octet_count**
  - Specifies the number of bytes for each packet as an integer from 40 through 32768. Default: 40

- **src { src_host_name | src_host_ipv6_address }**
  - Specifies an IP address to use in the packets as the source node. Default: originating system’s IP address
**src_host_name**: specifies the remote node using its logical host name which must be resolved via a DNS lookup.

**src_host_ipv6_address**: specifies the remote node using its assigned IP address specified entered using IPv6 colon-separated-hexadecimal notation.

---

**timeout seconds**

Specifies the maximum time (in seconds) to wait for a response from each route tracing packet as an integer from 2 through 100. Default: 5

---

**vrf vrf_name**

Specifies the name of an existing virtual routing and forwarding (VRF) context associated with this route as an alphanumeric string of 1 through 63 characters.

---

**grep grep_options | more**

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the **Regulating a Command’s Output** section of the **Command Line Interface Overview** chapter in this guide.

---

**Usage**

Trace an IPv6 route when troubleshooting network problems where certain nodes are having significant packet delays or packet loss. This can also be used to identify bottlenecks in the routing of data within the network.

---

**Example**

The following command traces the route to remote host *remoteABC* and sends the output to the more command.

```
traceroute6 remoteABC | more
```

The following command traces the route to remote host *2000:4A2B::1f3F*'s port 2047 waiting a maximum of 2 seconds for responses.

```
traceroute6 2000:4A2B::1f3F port 2047 timeout 2
```
update active-charging

Updates specified active charging option(s) for the matching sessions.

Product
ACS
PSF
NAT

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

update active-charging { switch-to-fw-and-nat-policy fw_nat_policy_name | switch-to-rulebase rulebase_name | switch-to-tpo-policy tpo_policy_name } { all | callid call_id | fw-and-nat-policy fw_nat_policy_name | imsi imsi | ip-address ip_address | msid msid | rulebase rulebase_name | tpo-policy tpo_policy_name | username user_name } [ -noconfirm ] [ | { grep grep_options | more } ]

switch-to-fw-and-nat-policy fw_nat_policy_name

Specifies an existing Firewall-and-NAT policy to switch to as an alphanumeric string of 1 through 63 characters.

switch-to-rulebase rulebase_name

Specifies an existing rulebase to switch to as an alphanumeric string of 1 through 63 characters.

switch-to-tpo-policy tpo_policy_name

Important: The Traffic Performance Optimization (TPO) in-line service is not supported in this release.

all

Updates rulebase/policy for all subscribers.

callid call_id

Updates rulebase/policy for the Call Identification number specified as an eight-digit hexadecimal number.

fw-and-nat-policy fw_nat_policy_name

Updates the rulebase/policy for sessions matching an existing Firewall-and-NAT policy specified as an alphanumeric string of 1 through 63 characters.
**imsi**  
Updates rulebase/policy for International Mobile Subscriber Identification (IMSI) specified here.  
*imsi* must be 3 digits of MCC (Mobile Country Code), 2 or 3 digits of MNC (Mobile Network Code), and the rest with MSIN (Mobile Subscriber Identification Number). The total should not exceed 15 digits. For example, 123-45-678910234 can be entered as 12345678910234.

**ip-address**  
Updates rulebase/policy for the IP address specified in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

**msid**  
Updates rulebase/policy for an MSID specified as a string of 1 through 24 characters.

**rulebase**  
Updates rulebase/policy for sessions matching an existing rulebase specified as an alphanumeric string of 1 through 63 characters.

**tpo-policy**  
Updates rulebase/policy for sessions matching an existing rulebase specified as an alphanumeric string of 1 through 63 characters.

---

**Important**: The Traffic Performance Optimization (TPO) in-line service is not supported in this release.

**username**  
Updates rulebase/policy for user specified as a an alphanumeric of characters and/or wildcard characters (‘$’ and ‘*’) of 1 through 127 characters.

**-noconfirm**  
Executes the command without any additional prompt and confirmation from the user.

```
| { grep grep_options | more }
```

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.  
For details on the usage of **grep** and **more**, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference.

---

**Usage**  
Use this command to change specified active charging option(s) for the matching sessions.

**Example**  
The following command changes the rulebase for sessions using the rulebase named `standard` to use the rulebase named `super`:

```
update active-charging switch-to-rulebase super rulebase standard
```
**update cscf**

Causes a NOTIFY to be triggered from Call Session Control Function (CSCF) based on registration state and event and indicating the expiry timer value for each contact as “reauthentication-time” provided from the CLI. The subscriber is supposed to send a fresh REGISTER message within “reauthentication-time”, which will be challenged by CSCF as part of reauthentication. If reauthentication fails, the subscriber will be cleared after “reauthentication-time”.

**Product**
SCM (P-CSCF, S-CSCF)

**Privilege**
Administrator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local] host_name#  
```

**Syntax**

```
update cscf subscriber { all | username user_name } cscf-service service_name { { [ contact contact_address ] reg-state { active event { refreshed | shortened } time sec } | terminated event { deactivated | expired | rejected | unregistered } } | reauthentication-time sec } [ verbose ]
```

- **subscriber { all | username user_name }**
  Updates CSCF subscriber data.
  - all: Updates data for all subscribers within a specified CSCF service.
  - username user_name: Specifies the name of a user within the current context as an alphanumeric string of 1 through 127 characters that is case sensitive.

- **cscf-service service_name**
  Specifies a configured CSCF service as an alphanumeric string of 1 and 63 characters that is case sensitive.

- **contact contact_address**
  Specifies the contact address of the subscriber as an alphanumeric string of 1 through 255 characters.

- **reg-state**
  Specifies the registration state of the subscriber.

- **active event { refreshed | shortened } time sec**
  Specifies the registration state active event type.
  - refreshed: Specifies registration state active event as refreshed.
  - shortened: Specifies registration state active event as shortened.

- **time sec**
  Specifies the time (in seconds) within which subscriber is expected to re-authenticate as an integer from 1 to 86400.
terminated event { deactivated | expired | rejected | unregistered }

Specifies the registration state terminated event type.

deactivated: Specifies registration state terminated event as deactivated.
expired: Specifies registration state terminated event as expired.
rejected: Specifies registration state terminated event as rejected.
unregistered: Specifies registration state terminated event as unregistered.

reauthentication-time sec

Specifies the time (in seconds) within which the subscriber is expected to re-authenticate as an integer from 1 to 86400.

verbose

Show detailed information.

Usage

This command is only applicable for a P-CSCF and S-CSCF service. When optional contact ID is not specified, all the contact IDs associated with specified user or all users will be updated and trigger NOTIFY.

Important: reauthentication-time should be greater than the current expiry time of the contact so that CSCF will initiate the NOTIFY message.

Example

The following command sets the re-authentication time for all CSCF subscribers in the scscf1 S-CSCF service to 500 seconds:

    update cscf subscriber all cscf-service scscf1 reauthentication-time 500
update firewall policy

This command is obsolete.
**update ip access-list**

When you update an IP Access list, this command forces the new version of the access list to be applied to any subscriber sessions that are currently using that list.

**Product**

- PDSN
- GGSN
- ASN-GW

**Privilege**

Security Administrator, Administrator

**Mode**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
update ipv6 access-list list_name subscribers [ command_keyword ] [ filter_keywords ] [-noconfirm] [verbose] 
```

**list_name**

Specifies the name of an existing IP Access list that you want to apply to the subscriber as an alphanumeric string of 1 through 47 characters.

**[ command_keyword ] [ filter_keywords ]**

These are the same command keywords and filter keywords available for the ```show subscribers``` command.

**-noconfirm**

Executes the command without any additional prompt and confirmation from the user.

**verbose**

Show detailed information.

**Usage**

Use this command to force existing subscriber sessions that are already using a specific IP Access list to have that IP Access list reapplied. This is useful when you edit an IP Access list and want to make sure that even existing subscriber sessions have the new changes applied.

**Example**

To apply the IP Access list named `ACLlist11` to all existing subscribers that are already using that IP Access list, enter the following command:

```
update ip access-list ACLlist11 subscribers all
```
update ipv6 access-list

When you update an IP Access list, this command forces the new version of the access list to be applied to any subscriber sessions that are currently using that list.

Product
PDSN
GGSN
ASN-GW

Privilege
Security Administrator, Administrator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

update ipv6 access-list list_name subscribers [ command_keyword ] [ filter_keywords ] [-noconfirm] [verbose]

**list_name**
Specifies the name of an existing IPv6 Access list that you want to apply to the subscriber as an alphanumeric string of 1 through 47 characters.

[ command_keyword ] [ filter_keywords ]
These are the same command keywords and filter keywords available for the show subscribers command.

-noconfirm
Executes the command without any additional prompt and confirmation from the user.

-verbose
Show detailed information.

Usage
Use this command to force existing subscriber sessions that are already using a specific IPv6 Access list to have that IPv6 Access list reapplied. This is useful when you edit an IPv6 Access list and want to make sure that even existing subscriber sessions have the new changes applied.

Example
To apply the IPv6 Access list named ACLv6List1 to all existing subscribers that are already using that IP Access list, enter the following command:

update ipv6 access-list ACLv6List1 subscribers all
update local-user database

Updates the local user (administrative) database with current user information. Run this command immediately after creating, removing or editing administrative users.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
update local-user database
```

**Usage**
Use this command to update the local-user database with current information.

**Example**

The following command updates the local-user database:

```
update local-user database
```
update module

Loads a specified plugin module from the Module Priority List with the lowest priority number. This will also copy the Module priority list onto the Version priority list. This function is associated with the patch process for accommodating dynamic software upgrades.

**Product**
ADC

**Privilege**
Security Administrator, Administrator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
update module plugin_name
```

**Usage**

Specifies the name of an existing plugin module that you want to update as an alphanumeric string of 1 through 16 characters. If the named module is not known to the system, an error message is displayed.

Use this command to initiate an update of a new software plugin module. If it fails to load, the module with next highest priority will be loaded. If none of the modules are installed, the default patch which comes along with the ASR 5000 build is automatically loaded. The specified module must have been previously unpacked/verified and configured via the `install plugin` and `plugin` commands respectively. For additional information, refer to the Plugin Configuration Mode Commands chapter.

**Example**

The following command updates the plugin module named `p2p`:

```
update module p2p
```
update qos policy map

Updates QoS profile information based on specific subscriber policy maps.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

update qos policy-map map_name use-granted-profile-id id1 [ id2 ] [ id3 ] subscribers [ command_keyword ] [ filter_keywords ] [ -noconfirm ] [ verbose ] [ match-requested-profile-id ] [ | { grep grep_options | more } ]

map_name
Specifies the name of an existing policy map as an alphanumeric string of 1 through 15 characters.

use-granted-profile-id id1 [ id2 ] [ id3 ]
Specifies the profile IDs to update. Up to three different profile IDs can be specified. Each profile ID is specified as a hexadecimal value from 0x0 and 0xFFFF.

subscribers [ command_keyword ] [ filter_keywords ]
These are the same command keywords and filter keywords available for the show subscribers command.

[ -noconfirm ]
Updates matching subscribers without prompting for confirmation.

[ verbose ]
Displays details for the profile updates.

[ match-requested-profile-id ]
Sends session-updates only to profile-ids matching the profile-ids in the requested list.

grep grep_options | more
Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in this guide.
Usage
Use this command to update subscriber session profile IDs based on the specified criteria.

Example
The following command updates profile IDs 0x3E and 0x4C for all subscriber sessions and sends session-updates with the IDs:

```
update qos policy-map test use-granted-profile-id 0x3E 0x4C subscribers all match-requested-profile-id
```
update qos tft

Updates the subscriber traffic flow template (TFT) associated with the flow ID and direction.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
update qos tft flow-id flow-id flow-dir { forward | reverse } use-granted-profile-id id1 [ id2 ] [ id3 ] subscribers [ command_keyword ] [ filter_keywords ] [-noconfirm ] [ verbose ] [ match-requested-profile-id ] [ | { grep grep_options | more }]
```

- **flow-id** `flow-id`
  Sends session updates only when the flow ID matches the flow-id and flow-direction. `flow-id` must be specified as an integer from 1 through 255.

- **flow-dir** `{ forward | reverse }`
  Specifies the direction of the TFT flow.

- **subscribers** `{ command_keyword } [ filter_keywords ]`
  These are the same command keywords and filter keywords available for the `show subscribers` command.

**Usage**
Supports QoS updates based on subscriber TFTs.

**Example**

```
update qos tft flow-id 0 flow-dir reverse use-granted-profile-id 0x0 subscribers all -noconfirm
```
Exec Mode Commands (T-Z)

upgrade

Installs major software releases to the system.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local] host_name#

Syntax

upgrade { online | patch } image_url config cfg_url [ -noconfirm ]

<table>
<thead>
<tr>
<th>online</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perform a software upgrade from one release version to another. The online upgrade is only available for software release 3.5 and higher.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>patch</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install an interim, or patch, software release.</td>
</tr>
</tbody>
</table>

**Important**: Software Patch Upgrades are not supported in this release.

image_url

Specifies the location of a image file to use for system startup. The URL may refer to a local or a remote file. The URL must be formatted as follows:

For the ASR 5000:

```
[ file: ] { /flash | /pcmcia1 | /hd } [ /directory ]/file_name
[ http: | tftp: ]//{ host[ :port# ] } [ /directory ]/file_name
```

For the ASR 5500:

```
[ file: ] { /flash | /usb1 | /hd } [ /directory ]/file_name
[ http: | tftp: ]//{ host[ :port# ] } [ /directory ]/file_name
```

**Important**: Do not use the following characters when entering a string for the field names below: “/” (forward slash), “:” (colon) or “@” (at sign).

directory is the directory name.
filename is the actual file of interest.
Exec Mode Commands (T-Z)

**upgrade**

- **host** is the IP address or host name of the server.
- **port#** is the logical port number that the communication protocol is to use.

**Important:** A file intended for use on an ASR 5000 uses the convention xxxx.ASR5000.bin, where xxxx is the software build information.

**Important:** When using the TFTP, you should use a server that supports large blocks, per RFC 2348. This can be implemented by using the “block size option” to ensure that the TFTP service does not restrict the file size of the transfer to 32MB.

```plaintext
config config_path
```

Specifies the location of a configuration file to use for system startup. This must be formatted as follows:
For the ASR 5000:

```
[ file: ]{ /flash | /pcmcia | /hd }[ /path ]/filename
```

For the ASR 5500:

```
[ file: ]{ /flash | /usb1 | /hd }[ /path ]/filename
```

Where **path** is the directory structure to the file of interest, and **filename** is the name of the configuration file. This file typically has a .cfg extension.

- **-noconfirm**

Executes the command without any additional prompt and confirmation from the user.

**Usage**

Use the **upgrade online** command to perform a software upgrade when upgrading from one software release version to another, providing that both versions support this feature. For example, you can use this method to upgrade from release version 3.5 (any build number) to version 4.0 (any build number), but you cannot use this method to upgrade from release version 3.0 to version 3.5 since version 3.0 does not support the feature.

**Important:** Software Patch Upgrades are not supported in this release.

**Important:** This command is not supported on all platforms.

**Example**

The following command performs a major software release upgrade from an older version to a newer version. In this example the new software image file is in a subdirectory on a tftp server, and the configuration file is in a subdirectory on the local flash at tftp://host[/path]/filename.

```
upgrade online tftp://imageserver/images/image.bin config
/flash/configurations/localconfig.cfg
```
upgrade content-filtering

Upgrades the Static Rating Database (SRDB) for Category-based Content Filtering application.

**Product**
CF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
upgrade content-filtering category { database | rater-pkg }
```

- **upgrade content-filtering category database**
  
  Triggers the upgrade of the Category-based Content Filtering Static Rating Database (SRDB).

- **upgrade content-filtering category rater-pkg**
  
  
  The *rater.pkg* file contains the models and feature counters that are used to return the dynamic content rating. The upgrade will trigger distribution of the *rater.pkg* to all the SRDBs.

**Important:** This command is customer specific. For more information, please contact your local sales representative.

**Usage**

Use this command to load the Static Rating Database (SRDB) into memory for Category-based Content Filtering application, and/or to load the *rater.pkg* file.

If the default directory of /cf does not exist on the flash, it will create the same. It also locates the recent full database and loads it into memory. This command also clears the old and excess incremental databases.

**Important:** This command is not supported on all platforms.

**Example**

The following command upgrades the SRDB for the Category-based Content Filtering application:

```
upgrade content-filtering category database
```
upgrade tethering-detection

Upgrades the Tethering Detection feature’s database(s).

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

**Syntax**

```
upgrade tethering-detection database { all | os-signature | tac | ua-signature } [-noconfirm ]
```

- **all**
  Upgrades all Tethering Detection databases—OS, TAC and UA.

- **os-signature**
  Upgrades only the OS database.

- **tac**
  Upgrades only the TAC database.

- **ua-signature**
  Upgrades only the UA database.

- **- noconfirm**
  Executes the command without any prompts and confirmation from the user.

**Usage**

Use this command to upgrade the database(s) used by the Tethering Detection feature. This command upgrades the database(s) from file(s) kept in designated path. The name of the existing source file is prefixed with the word “new-“. For example for OS DB, if the existing file name is “os-db”, the upgrade file name is “new-os-db”. If there is a file named “new-xxx-db”, it is verified that it is a valid Tethering Detection database and then loaded into memory. If successful, the files is renamed “xxx-db” to “xxx-db-<number>” and then renamed “new-xxx-db” to “new-xxx-db”. For example, the command `upgrade tethering-database ua-signature -noconfirm` results in loading the file by name “new-ua-db” if it is present in the designated directory. In case of a successful upgrade, the previous version of the database is stored as backup in a file named “ua-db-1”. Also, the newly uploaded database file is renamed as “ua-db”.

Cisco ASR 5x00 Command Line Interface Reference
Also see the `tethering-database` command in the *ACS Configuration Mode Commands* chapter.

The following command upgrades all Tethering Detection databases:

```
upgrade tethering-detection database all -noconfirm
```
up upgrade url-blacklisting database

Upgrades the URL blacklisting database.

**Product**
CF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec
The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
upgrade url-blacklisting database [-noconfirm]
```

- **-noconfirm**
  Executes the command without any additional prompt and confirmation from the user.

**Usage**
Use this command to upgrade and load a URL blacklisting database whenever required.

**Example**

```
upgrade url-blacklisting database
```
Chapter 127
Exec Mode show Commands (A-C)

This section includes the commands `show aaa` through `show css service`.

The Exec Mode is the initial entry point into the command line interface system. Exec mode `show` commands are useful in troubleshooting and basic system monitoring.

**Mode**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
show aaa

Displays AAA (Authentication Authorization and Accounting) statistics for the current context.

Product
PDSN
GGSN
SGSN

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show aaa { group { all | name aaa_group_name } | local counters } [ | { grep grep_options | more } ]

| group { all | name aaa_group_name } |
| Displays AAA information. |
| •all: If the exec context is local, information for all the default AAA groups, and the AAA groups configured in all the contexts are displayed. If the exec context is not local, information for only the context-specific AAA groups are displayed. |
| •name aaa_group_name: Displays information for an existing AAA group specified as an alphanumeric string of 0 through 64 characters. |

| local counters |
| Displays information for current context. |

| | { grep grep_options | more } |
| Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent. |
| For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter. |

Usage
This command is used to view accounting and authentication statistics for the current context.

Example
The following command displays AAA statistics for the current context:

show aaa local counters

The following command displays AAA statistics for the AAA group aaa_group1:
show aaa group name aaa_group1

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*.
show active-charging analyzer statistics

Displays statistical information for protocol analyzers.

**Product**
ACS

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
show active-charging analyzer statistics [ name protocol_name [ instance instance_number ] [ verbose ] ] [ | { grep grep_options | more } ]
```

**name protocol_name**
Displays detailed information for the specified protocol analyzer:
- dns
- file-transfer
- ftp
- h323
- http
- icmp
- icmpv6
- imap
- ip
- ipv6
- mms
- p2p [ application p2p_list | protocol-group group_list ]: Peer-to-peer analyzer.
  - p2p application p2p_list: The supported applications are:
    - actionvoip
    - actsync
    - adobeconnect
    - aimini
    - amazoncloud
    - antsp2p
    - apple-push
```
• apple-store
• applejuice
• applemaps
• ares
• armagettron
• avi
• badoo
• baidumovie
• battlefld
• bbm
• beatport
• bitcasa
• bittorrent
• bittorrent-sync
• blackberry-store
• blackberry
• blackdialer
• box
• callofduty
• chikka
• cisco-jabber
• citrix
• clubbox
• clubpenguin
• crossfire
• cyberghost
• ddlink
• didi
• directconnect
• dofus
• dropbox
• edonkey
• facebook
• facetime

**Important:** The `facetime` protocol is available only in releases 9.0 and 11.0. This protocol is not available in release 10.0.
show active-charging analyzer statistics

*fasttrack
*feidian
*fiesta
*filetopia
*flash
*flickr
*florensia
*foursquare
*freenet
*friendster
*fring
*funshion
*gadu_gadu
*gamekit

**Important:** The **gamekit** protocol is available only in releases 9.0 and 11.0. This protocol is not available in release 10.0.

*gmail
*gnutella
*goober
*google-music
*google-push
*google
*googleplay
*googleplus
*gotomeeting
*gtalk
*guildwars
*halflife2
*hamachivpn
*hbogo
*heytell
*hike-messenger
*hls
*hotspotvpn
*hulu
*hyves
```markdown
Exec Mode show Commands (A-C)

- iax
- icall
- icecast
- icloud
- idrive
- igo
- ihearradio
- imesh
- imessage
- imgur
- imo
- instagram
- iplayer
- iptv
- irc
- isakmp
- iskoot
- itunes
- jabber
- jap
- jumblo
- kakaotalk
- kik-messenger
- kontiki
- kugoo
- kuro
- linkedin
- lync
- magicjack
- manolito
- mapfactor
- mapi
- maplestory
- meebo
- mgcp
- mojo
- monkey3
```
show active-charging analyzer statistics

*mozy
*msn
*msrp
*mute
*mypeople
*myspace
*nateontalk
*naverline
*navigon
*netmotion
*nimbuzz
*nokia-store
*octoshape
*off
*ogg
*oist
*ooovoo
*opendrive
*openft
*openvpn
*orb
*oscar
*outlook
*paltalk
*pando
*pandora
*path
*pcanywhere
*pinterest
*plingm
*poco
*popo
*pplive
*ppstream
*ps3
*qq
*qqgame
show active-charging analyzer statistics

- qqlive
- quake
- quicktime
- radio-paradise
- radius
- rdp
- rdt
- regram
- rfactor
- rhapsody
- rmstream
- rodi
- rynga
- samsung-store
- scydo
- secondlife
- shoutcast
- silverlight
- siri
- skinny
- skydrive
- skype
- slacker-radio
- slingbox
- smartvoip
- snapchat
- softether
- sopcast
- soribada
- soulseek
- soundcloud
- spdy
- speedtest
- splashfighter
- spotify
- ssdp
- stealthnet
show active-charging analyzer statistics

*steam
*stun
*sudaphone
*svtplay
>tagged
*talkatone
*tango
*teamspeak
*teamviewer
*telegram
*thunder
*tor
*truecaller
*truphone
*tumblr
*tunnelvoice
*tvants
*tvuplayer
*twitch
*twitter
*ultrabac
*ultrasurf
*upc-phone
*usenet
*ustream
*uusee
*vchat
*veohrtv
*viber
*vine
*voipdiscount
*vopium
*vpnx
*voxer
*vtok
*vtun
*warcft3
show active-charging analyzer statistics

```
• waze
• webex
• wechat
• whatsapp
• wii
• windows-azure
• windows-store
• winmx
• winny
• wmstream
• wofkungfu
• wofwarcraft
• wuala
• xbox
• xdcc
• xing
• yahoo
• yahoomail
• youku
• yourfreetunnel
• youtube
• tattoo
```

```
p2p protocol-group group_list: The following P2P protocol groups are supported:
• generic
• anonymous-access
• business
• communicator
• cloud
• e-store
• e-mail
• e-news
• internet-privacy
• filesharing
• gaming
• p2p-filesharing
• p2p-anon-filesharing
```
EXECUTION MODE SHOW COMMANDS (A-C)

**show active-charging analyzer statistics**

- remote-control
- social-nw-gaming
- social-nw-generic
- social-nw-videoconf
- standard
- streaming

**wide [ all ]**: Displays all available P2P statistics in a single wide line. The **all** keyword displays all available P2P statistics without suppressing zeroes.

- pop3
- pptp
- rtcp
- rtp
- rtsp
- sdp
- secure-http
- sip
- smtp
- tcp
- tftp
- udp
- wsp
- wtp

```
[ instance instance_number ]
```

Displays the ACS/Session Manager information for specific instances.

*instance_number* must be an integer from 1 through 65535.

**verbose**

Specifies to display detailed (all available) information. If not specified, concise information is displayed.

```
| { grep grep_options | more }
```

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

**Usage**

Use this command to display statistic information for active charging protocol analyzers.

**Example**

The following command displays detailed statistic information for all P2P protocol analyzers:
show active-charging analyzer statistics name p2p verbose

The following command displays detailed statistic information for all TCP protocol analyzers:

show active-charging analyzer statistics name tcp verbose

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference.*
show active-charging bandwidth-policy

Displays information on bandwidth policies configured in a service.

Product
ACS

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show active-charging bandwidth-policy { all | name bandwidth_policy_name } [ | { grep grep_options | more } ]

- **all**
  Displays information for all bandwidth policies configured in the service.

- **name bandwidth_policy_name**
  Displays detailed information for an existing bandwidth policy specified as an alphanumeric string of 1 through 63 characters.

- **| { grep grep_options | more }**
  Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent. For details on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage
Use this command to view information on bandwidth policies configured in a service.

Example
The following command displays detailed information for the bandwidth policy named `standard`:

```
show active-charging bandwidth-policy name standard
```
show active-charging charging-action

Displays information for charging actions configured in the Active Charging Service (ACS).

Product
ACS

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

```
show active-charging charging-action { { { all | name charging_action_name } [ service name acs_service_name ] } | statistics [ name charging_action_name ] } [ | { grep grep_options | more } ]
```

- **all**
  Displays information for each configured charging action.

- **name charging_action_name**
  Displays detailed information for an existing charging action specified as an alphanumeric string of 1 through 63 characters.

- **statistics**
  Displays statistical information for all configured charging actions.

- **service name acs_service_name**
  Displays information for all or a specific charging action in the specified ACS. `acs_service_name` is an alphanumeric string of 1 through 15 characters.

| { grep grep_options | more }

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of `grep` and `more`, refer to the "Regulating a Command’s Output" section of the Command Line Interface Overview chapter.

Usage

Use this command to display information for charging actions configured in a service.

Example

The following command displays a detailed information for all charging actions:

```
show active-charging charging-action all
```
**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference.*
show active-charging content-filtering category policy-id

Displays Content Filtering (CF) category policy definitions. This command is not available on StarOS 8.0 and earlier releases.

Product
CF

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

display active-charging content-filtering category policy-id { all | id policy_id } [ | { grep grep_options | more } ]

all
Displays definitions of all Content Filtering category policies.

id policy_id
Displays definitions of an existing Content Filtering category policy specified as an integer from 1 through 4294967295.

| { grep grep_options | more }

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.
For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage
Use this command to view Content Filtering category definitions for a specific/all Policy IDs.

Example
The following command displays Content Filtering category definitions for policy ID 3:

show active-charging content-filtering category policy-id id 3

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show active-charging content-filtering category statistics

Displays category-based content filtering statistics.

Product
CF

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local] host_name#

Syntax

```
show active-charging content-filtering category statistics [ rulebase { name rulebase_name | all } ] [ verbose ] [ | { grep grep_options | more } ]
```

- **rulebase { name rulebase_name | all }
  Displays category-based content filtering statistics, either for all or for a specific rulebase.
  - **name rulebase_name**: Specifies an existing rulebase as an alphanumeric string of 1 through 63 characters.
  - **all**: Displays category-based content filtering statistics for each rulebase in the ACS.

- **verbose
Specifies to display detailed (all available) information. If not specified, concise information is displayed.

- | { grep grep_options | more }
  Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.
  For details on the usage of **grep** and **more**, refer to the **Regulating a Command’s Output** section of the **Command Line Interface Overview** chapter.

Usage
Use this command to view category-based content filtering statistics for a specific rulebase, or cumulative statistics for all rulebases in the ACS.

Example
The following command displays category-based content filtering statistics for the rulebase named **consumer**:

```
show active-charging content-filtering category statistics rulebase name consumer
```

The following command displays cumulative category-based content filtering statistics for all rulebases in verbose mode:
show active-charging content-filtering category statistics verbose

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show active-charging content-filtering server-group

Displays information for Content Filtering Server Group (CFSG) configured in the service.

**Product**
CF

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local] host_name#
```

**Syntax**

```
show active-charging content-filtering server-group [ name cfsg_name | statistics [ name cfsg_name [ acsmgr instance instance_number [ priority priority ] ] | verbose ] ] | { grep grep_options | more }
```

- `name cfsg_name`
  Specifies name of an existing CFSG as an alphanumeric string of 1 through 63 characters.

- `acsmgr instance instance_number`
  Specifies the manager instance as an integer from 1 through 65535.

- `priority priority`
  Specifies the priority of the server for which statistics has to be displayed as an integer from 1 through 65535.

- `verbose`
  Specifies to display detailed (all available) information, for each ICAP server connection at each instance. If not specified, concise information is displayed.

  ```
  | { grep grep_options | more }
  ```

  Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent. For details on the usage of `grep` and `more`, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter.

**Usage**

Use this command to view CFSG information/statistics.

- `show active-charging content-filtering server-group name cfsg_name`: The output of this command displays detailed information for the specified CFSG.
- `show active-charging content-filtering server-group statistics name cfsg_name`: The output of this command displays cumulative statistics for the specified CFSG. This will include all the instances and all the servers configured in the CFSG.
show active-charging content-filtering server-group statistics name cfs_name
acsmgr instance instance_number: The output of this command displays the cumulative statistics of all the ICAP server connections on the specified manager instance.

show active-charging content-filtering server-group statistics name cfs_name
acsmgr instance instance_number priority priority: The output of this command displays the statistics for the specified ICAP server connection on the specified manager instance.

show active-charging content-filtering server-group statistics verbose: The output of this command displays statistics of each ICAP server connection at each instance.

Example

The following command displays information for the CFSG named test12:

```
show active-charging content-filtering server-group name test12
```

The following command displays detailed information for all CFSGs:

```
show active-charging content-filtering server-group statistics verbose
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show active-charging credit-control

Displays statistics for Diameter/RADIUS Prepaid Credit Control Service in the Active Charging Service (ACS).

Product
ACS

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show active-charging credit-control { statistics [ group group_name | server { ip-address ip_address [ port port_num ] | name server_name } ] | session-states [ rulebase rulebase_name ] [ content-id content_id ] } [ | { grep grep_options | more } ]

statistics [ group group_name | server { ip-address ip_address [ port port_num ] | name server_name } ]

Displays prepaid credit control statistics.

*group group_name*: Displays statistics for an existing credit control group specified as an alphanumeric string of 1 through 63 characters.

*server { ip-address ip_address [ port port_num ] | name server_name }*

Displays statistics for the specified credit control server.

*ip-address ip_address*: Displays available statistics for the specified server’s address.

*port port_num*: Displays available statistics for the specified server’s port number.

*name server_name*: Displays the credit control statistics for the specified server.

session-states [ rulebase rulebase_name ] [ content-id content_id ]

Displays prepaid CCA session status based on rulebase and/or content ID.

*rulebase rulebase_name*: Displays the Credit Control Application (CCA) session state counts for an existing rulebase specified as an alphanumeric string of 1 through 63 characters.

*content-id content_id*: Displays CCA session state counts for a content ID of a credit control service specified as an integer from 1 through 65535.

| { grep grep_options | more } |

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.

For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.
**Usage**

Use this command to view statistics for Diameter/RADIUS prepaid credit control service in the ACS.

**Example**

The following command shows ACS statistics of configured Diameter or RADIUS Credit Control Application:

```
show active-charging credit-control statistics
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*.
show active-charging dns-learnt-ip-addresses

Displays DNS learnt IP address statistics for the DNS Snooping feature.

Product
ACS

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show active-charging dns-learnt-ip-addresses statistics { sessmgr { all | instance sessmgr_instance_number } [ verbose ] | summary } [ | { grep grep_options | more } ]

| sessmgr { all | instance sessmgr_instance_number } [ verbose ] |

Displays information for all or the specified Session Manager (SessMgr) instance.

- **all**: Displays information for all SessMgr instances.
- **instance sessmgr_instance_number**: Displays information for a SessMgr instance specified as an integer from 1 through 65535.
- **verbose**: Displays detailed statistics for specified criteria. Use this keyword to view the learnt IP addresses.

| summary |

Displays summary information.

| | { grep grep_options | more } |

Specifies that the output of this command is to be piped (sent) to the command specified. You must specify a command to which the output will be sent.

For details on the usage of `grep` and `more`, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to view statistics for the DNS Snooping feature related DNS learnt-ip-addresses. This command displays the number of learnt IP entries per rule line. It displays on a service level the number of resolved (learnt) IP addresses per rule line per rulebase (once if a rule line is used multiple times in the same rulebase as it is shared across rulebase) per destination context per SessMgr instance. It also displays the number of entries flushed due to TTL expiry. The field entries_replaced gives the number of entries replaced (same IP returned again) in the pool due to a DNS response by same/another subscriber for same domain-name, wherein the TTL of the entry will be replaced. IPv4-overflows will start incrementing when the maximum limit of 51200 across system is reached OR limit of 200 per pattern is reached.
Ipv6-overflows will start incrementing when maximum limit of 25600 across system is reached OR limit of 100 per pattern is reached. Limits are:
- Maximum of 51,200 IPv4 entries per instance shared across IPv4 all pools.
- Maximum of 200 IPv4 entries per pool (pool is same as discussed before (per rule-line pattern)).
- Maximum of 25,600 IPv6 entries per instance shared across all IPv6 pools.
- Maximum of 100 IPv6 entries per pool.

In releases prior to 14.0, this CLI command `show active-charging dns-learnt-ip statistics sessmgr all` displayed all the configured patterns and rulebase names for each of the pattern entry, even though the pattern has not learnt any IP address. When a large number of DNS snooping ruledefs are configured (configured as ip server-domain name under ruledef configuration), the memory allocated for sending this information exceeded the message size limit for messenger calls and hence the crash was observed.

To avoid the crash occurring, in 14.0 and later releases, the output of the CLI command `show active-charging dns-learnt-ip statistics sessmgr all` is modified to display only the patterns for which at least one IPv4/IPv6 address is learnt as all other information is available from the configuration. Also for each of the patterns this CLI command will not be displaying rulebase name as it can be printed once.

**Example**

The following command displays summary statistics for DNS learnt IP addresses:

```
show active-charging dns-learnt-ip-addresses statistics summary
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show active-charging edr-format

Displays information about Event Data Record (EDR) formats configured in the Active Charging Service (ACS).

Product
ACS

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show active-charging edr-format [ statistics ] [ all | name edr_format_name ] [ | { grep grep_options | more } ]

- **all**
  Displays information for all EDR formats.

- **statistics**
  Displays statistics for all or an existing EDR format.
  If neither `all` nor `name` is specified, summarized statistics over all EDR formats is displayed.

- **name edr_format_name**
  Displays information for an existing EDR format specified as an alphanumeric string of 1 through 63 characters.

  | { grep grep_options | more } |
  Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.
  For details on the usage of `grep` and `more`, refer to the `Regulating a Command’s Output` section of the `Command Line Interface Overview` chapter.

Usage

Use this command to display information for EDR format(s) in the ACS.

Example

The following command displays all configured EDR formats in the ACS.

```
show active-charging edr-format all
```

**Important:** Output descriptions for commands are available in the `Statistics and Counters Reference`. 
show active-charging edr-udr-file

Displays CDR flow control information. This command also displays the Event Data Record (EDR) and Usage Data Record (UDR) file information.

Product
ACS

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show active-charging edr-udr-file { flow-control-counters [ verbose ] | statistics } [ | { grep grep_options | more } ]

flow-control-counters [ verbose ]
Displays the counters for dropped EDR/UDR records. These counters are for when CDRMOD uses flow control to stop ACS/Session Managers from sending the records.
verbose displays detailed information.

statistics

Important: This keyword is obsolete. The option is now supported through the show cdr command.

Displays EDR and UDR file statistics.

| { grep grep_options | more }

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage
Use this command to view CDR flow control information.

Example
The following command displays EDR and UDR files statistics:

show active-charging edr-udr-file statistics

The following command displays CDR flow control information:

show active-charging edr-udr-file flow-control-counters
Important: Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show active-charging file-space-usage

Displays the file space used by Charging Data Record (CDR) and Event Data Record (EDR) files.

Product
ACS

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:
[local]host_name#

Syntax

show active-charging file-space-usage [ | { grep grep_options | more } ]

| { grep grep_options | more }

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.

For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage

Use this command to view CDR/EDR file space usage information. The context in which this command is used is not relevant.
show active-charging firewall statistics

Displays Active Charging Stateful Firewall statistics.

Product
PSF

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show active-charging firewall statistics [ callid call_id | domain-name domain_name | nat-realm nat_realm_name | protocol { icmp | icmpv6 | ip | ipv6 | other | tcp | udp } | username user_name ] [ acsmgr instance instance_number ] [ verbose ] [ wide ] [ | { grep grep_options | more } ]

acsmgr instance instance_number

Specifies the ACS/Session Manager instance ID as an integer from 1 through 65535.

callid call_id

Specifies the call identification number as an 8-digit hexadecimal number.

domain-name domain_name

Specifies the domain name as an alphanumeric string of 1 through 127 characters.

nat-realm nat_realm_name

Specifies the NAT realm name as an alphanumeric string of 1 through 31 characters.

protocol { icmp | ip | other | tcp | udp }

Specifies the protocol:

- icmp: ICMPv4
- icmpv6
- ip: IPv4
- ipv6
- tcp
- udp
show active-charging firewall statistics

username user_name
Specifications the user name as an alphanumeric string of 1 through 127 characters.

verbose
Specifications to display detailed (all available) information. If not specified, concise information is displayed.

wide
Displays all available information in a single wide line.

| { grep grep_options | more }
Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent. For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage
Use this command to view Stateful Firewall statistics. If you are in the local context, statistics for all contexts are displayed. Otherwise, only statistics of your current context are displayed.

Example

The following command displays Stateful Firewall statistics:

show active-charging firewall statistics

**Important:** Output descriptions for commands are available in the Statistics and Counters Reference.
show active-charging firewall track-list

Displays the list of servers being tracked for involvement in any Denial-of-Service (DOS) attacks.

Product
PSF

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

\[\text{show active-charging firewall track-list attacking-servers } [ \ | \ { \text{grep grep_options } | \text{more} \} ] \]

| \{ grep grep_options | more \}

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent. For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage
Use this command to view details of servers being tracked for involvement in any DOS attack.

Example
The following command displays the list of servers being tracked for involvement in any DOS attacks:

\[\text{show active-charging firewall track-list attacking-servers}\]

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show active-charging flow-control-counters

Displays information for dropped EDR and UDR records.

Product
ACS

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show active-charging flow-control-counters [ verbose ] [ | { grep grep_options | more } ]

verbose
Specifies to display detailed (all available) information. If not specified, concise information is displayed.

| { grep grep_options | more }

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.
For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage

Use this command to view EDR-UDR flow control information—for dropped EDR and UDR records.

Example

The following command displays detailed EDR-UDR flow control information:

show active-charging flow-control-counters verbose

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show active-charging flow-mappings

Displays information about all the active flow mappings based on the applied filters.

Product
PSF
NAT

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show active-charging flow-mappings [ all | call-id call_id | [ nat { not-required | required [ nat-realm nat_realm_name ] } | trans,proto { tcp | udp } ] + [ | { grep grep_options | more } ]

all
Displays all the available active-charging flow-mapping information.

call-id call_id
Displays detailed information for a call ID specified as an 8-digit hexadecimal number.

nat { required [ nat-realm string ] not-required }
Displays the active charging flow mappings for which NAT is enabled or disabled.

trans,proto { tcp | udp }
Displays the transport layer.

| { grep grep_options | more }
Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.
For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage
Use this command to view the Active Charging flow-mapping details.

Example
The following command displays the total number of Active Charging flow-mappings:

show active-charging flow-mappings all
The following command displays the flow-mappings for which NAT is enabled and the NAT-realm used is natpool3:

`show active-charging flow-mappings nat required nat-realm natpool3`

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference.*
show active-charging flows

Displays information for active charging flows.

**Product**
ACS

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#  
```

**Syntax**

```
show active-charging flows { all | [ callid call_id ] [ connected-time [ < | > | greater-than | less-than ] seconds ] [ control-connection { ftp | pptp | rtsp | sip | tftp } ] [ flow-id flow_id ] [ full ] [ idle-time [ < | > | greater-than | less-than ] seconds ] [ firewall { not-required | required } ] [ imsi imsi_value ] [ ip-address { server | subscriber } [ < | > | IPv4 | greater-than | less-than ] address ] [ msisdn msisdn_num ] [ nat { not-required | required [ nat-ip nat_ip_address ] [ binding-info ] } ] [ pacing-bitrate [ < | > | = | greater-than | less-than | equal-to ] number ] [ port-number { server | subscriber } [ < | > | IPv4 | greater-than | less-than ] number ] [ rx-bytes [ < | > | greater-than | less-than ] number ] [ rx-packets [ < | > | greater-than | less-than ] number ] [ session-id session_id ] [ summary ] [ trans-PROTO { icmp | tcp | udp } ] [ tx-bytes [ < | > | greater-than | less-than ] number ] [ tx-packets [ < | > | greater-than | less-than ] number ] [ type flow_type ] [ username user_name ] } [ | { grep grep_options | more } ]
```

- **all**
  Displays information for all active charging flows.

- **callid call_id**
  Displays the specific Call Identification Number. `call_id` must be an eight digit hexadecimal number.

- **connected-time [ < | > | greater-than | less-than ] seconds**
  Displays information for flows filtered by connected time period.
  - **< seconds**:
    Displays flows that have been connected less than the specified number of seconds.
  - **> seconds**:
    Displays flows that have been connected more than the specified number of seconds.
  - **greater-than seconds**:
    Displays flows that have been connected more than the specified number of seconds.
  - **less-than seconds**:
    Displays flows that have been connected less than the specified number of seconds.

  **seconds** is an integer from 0 through 4294967295.
Exec Mode show Commands (A-C)

show active-charging flows

control-connection { ftp | pptp | rtsp | sip | tftp }
Displays information for control connection of flows.
- ftp: Displays control connection information for the FTP flow.
- pptp: Displays control connection information for the PPTP flow.
- rtsp: Displays control connection information for the RTSP flow.
- sip: Displays control connection information for the SIP flow.
- tftp: Displays control connection information for the TFTP flow.

firewall { not-required | required }
Displays information for flows filtered by Firewall required or not required setting.
- not-required: Sessions with Firewall processing are not required.
- required: Sessions with Firewall processing are required.

flow-id flow_id
Displays concise information for specified active charging flow ID.

full
Displays all available information for the specified flows.

idle-time [ < | > | greater-than | less-than ] seconds
Displays information for flows filtered by idle time period.
- < seconds: Displays flows that have been idle less than the specified number of seconds.
- > seconds: Displays flows that have been idle more than the specified number of seconds.
- greater-than seconds: Displays flows that have been idle more than the specified number of seconds.
- less-than seconds: Displays flows that have been idle less than the specified number of seconds.
seconds is an integer from 0 through 4294967295.

imsi imsi_value
Displays information for an International Mobile Subscriber Identity (IMSI). imsi_value must be a sequence of digits and/or wild characters.

ip-address [ server | subscriber ] [ < | > | IPv4 | greater-than | less-than ] address
Displays information for flows filtered by IPv4 IP address.
- server: Specifies the IP address for a specific server.
- subscriber: Displays subscriber details for the IP address specified in IPv4 dotted-decimal format.
- < address: Specifies an IPv4 IP address that is less than address.
- > address: Specifies an IPv4 IP address that is greater than address.
- greater-than address: Specifies an IPv4 IP address that is greater than address.
- less-than address: Specifies an IPv4 IP address that is less than address.
address is an IP address expressed in IPv4 dotted-decimal notation.
**msisdn msisdn_num**

Displays information for the mobile user identified by the Mobile Subscriber ISDN Number (MSISDN). *msisdn_num* must be a numeric string of 1 to 15 digits.

**nat { not-required | required [ nat-ip nat_ip_address [ nat-port nat_port ] ] [ binding-info ] }**

**Important:** The *nat* keyword and options are only available in StarOS 8.3 and later releases.

Displays information for flows filtered by Network Address Translation (NAT) required or not required setting.

- **not-required:** Sessions with NAT processing are not required.
- **required:** Sessions with NAT processing are required.
- **nat-ip nat_ip_address:** Sessions using the NAT IP address expressed in IPv4 dotted-decimal notation.
- **nat-port nat_port:** Sessions using the specified NAT IP address and NAT port number specified as an integer from 0 through 65535.
- **binding-info:** Displays the NAT binding information of the NATed flow.

**pacing-bitrate [ < | > | = | greater-than | less-than | equal-to ] number**

Displays information on video flows filtered by a video pacing bit rate specified an integer from 1 to 256000000.

- **< number:** Specifies a number that is less than the specified video pacing bit rate.
- **> number:** Specifies a number that is greater than the specified video pacing bit rate.
- **= number:** Specifies a number that is equal to the specified video pacing bit rate.
- **greater-than number:** Specifies a number that is greater than the specified video pacing bit rate.
- **less-than number:** Specifies a number that is less than the specified video pacing bit rate.
- **equal-to number:** Specifies a number that is equal to the specified video pacing bit rate.

**port-number [ server | subscriber ] [ < | > | IPv4 | greater-than | less-than ] number**

Displays information on flows filtered by port number.

- **server:** Specifies the port-number for a specific server.
- **subscriber:** Specifies subscriber details for this port-number, and must be an integer from 0 through 65535.
- **< number:** Specifies a port number that is less than the specified port-number.
- **> number:** Specifies a port number that is greater than the specified port-number.
- **greater-than number:** Specifies a port number that is greater than the specified port-number.
- **less-than number:** Specifies a port number that is less than the specified port-number.

**rx-bytes [ < | > | greater-than | less-than ] number**

Displays information on flows filtered by the number of bytes received in the flow.

- **< number:** Specifies the number of bytes that is less than the specified rx-bytes.
Exec Mode show Commands (A-C)

**show active-charging flows**

- **number**: Specifies number of bytes that is greater than the specified rx-bytes.
- **greater-than number**: Specifies number of bytes that is greater than the specified rx-bytes.
- **less-than number**: Specifies number of bytes that is less than the specified rx-bytes.

`number` must be an integer from 0 through 18446744073709551615.

**rx-packets [ < | > | greater-than | less-than ] number**
Displays information on flows filtered by the number of packets received in the flow.
- **greater-than number**: Specifies the number of packets that is greater than the specified rx-packets.
- **less-than number**: Specifies the number of packets that is less than the specified rx-packets.

`number` must be an integer from 0 through 18446744073709551615.

**session-id session_id**
Displays detailed information for specific active charging session ID.

**summary**
Displays summary information for defined sessions, based on defined parameters.

**transproto { icmp | tcp | udp }**
Displays information on flows filtered by the transport protocol.
- **icmp**: ICMP protocol type flow
- **tcp**: TCP protocol type flow
- **udp**: User Datagram Protocol (UDP) flows

**tx-bytes [ < | > | greater-than | less-than ] number**
Displays information on flows filtered by the number of bytes received in the flow.
- **< number**: Specifies the number of bytes that is less than the specified tx-bytes.
- **> number**: Specifies number of bytes that is greater than the specified tx-bytes.
- **greater-than number**: Specifies number of bytes that is greater than the specified tx-bytes.
- **less-than number**: Specifies number of bytes that is less than the specified tx-bytes.

`number` must be an integer from 0 through 18446744073709551615.

**tx-packets [ < | > | greater-than | less-than ] number**
Displays information on flows filtered by the number of packets received in the flow.
- **greater-than number**: Specifies the number of packets that is greater than the specified tx-packets.
- **less-than number**: Specifies the number of packets that is less than the specified tx-packets.

`number` must be an integer from 0 through 18446744073709551615.

**type flow_type**
Displays information on flows filtered by flow type of application protocol.
`flow_type` must be one of the following:
- **dns**
- **ftp**
show active-charging flows

• http
• icmp
• icmpv6
• imap
• ip
• ipv6
• mms

• p2p [ application p2p_list [ traffic-type traffic_type ] | protocol-group group_list ]: Peer-to-peer analyzer.

  p2p application p2p_list: P2P protocol type flows include one or more of the following applications:
  • actionvoip
  • actsync
  • adobecconnect
  • aimini
  • amazoncloud
  • antsp2p
  • apple-push
  • apple-store
  • applejuice
  • applemaps
  • ares
  • armagettron
  • avi
  • badoo
  • baidumovie
  • battlefd
  • bbm
  • beatport
  • bitcasa
  • bittorrent
  • bittorrent-sync
  • blackberry-store
  • blackberry
  • blackdialer
  • box
  • callofduty
show active-charging flows

- chikka
- cisco-jabber
- citrix
- clubbox
- clubpenguin
- comodounite
- crossfire
- cyberghost
- ddlink
- didi
- directconnect
- dofus
- dropbox
- ebuddy
- edonkey
- facebook
- facetime

**Important:** The *facetime* protocol is available only in releases 9.0 and 11.0. This protocol is not available in release 10.0.

- fasttrack
- feidian
- ficall
- fiesta
- filetopia
- flash
- flickr
- florensia
- foursquare
- freenet
- friendster
- fring
- funshion
- gadu_gadu
- gamekit
show active-charging flows

**Important:** The gamekit protocol is available only in releases 9.0 and 11.0. This protocol is not available in release 10.0.

*gmail
*gnutella
*goober
*google-music
*google-push
*google
*googleplay
*googleplus
*gotomeeting
*gtalk
*guildwars
*halflife2
*hamachivpn
*hbogo
*heytell
*hike-messenger
*hls
*hotspotvpn
*hulu
*hyves
*iax
*icall
*icecast
*icloud
*idrive
*igo
*iheartradio
*imesh
*imessage
*imgur
*imo
*implus
*instagram
*iplayer
show active-charging flows
• nokia-store
• octoshape
• off
• ogg
• oist
• oovoo
• opendrive
• openft
• openvpn
• operamini
• orb
• oscar
• outlook
• paltalk
• pando
• pandora
• path
• pcanywhere
• pinterest
• plingm
• poco
• popo
• pplive
• ppstream
• ps3
• qq
• qqqgame
• qqlive
• quake
• quicktime
• radio-paradise
• radius
• rdp
• rdt
• regram
• rfactor
• rhapsody
show active-charging flows

- rmstream
- rodi
- rynga
- samsung-store
- scydo
- secondlife
- shoutcast
- silverlight
- siri
- skinny
- skydrive
- skype
- slacker-radio
- slingbox
- smartvoip
- snapchat
- softether
- sopcast
- soribada
- soulseek
- soundcloud
- spdy
- speedtest
- splashfighter
- spotify
- ssdp
- stealthnet
- steam
- stun
- sudaphone
- svtplay
- tagged
- talkatone
- tango
- teamspeak
- teamviewer
- telegram
• thunder
• tor
• truecaller
• truphone
• tumblr
• tunnelvoice
• tvants
• tvuplayer
• twitch
• twitter
• ultrabac
• ultrasurf
• upc-phone
• usenet
• ustream
• uusee
• vchat
• veoh.tv
• viber
• vine
• voipdiscount
• vopium
• vpnx
• voxer
• vtok
• vtun
• warcft3
• waze
• webex
• wechat
• weibo
• whatsapp
• wii
• windows-azure
• windows-store
• winmx
• winny
show active-charging flows

- wmstream
- wofkungfu
- wofwarcraft
- wuala
- xbox
- xdcc
- xing
- yahoo
- yahoomail
- youku
- yourfreetunnel
- youtube
- zattoo

**traffic-type** traffic_type: P2P protocol flows include the following traffic type classifications:

- audio
- file-transfer
- im
- video
- voipout
- unclassified

**important**: The traffic type for a P2P protocol may vary depending on the P2P protocol.

- p2p protocol-group group_list: The following P2P protocol groups are supported:
  - generic
  - anonymous-access
  - business
  - communicator
  - cloud
  - e-store
  - e-mail
  - e-news
  - internet-privacy
  - filesharing
  - gaming
show active-charging flows

- p2p-filesharing
- p2p-anon-filesharing
- remote-control
- social-nw-gaming
- social-nw-generic
- social-nw-videoconf
- standard
- streaming

- pop3
- pptp
- rtcp
- rtp
- rtsp
- secure-http
- sip
- smtp
- tcp
- tftp
- udp
- unknown: Unknown type of protocol type flow not listed here.
- wsp-connection-less
- wsp-connection-oriented

username user_name

Specifies the user name as a sequence of characters and/or wildcard characters ($ and *). user_name must be an alphanumeric string of 1 through 127 characters.

| { grep grep_options | more }

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.
For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage

Use this command to display charging flow type information.

Example

The following command displays a detailed flow information for a session ID of test:

    show active-charging flows session-id test
The following command displays a detailed flow information for a P2P type session:

```
show active-charging flows full type p2p
```

The following command displays a detailed information for a P2P type flow:

```
show active-charging flows type p2p
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show active-charging fw-and-nat policy

Displays Firewall-and-NAT Policy information.

**Important:** This command is only available in StarOS 8.1, and in StarOS 9.0 and later. For more information on this command please contact your local service representative.

**Product**
ACS
PSF
NAT

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name# 
```

**Syntax**

```
show active-charging fw-and-nat policy { { { all | name fw_nat_policy_name } [ service name acs_service_name ] } | { statistics { all | name fw_nat_policy_name } } } [ | { grep grep_options | more } ]
```

- **all**
  Displays information for all Firewall-and-NAT policies configured, optionally all in a specified service.

- **name fw_nat_policy_name**
  Displays detailed information for an existing Firewall-and-NAT policy specified as an alphanumeric string of 1 through 63 characters.

- **service name acs_service_name**
  Displays information for all or the specified Firewall-and-NAT policy in the specified ACS.
  `acs_service_name` must be the name of the active-charging service, and must be an alphanumeric string of 1 through 15 characters.

- **statistics**
  Displays statistics for all or the specified Firewall-and-NAT policy.

  ```
  | { grep grep_options | more } 
  ```
  Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.
  For details on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.
**Usage**

Use this command to view Firewall-and-NAT Policy information.

**Example**

The following command displays detailed information for the Firewall-and-NAT policy named `standard`:

```
show active-charging fw-and-nat policy name standard
```
show active-charging group-of-objects

Displays information for ACS group-of-objects.

Product
ACS

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec
The following prompt is displayed in the Exec mode:

[local] host_name#

Syntax

show active-charging group-of-objects { all | name group_of_objects_name } [ | { grep grep_options | more } ]

all
Displays details of all group-of-objects configured in the system.

name group_of_objects_name
Displays details for the specified group-of-objects.

For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage
Use this command to view information for all/specific group-of-objects.

Example
The following command displays information for a group-of-objects named test.

show active-charging group-of-objects name test

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show active-charging group-of-prefixed-urls

D displays information on group of prefixed URLs configured in an Active Charging Service (ACS).

**Product**
ACS

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
show active-charging group-of-prefixed-urls { all | name prefixed_url_group } [ service name acs_service_name ] [ | { grep grep_options | more } ]
```

| all
| Displays information for all group of prefixed URLs configured in an ACS.

| name prefixed_url_group
| Displays detailed information for the group of prefixed URLs specified as an alphanumeric string of 1 through 63 characters.

| service name acs_service_name
| Displays information for all or the specified group of prefixed URLs in the specified ACS. acs_service_name must be the name of the ACS expressed as alphanumeric string of 1 through 15 characters.

| | { grep grep_options | more } |
| Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter

**Usage**

Use this command to view information on group of prefixed URLs configured in the ACS.

**Example**

The following command displays for the group of prefixed URLs named **test123**:

```
show active-charging group-of-prefixed-urls name test123
```
show active-charging group-of-ruledefs

Displays information for all groups or a specified group of ruledefs configured in the Active Charging Service (ACS).

**Product**
ACS

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

[local]\host_name#

**Syntax**

```
show active-charging group-of-ruledefs { { all | name group_of_ruledefs_name } [ service name acs_service_name ] | statistics name group_of_ruledefs_name } [ | { grep grep_options | more } ]
```

- **all**
  Displays information for all groups of ruledefs configured, optionally all in a specified ACS.

- **name group_of_ruledefs_name**
  Displays detailed information for an existing group of ruledefs specified as an alphanumeric string of 1 through 63 characters.

- **service name acs_service_name**
  Displays information for all groups or the specified group of ruledefs within the ACS. `acs_service_name` must be the name of the ACS, and must be an alphanumeric string of 1 through 15 characters.

- **statistics name group_of_ruledefs_name**
  Displays statistics for an existing group of ruledefs specified as an alphanumeric string of 1 through 63 characters.

  | { grep grep_options | more }

  Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.

  For details on the usage of `grep` and `more`, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter.

**Usage**

Use this command to view information on group of ruledefs configured in a ACS.

**Example**

The following command displays information on all groups of ruledefs configured:
show active-charging group-of-ruledefs all
show active-charging nat statistics

Displays Network Address Translation (NAT) realm statistics.

Product
NAT

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show active-charging nat statistics [ instance instance_number | nat-realm nat_realm_name [ summary ] | unsolicited-pkts-server-list [ instance instance_number ] ] [ | { grep grep_options | more } ]

show active-charging nat statistics

When issued in the local context, this command displays statistics for all NAT realms in all contexts. When issued in a specific context, this command displays statistics for all NAT realms in that context.

show active-charging nat statistics instance instance_number

When issued in the local context, this command displays statistics for the specified ACS/Session Manager instance in all contexts. When issued in a specific context, this command displays statistics for the specified ACS/Session Manager instance in that context.

show active-charging nat statistics nat-realm nat_realm_name

When issued in the local context, this command displays statistics for the specified NAT realm in all contexts. When issued in a specific context, this command displays statistics for the specified NAT realm in that context.

show active-charging nat statistics unsolicited-pkts-server-list instance instance_num

When issued in the local context, this command displays statistics for unsolicited packets in all contexts. When issued in a specific context, this command displays statistics for unsolicited packets that context.

instance instance_number

Displays statistics for the specified ACS/Session Manager instance.

instance_number must be an integer from 1 through 65535.

nat-realm nat_realm_name

Specifies the NAT realm’s / NAT realm group’s name.

nat_realm_name must be an alphanumeric string of 1 through 31 characters.
**summary**

When the `nat_realm_name` specified is a “pool group” and the `summary` option is used, summary statistics of all pools in the pool group are displayed.

When the `nat_realm_name` specified is a pool and the `summary` option is not used, all available statistics for the specified pool are displayed.

When the `nat_realm_name` specified is a “pool group” and the `summary` option is not used, all available statistics of each pool in the specified “pool group” are displayed.

**unsolicited-pkts-server-list**

Displays statistics with the list of servers from where most number of unsolicited packets are received for the specified ACS/Session Manager instance.

```
| { grep grep_options | more }
```

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.

For details on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

**Usage**

Use this command to view NAT realm statistics.

**Example**

The following command when issued in the local context, displays NAT realm statistics for NAT realms named `test135` in all contexts:

```
show active-charging nat statistics nat-realm test135
```
show active-charging packet-filter

Displays information on packet filters configured in an Active Charging Service (ACS).

**Product**
ACS

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
show active-charging packet-filter { all | name packet_filter_name } [ service name
acs_service_name ] [ | { grep grep_options | more } ]
```

- **all**
  Displays information for all packet filters configured, optionally all configured in an ACS.

- **name packet_filter_name**
  Displays detailed information for an existing packet filter specified as an alphanumeric string of 1 through 63 characters.

- **service name acs_service_name**
  Displays information for all filters or the specified packet filter in the specified ACS. *acs_service_name* must be the name of the ACS, and must be an alphanumeric string of 1 through 15 characters.

- **| { grep grep_options | more }**
  Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.
  For details on the usage of **grep** and **more**, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter.

**Usage**

Use this command to view information on packet filters configured in an ACS.

**Example**

The following command displays information for the packet filter *filter12*:

```
show active-charging packet-filter name filter12
```
show active-charging pcp-service

Displays statistics for Port Control Protocol (PCP) service in the Active Charging Service (ACS).

Important: This command is customer specific. For more information contact your Cisco account representative.

Product
- ACS
- NAT
- PSF

Privilege
- Security Administrator, Administrator, Operator, Inspector

Mode
- Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

```
show active-charging pcp-service { all | name pcp_service_name | statistics [ instance instance_number | name pcp_service_name | wide ] } [ ] { grep grep_options | more }
```

- **all**
  - Displays information for all PCP services configured in the service.

- **name pcp_service_name**
  - Displays information for an existing PCP service specified as an alphanumeric string of 1 through 63 characters.

- **statistics [ instance instance_number | name pcp_service_name | wide ]**
  - Displays statistical information for all configured PCP services.
    - **instance instance_number**: Displays statistics for the specified ACS/Session Manager instance.
    - **name pcp_service_name**: Displays statistics for the specified PCP service.
    - **wide**: Displays all available information in a single wide line.

| { grep grep_options | more }

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.

For details on the usage of `grep` and `more`, refer to the `Regulating a Command’s Output` section of the `Command Line Interface Overview` chapter.

Usage

Use this command to view statistics for PCP service in the ACS.
**show active-charging pcp-service statistics**: The output of this command displays statistics for all PCP services in all contexts when issued in the local context. When issued in a specific context, this command displays statistics for all PCP services in that context.

**show active-charging pcp-service instance instance_number**: When issued in the local context, this command displays statistics for the specified ACS/Session Manager instance in all contexts. When issued in a specific context, this command displays statistics for the specified ACS/Session Manager instance in that context.

**show active-charging pcp-service name pcp_service_name**: The output of this command displays the statistics for the specified PCP service.

**Example**

The following command displays PCP service statistics for a PCP service named `pcp1`:

```
show active-charging pcp-service statistics name pcp1
```

**Important**: Output descriptions for commands are available in the *Statistics and Counters Reference.*
show active-charging qos-group-of-ruledefs

Displays information for ACS QoS-group-of-ruledefs.

Product
ACS

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show active-charging qos-group-of-ruledefs { all | name qos_group_of_ruledefs_name } [ | { grep grep_options | more } ]

all
Displays details of all qos-group-of-ruledefs configured in the system.

display qos-group-of-ruledefs name
Displays details for the specified qos-group-of-ruledefs.
qos_group_of_ruledefs_name must be the name of a qos-group-of-ruledefs, and must be an alphanumeric string of 1 through 63 characters.

| { grep grep_options | more }
Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.
For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage
Use this command to view details of all/specific qos-group-of-ruledefs.

Example
The following command displays of a qos-group-of-ruledefs named test.

show active-charging qos-group-of-ruledefs name test

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show active-charging regex

Displays regular expression (regex) related statistics and information.

Product
ACS

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local] host_name#

Syntax

`show active-charging regex { statistics { memory | ruledef } { all | instance instance_number | summary } } | status { all | instance instance_number } } [ | { grep grep_options | more ]`

**statistics { memory | ruledef } { all | instance instance_number | summary }**

Displays regex-related statistics.

- **memory**: Displays regex memory related statistics.
- **ruledef**: Displays regex ruledef related statistics.
- **all**: Displays specified statistics for all Session Manager instances.
- **instance instance_number**: Displays specified statistics for specified Session Manager instance.
  
  `instance_number` must be an integer from 1 through 65535.
- **summary**: Displays summary information for specified parameter.

**status { all | instance instance_number }**

Displays status information of regex engines.

- **all**: Displays status for all regex engines.
- **instance instance_number**: Displays status of regex engine for specified Session Manager instance.
  
  `instance_number` must be an integer from 1 through 65535.

| { grep grep_options | more ]

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.

For details on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage

Use this command to view regular expression (regex) related statistics and status of regex engines.
Example

The following command displays status information of all regex engines:

```
show active-charging regex status all
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference.*
show active-charging rulebase

Displays information for ACS rulebases.

Product
ACS

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show active-charging rulebase { { { all | name rulebase_name } [ service name acs_service_name ] } | statistics [ name rulebase_name ] } [ | { grep grep_options | more } ]

| all |
| Displays details of all rulebases configured in the system.

| name rulebase_name |
| Displays details of an existing rulebase specified as an alphanumeric string of 1 through 63 characters.

| service name acs_service_name |
| Displays details of all or the specified rulebase configured in the specified ACS. `acs_service_name` must be the name of the ACS, and must be an alphanumeric string of 1 through 15 characters.

| statistics |
| Displays statistical information for all or the specified rulebase.

| { grep grep_options | more } |
| Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent. For details on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage
Use this command to view various statistics for a specific charging rulebase.

Example
The following command displays active charging rulebase statistics.

```
show active-charging rulebase statistics
```

The following command displays configurations and statistics for a rulebase named `rulebase_1`.

```
show active-charging rulebase name rulebase_1
```
show active-charging rulebase name rulebase_1

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference.*
**show active-charging ruledef**

Displays information for ACS ruledefs.

**Product**
- ACS
- PSF

**Privilege**
- Security Administrator, Administrator, Operator, Inspector

**Mode**
- Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
show active-charging ruledef { all | charging | firewall | name { ruledef_name | post-processing | routing | statistics [ all { charging | firewall [ wide ] | post-processing | tpo } | name ruledef_name [ wide ] ] | tpo } [ | { grep grep_options | more } ]
```

- **all**
  Displays information for all ruledefs configured in the ACS.

- **charging**
  Displays information for all Charging ruledefs configured in the ACS.

- **firewall**
  Displays information for all Stateful Firewall ruledefs configured in the ACS.

- **name ruledef_name**
  Displays detailed information for an existing ruledef specified as an alphanumeric string of 1 through 63 characters.

- **post-processing**
  Displays information for all post-processing ruledefs configured in the ACS.

- **routing**
  Displays information for all Routing ruledefs configured in the ACS.

- **service service_name**
  This keyword is obsolete.

**Important:** This keyword is only available in StarOS 8.3 and later.

Displays information for all post-processing ruledefs configured in the ACS.
**statistics** [ all { charging | firewall [ wide ] | post-processing | tpo } | name ruledef_name [ wide ] ]

Displays statistical information for all/specified ruledefs configured in the ACS. If none of the optional arguments are supplied, statistics totaled for all ruledefs will be displayed.

- **all**: Displays statistics for all ruledefs of the specified type configured in the ACS.
- **charging**: Displays statistics for all Charging ruledefs configured in the ACS.
- **firewall**: Displays statistics for all Firewall ruledefs configured in the service.
- **post-processing**: Displays statistics for all Post-processing ruledefs configured in the ACS.

**Important**: The **post-processing** keyword is available only in StarOS 8.3 and later releases.

* **tpo**

**Important**: The Traffic Performance Optimization (TPO) in-line service is not supported in this release.

- **name ruledef_name**: Displays statistics for an existing ruledef specified as an alphanumeric string of 1 through 63 characters.
- **wide**: Displays all available information in a single wide line.

| { grep grep_options | more } |

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter.

**Usage**

Use this command to view information for ruledefs configured in the ACS.

**Example**

The following command displays ACS ruledef statistics.

```
show active-charging ruledef statistics
```

**Important**: Output descriptions for commands are available in the *Statistics and Counters Reference*.  

---

Cisco ASR 5x00 Command Line Interface Reference
show active-charging service

Displays detailed information about an Active Charging Service (ACS).

Product
ACS

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec
The following prompt is displayed in the Exec mode:

[local]\host_name#

Syntax

show active-charging service { all | name acs_service_name } [ | { grep grep_options | more } ]

all
Displays information for all configured ACSs.

name acs_service_name
Displays detailed information for the ACS specified as an alphanumeric string of 1 through 15 characters.

| { grep grep_options | more }
Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.
For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage
Use this command to view ACS details.

Example
The following command displays details for the ACS named test1.

    show active-charging service name test1

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show active-charging sessions

Displays statistics for Active Charging Service (ACS) sessions.

Product
ACS

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show active-charging sessions [ full | wide | wfl | summary ] [ filter_keyword + ] + [ all ] [ { grep grep_options | more } ]

- **full [ wide ]**
  Displays all available information for the specified session. Optionally all available information can be displayed in a single wide line.

- **summary**
  Displays active sessions count and packet and bytes statistics.

- **wfl**
  Displays all available information including MSISDN and rulebase in a single wide line.

- **display-dynamic-charging-rules**
  Displays information for the dynamic charging rules configured per session under Gx interface support.

- **dynamic-charging**
  Displays information for dynamic charging sessions.

- **filter_keyword**
  The following keywords are filters that modify or filter the output of the Command Keywords. Not all filters are available for all command keywords. Multiple filter keywords can be entered on a command line. When multiple filter keywords are specified, the output conforms to all of the filter keywords specifications. For example, if you enter the following command:

```
show active-charging sessions full active-charging-service acs_1
```
  Counters for active charging sessions active in ACS `acs_1` with full details is displayed. Information for all other services is not displayed.

- **acsmgr instance instance_number**
  Displays session information for a specific ACS/Session Manager instance.
## Exec Mode show Commands (A-C)

### show active-charging sessions

#### active-charging-service <acs_service_name>
Displays session information for the ACS specified as an alphanumeric string of 1 through 15 characters.

#### all
Displays session information for all active charging sessions.

#### cae-readdressing
Displays the Content Adaptation Engine (CAE) re-addressing session information for active charging sessions.

#### callid
Specifies the call identification number.

#### display-dynamic-charging-rules
Displays dynamic charging rules configured.

#### dynamic-charging
Displays session information for all dynamic charging sessions.

#### firewall { not-required | required }
Displays session information for sessions with Firewall Processing required or not required, as specified.

#### flows {active | idle | total} [ < | = | > | equal-to | greater-than | less-than ] { bytes }
Displays information for all active charging flows filtered by all information, active, or idle sessions.

- `<bytes` or `less-than bytes`: Specifies filtering of flows that is less than the specified number of bytes.
- `> bytes` or `greater-than bytes`: Specifies filtering of flows that is greater than the specified number of bytes.
- `= bytes` or `equal-to bytes`: Specifies filtering of flows that is equal to the specified number of bytes.

  `bytes` must be an integer from 0 through 18446744073709551615.

#### fw-and-nat policy <fw_nat_policy_name>
Displays information for the Firewall-and-NAT Policy specified as an alphanumeric string of 1 through 63 characters.

#### imsi
Specifies the International Mobile Subscriber Identity (IMSI) of the subscriber session.

#### ip-address
Specifies the IP address for the specific charging service.

#### max-flows { < | = | > | equal-to | greater-than | less-than } { bytes }
Displays information for the maximum flows made by the session.

- `<bytes` or `less-than bytes`: Specifies filtering of maximum flows that is less than the specified number of bytes.
show active-charging sessions

- `> bytes or greater-than bytes`: Specifies filtering of maximum flows that is greater than the specified number of bytes.
- `= bytes or equal-to bytes`: Specifies filtering of maximum flows that is equal to the specified number of bytes.

`bytes` must be an integer from 0 through 18446744073709551615.

`msid` displays active charging session information for a specific subscriber’s Mobile Station Identification (MSID) number.

`msisdn msisdn_number` displays active charging session information for a specific subscriber’s Mobile Station Integrated Services Digital Network (MSISDN) number. `msisdn_number` must be an integer with a maximum of 15 digits.

`ipv4` displays active charging session information with IPv4 Firewall enabled/disabled.

`ipv6` displays active charging session information with IPv6 Firewall enabled/disabled.

`nat { not-required | required [ nat-realm nat_realm_name ] } [ ipv4 | ipv6 ]` displays session information for sessions with NAT required or not required, as specified. `nat-realm nat_realm_name` specifies the name of a NAT realm as an alphanumeric string of 1 through 63 characters.

- `ipv4`: Displays active-charging sessions for which NAT44 processing is required.
- `ipv6`: Displays active-charging sessions for which NAT64 processing is required.

`rulebase` displays information for a rulebase that is configured in an active charging session.

`rx-data` displays the bytes received in the session.

`session-id` displays detailed session information for a specific session identification.

`transrating` displays the transrating sessions.

`tx-data` displays the bytes sent in the session.

`type` displays session information for specified DNS application type(s).

* `dns`
show active-charging sessions

*ftp
*h323
*http
*icmp
*icmpv6
*imap
*ip
*ipv6
*mms

*p2p [ application p2p_list [ traffic-type traffic_type ] | protocol-group group_list ]: Displays session information for a P2P application type and P2P protocol group.

p2p application p2p_list: The supported P2P applications are:
- *actionvoip
- *actsync
- *adobeconnect
- *aimini
- *amazoncloud
- *antsp2p
- *apple-push
- *apple-store
- *applejuice
- *applemaps
- *ares
- *armagettron
- *avi
- *badoo
- *baidumovie
- *battlefd
- *bbm
- *beatport
- *bitcasa
- *bittorrent
- *bittorrent-sync
- *blackberry-store
- *blackberry
- *blackdialer
- *box
Exec Mode show Commands (A-C)

- callofduty
- chikka
- cisco-jabber
- citrix
- clubbox
- clubpenguin
- comodounite
- crossfire
- cyberghost
- ddlink
- didi
- directconnect
- dofus
- dropbox
- ebuddy
- edonkey
- facebook
- facetime

**Important:** The facetime protocol is available only in releases 9.0 and 11.0. This protocol is not available in release 10.0.

- fasttrack
- feidian
- ficall
- fiesta
- filetopia
- flash
- flickr
- florensia
- foursquare
- freenet
- friendster
- fring
- funshion
- gadu_gadu
- gamekit
show active-charging sessions

**Important:** The gamekit protocol is available only in releases 9.0 and 11.0. This protocol is not available in release 10.0.

- gmail
- gnutella
- goober
- google-music
- google-push
- google
- googleplay
- googleplus
- gotomeeting
- gtalk
- guildwars
- halflife2
- hamachivpn
- hbogo
- heytell
- hike-messenger
- hls
- hotspotvpn
- hulu
- hyves
- iax
- icall
- icecast
- icloud
- idrive
- igo
- iheartradio
- imesh
- imessage
- imgur
- implus
- imo
- instagram
- iplayer
*iptv
*irc
*isakmp
*iskoot
*itunes
*jabber
*jap
*jumblo
*kakaotalk
*kik-messenger
*kontiki
*kugoo
*kuro
*linkedin
*lync
*magicjack
*manolito
*mapfactor
*mapi
*maplestory
*meebo
*mgcp
*mig33
*mojo
*monkey3
*mozy
*msn
*msrp
*mute
*mypeople
*myspace
*nateontalk
*naverline
*navigon
*netflix
*netmotion
*nimbuzz
show active-charging sessions

- nokia-store
- octoshape
- off
- ogg
- oist
- oovoo
- opendrive
- openft
- openvpn
- operamini
- orb
- oscar
- outlook
- paltalk
- pando
- pandora
- path
- pcanywhere
- pinterest
- plingm
- poco
- popo
- pplive
- ppstream
- ps3
- qq
- qggame
- qqlive
- quake
- quicktime
- radio-paradise
- rdp
- rdt
- regram
- rfactor
- rhapsody
- rmstream
show active-charging sessions

- rodi
- rynga
- samsung-store
- scydo
- secondlife
- shoutcast
- silverlight
- siri
- skinny
- skydrive
- skype
- slacker-radio
- slingbox
- smartvoip
- snapchat
- softether
- sopcast
- soribada
- soulseek
- soundcloud
- spdy
- speedtest
- splashfighter
- spotify
- ssdp
- stealthnet
- steam
- stun
- sudaphone
- svtplay
- tagged
- talkatone
- tango
- teamspeak
- teamviewer
- telegram
- thunder
show active-charging sessions

*tor
*truecaller
*truphone
*tumblr
*tunnelvoice
*tvants
*tvuplayer
*twitch
*twitter
*ultrabac
*ultrasurf
*upc-phone
*usenet
*ustream
*uusee
*vchat
*veohuv
*viber
*vine
*voipdiscount
*vopium
*vpnx
*voxer
*vtok
*vtun
*warcft3
*waze
*webex
*wechat
*weibo
*whatsapp
*wii
*windows-azure
*windows-store
*winmx
*winny
*wmstream
• wofkungfu
• wofwarcraft
• wuala
• xbox
• xdcc
• xing
• yahoo
• yahoomail
• youku
• yourfreetunnel
• youtube
• zattoo

**traffic-type** traffic_type: P2P protocol flows include the following traffic type classifications:

- audio
- file-transfer
- im
- video
- voipout
- unclassified

**Important:** The traffic type for a P2P protocol may vary depending on the P2P protocol.

**p2p protocol-group** group_list: The following P2P protocol groups are supported:

- generic
- anonymous-access
- business
- communicator
- cloud
- e-store
- e-mail
- e-news
- internet-privacy
- filesharing
- gaming
- p2p-filesharing
show active-charging sessions

• p2p-anon-filesharing
• remote-control
• social-nw-gaming
• social-nw-generic
• social-nw-videoconf
• standard
• streaming
  • pop3
  • pptp
  • rtcp
  • rtp
  • rtsp
  • secure-http
  • sip
  • smtp
  • tcp
  • tftp
  • udp
  • unknown
  • wsp-connection-less
  • wsp-connection-oriented

username
Displays session information for a specific user name.

dynamic-charging
Displays all the sessions having received at least one Gx message from Session Manager/IMS Authorization.

| { grep grep_options | more }
Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter.

**Usage**
Use this command to display the configuration information for an active charging session.

**Example**
The following command displays full information of an active charging session.

```
show active-charging sessions full all
```
The following command displays an active charging session summary.

```
show active-charging sessions summary
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show active-charging subscribers

Displays statistics and information on active subscribers.

**Product**
ACS

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
show active-charging subscribers callid call_id charging-updates [ statistics ] [ charging-action [ name charging_action_name ] | qos-group [ name qos_group_of_ruledefs_name ] | session ] [ [ | { grep grep_options | more } ]
```

- `callid call_id`
  Specifies a call identification number.
  `call_id` must be an eight digit HEX number.

- `charging-updates [ statistics ] [ charging-action [ name charging_action_name ] | qos-group [ name qos_group_of_ruledefs_name ] | session ]`
  Displays charging-update statistics for subscriber.
  - `statistics`: Displays statistics related to dynamic updates to charging parameters.
  - `charging-action [ name charging_action_name ]`: Displays charging-updates for activated charging-actions or specified charging action.
    - `charging_action_name` must be the name of a charging action, and must be an alphanumeric string of 1 through 63 characters in length.
  - `qos-group [ name qos_group_of_ruledefs_name ]`: Displays charging-updates for activated QoS groups or the specified QoS-group-of-ruledefs.
    - `qos_group_of_ruledefs_name` must be the name of a QoS-group-of-ruledefs, and must be an alphanumeric string of 1 through 63 characters in length.
  - `session`: Displays charging-updates for the session.

- `| { grep grep_options | more }`
  Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.
  For details on the usage of `grep` and `more`, refer to the `Regulating a Command's Output` section of the `Command Line Interface Overview` chapter.
Usage
Use this command to view subscriber statistics and information on dynamic updates to charging parameters per call ID.

Example
The following command displays all statistics related to dynamic updates to charging parameters for call ID ca50ea54:

```
show active-charging subscribers callid ca50ea54 charging-updates statistics
```

The following command displays information on charging updates for call ID ca50ea54 and ACS charging action named test12:

```
show active-charging subscribers callid ca50ea54 charging-updates charging-action name test12
```

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show active-charging subsystem

Displays service and configuration counters for the ACS.

**Product**
ACS

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

**Syntax**

```
show active-charging subsystem { all | facility acsmgr { all | instance instance_number } [ rulebase name rulebase_name ] | sip } [ | { grep grep_options | more } ]
```

- **all**
  Displays ACS subsystem information.

- **facility acsmgr { all | instance instance_number }**
  Displays logged events for all ACS/Session Managers or for a specific instance. 
  `instance_number` must be an integer from 1 through 65535.

- **rulebase name rulebase_name**
  Displays rulebase statistics for the specified rulebase. 
  `rulebase_name` must be the name of a rulebase, and must be an alphanumeric string of 1 through 63 characters.

- **sip**
  Displays SIP related statistics.

- `| { grep grep_options | more }`
  Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.
  For details on the usage of `grep` and `more`, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter.

**Usage**

Use this command to view ACS/Session Manager information.

**Example**

The following command displays ACS subsystem information:

```
show active-charging subsystem all
```
Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show active-charging tcp-proxy statistics

Displays TCP Proxy statistics.

**Product**
ACS

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

**Syntax**

```
show active-charging tcp-proxy statistics [ all | dynamic-disable | ip-layer | proxy-fac
| rulebase rulebase_name | socket-migration | tcp-layer ] [ verbose ] [ | { grep
grep_options | more } ]
```

- **all**
  Displays all TCP Proxy statistics aggregated over all rulebases, including for both IP and TCP layers.

- **dynamic-disable**
  Displays statistics for dynamic disabling of TCP Proxy.

- **ip-layer**
  Displays TCP Proxy statistics for IP layer.

- **proxy-fac**
  Displays TCP Proxy Flow Admission Control statistics.

- **rulebase rulebase_name**
  Displays TCP Proxy statistics for the rulebase specified as an alphanumeric string of 1 through 63 characters.

- **socket-migration**
  Displays TCP Proxy statistics for socket migration.

- **tcp-layer**
  Displays TCP Proxy statistics for TCP layer.

- **verbose**
  Displays detailed TCP Proxy statistics.
| { grep grep_options | more }

Specifies that the output of this command is to be piped (sent) to the command specified. You must specify a command to which the output will be sent.
For details on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

### Usage

Use this command to view TCP Proxy statistics.

### Example

The following command displays detailed TCP proxy statistics for the rulebase named `test14`:

```
show active-charging tcp-proxy statistics rulebase test14 verbose
```
show active-charging tethering-detection

Displays information/statistics pertaining to Tethering Detection databases.

**Product**
ACS

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

[local] host_name#

**Syntax**

```
show active-charging tethering-detection { database [ os-signature | tac | ua-signature ]+ [ sessmgr { all | instance instance_number } ] [ | { grep grep_options | more } | statistics ]
```

Displays information pertaining to the specified Tethering Detection database(s).
- **os-signature**: Displays Tethering Detection OS (Operating System) database information.
- **tac**: Displays Tethering Detection TAC (Transaction Authorization Code) database information.
- **ua-signature**: Displays Tethering Detection UA (User Agent) database information.
- **+**: Indicates that more than one of the preceding keywords can be entered in a single command.
- **sessmgr { all | instance instance_number }**: Displays SessMgr Tethering Detection database status.
  - **all**: Displays status for all SessMgr instances.
  - **instance instance_number**: Displays status for the SessMgr instance specified as an integer from 1 through 10000.

**statistics**

Displays Tethering Detection related statistics.

```
| { grep grep_options | more }
```

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter.

**Usage**

Use this command to view information/statistics pertaining to Tethering Detection databases.
The following command displays information pertaining to Tethering Detection UA and OS databases:

```
show active-charging tethering-detection database ua-signature os-signature
```

The following command displays information pertaining to all Tethering Detection databases:

```
show active-charging tethering-detection database
```
show active-charging timedef

Displays the details of timeslots configured in specified time definition(s).

**Important:** This command is only available in StarOS 8.1 and in StarOS 9.0 and later.

**Product**
ACS

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
show active-charging timedef { all | name timedef_name } [ service name acs_service_name ] [ | { grep grep_options | more } ]
```

- **all**
  Displays information for all timedefs configured in the service.

- **name timedef_name**
  Displays detailed information for the timedef specified as an alphanumeric string of 1 through 63 characters.

- **service name acs_service_name**
  Displays information for all or a specific timedef configured in the specified ACS. `acs_service_name` must be the name of the active-charging service, and must be an alphanumeric string of 1 through 15 characters.

- | { grep grep_options | more }
  Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.

  For details on the usage of `grep` and `more`, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter.

**Usage**

Use this command to view details of timeslots configured in specified timedef(s) that have been configured for the Time-of-Day Activation/Deactivation of Rules feature.

**Example**

The following command displays timeslot details of all timedefs configured in the ACS:

```
show active-charging timedef all
```
show active-charging tpo policy statistics

The Traffic Performance Optimization (TPO) in-line service is not supported in this release.
show active-charging tpo profile statistics

The Traffic Performance Optimization (TPO) in-line service is not supported in this release.
show active-charging udr-format

Displays information about UDR formats configured in an Active charging Service (ACS).

Product
ACS

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show active-charging udr-format { all | name udr_format_name } [ | { grep grep_options | more } ]

- **all**
  Displays information for all UDR formats.

- **name udr_format_name**
  Displays information for an existing UDR format specified as an alphanumeric string of 1 through 63 characters.

- **| { grep grep_options | more }**
  Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.
  For details on the usage of **grep** and **more**, refer to the Regulating a Command's Output section of the Command Line Interface Overview chapter.

Usage

Use this command to display information for UDR format(s) in an ACS.

Example

The following command displays all configured UDR formats in an ACS.

```bash
show active-charging udr-format all
```

**Important:** Output descriptions for commands are available in the Statistics and Counters Reference.
show active-charging url-blacklisting statistics

Displays URL Blacklisting statistics.

**Product**
CF

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
show active-charging url-blacklisting statistics [ rulebase { all | name rulebase_name } ] [ verbose ] [ | { grep grep_options | more } ]
```

- **rulebase { all | name rulebase_name }**
  Displays URL Blacklisting statistics for all or a specific rulebase.
  - `all`: Displays URL Blacklisting statistics for all configured rulebases.
  - `name rulebase_name`: Displays URL Blacklisting statistics for the rulebase specified as an alphanumeric string of 1 through 63 characters.

- **verbose**
  Displays detailed URL Blacklisting statistics.

- **| { grep grep_options | more }**
  Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.
  For details on the usage of `grep` and `more`, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter.

**Usage**

Use this command to view URL Blacklisting hits and misses statistics.

**Example**

The following command displays cumulative URL Blacklisting statistics:

```
show active-charging url-blacklisting statistics
```

The following command displays URL Blacklisting statistics for the rulebase `rulebase_1`:

```
show active-charging url-blacklisting statistics rulebase rulebase_1
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show active-charging video detailed-statistics

Displays detailed statistics for TCP video flows. The command options enable you to collect statistical data for video per UE device type, per radio access type, and per video container type.

**Product**

MVG

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Mode**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
show active-charging video detailed-statistics [ container { flv | mp4 | others } | rat { cdma | gprs | hspa | lte | others | umts | wlan } | ue { android | ios | laptop | others } ]
```

- **container { flv | mp4 | others }**
  
  Displays detailed statistics for TCP video flows based on the specified container file format.

- **rat { cdma | gprs | hspa | lte | others | umts | wlan }**
  
  Displays detailed statistics for TCP video flows based on the specified radio access type.

- **ue { android | ios | laptop | others }**
  
  Displays detailed statistics for TCP video flows based on the specified UE device type.

**Usage**

Use this command to display detailed statistics about video usage. Use the command options to display detailed statistics based on the UE device type, radio access type, or container file format.

**Example**

The following command displays detailed statistics about video usage based on the UE device type **ios**:

```
show active-charging video detailed-statistics ue ios
```
show active-charging xheader-format

Displays x-header format configurations for an Active Charging Service (ACS).

**Important:** This is a customer-specific command. Please contact your local sales representative for more information.

**Product**
ACS

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
show active-charging xheader-format { all | name xheader_format } [ | { grep grep_options | more } ]
```

- `all`
  Displays information for all x-header formats configured.

- `name xheader_format`
  Displays information for the x-header format specified as an alphanumeric string of 1 through 63 characters.

- `| { grep grep_options | more }`
  Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.
  For details on the usage of `grep` and `more`, refer to the *Regulating a Command’s Output* section of the Command Line Interface Overview chapter.

**Usage**

Use this command to view details of x-header formats configured in an ACS.

**Example**

The following command displays information for the x-header format named `test12`:

```
show active-charging xheader-format test12
```
show administrators

Displays information regarding all CLI users currently connected to the system.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax

```
show administrators [ session id ] [ | { grep grep_options | more } ]
```

**session id**
- Indicates the output is to contain additional information about the CLI user session including the assigned session ID.

```
| { grep grep_options | more }
```
- Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
- For details on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage

This command displays a list of administrative users that have command line interface sessions active.

Example

```
show administrators
show administrators session id
```

**Important:** Output descriptions for commands are available in the Statistics and Counters Reference.
show alarm

Displays alarm information.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local] host_name#

Syntax

show alarm { all | audible | central-office | facility | outstanding [ all | chassis | port slot/port | slot slot ] [ verbose ] | statistics } [ | { grep grep_options | more } ]

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Displays the state of all alarms in one screen.</td>
</tr>
<tr>
<td>audible</td>
<td>Displays the state of the internal audible alarm on the SMC (ASR 5000) or SSC (ASR 5500).</td>
</tr>
<tr>
<td>central-office</td>
<td>Displays the state of the CO Alarm contacts on the SPIO (ASR 5000) or SSC (ASR 5500).</td>
</tr>
<tr>
<td>facility</td>
<td>Displays the state of the facility (audible and CO) alarms.</td>
</tr>
</tbody>
</table>
| outstanding { all | chassis | port slot/port | slot slot ] [ verbose ] | Displays information on currently outstanding alarms.
  • all: Displays all alarm information.
  • chassis: Displays chassis/power/fan alarms.
  • port slot/port: Shows the alarm information for the specified port.
  • slot slot: Shows the alarm information for the card in the specified slot.
  • verbose: Displays more verbose output, including the internal alarm ID |
| statistics | Displays basic statistics on the alarming subsystem, including the current number of outstanding alarms of different severities and a cumulative total of alarms generated. |
show alarm

| { grep grep_options | more }

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent. For details on the usage of `grep` and `more`, refer to the *Regulating a Command Output* section of the *Command Line Interface Overview* chapter.

**Usage**

View alarms to verify system status or to periodically check the general health of the system.

**Important:** This command is not supported on all platforms.

**Example**

The following command displays all alarms that are currently outstanding:

```
show alarm outstanding all
```

The following command displays more detailed information on all alarms that are currently outstanding:

```
show alarm outstanding all verbose
```

The following command displays alarm statistics:

```
show alarm statistics
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference.*
show alcap counters

Displays the Access Link Control Application Part (ALCAP) protocol message counters related to ALCAP protocol sessions associated with a Home-NodeB Gateway (HNB-GW) service instance configured and running on a system.

Product
HNB-GW

Privilege
Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

```plaintext
show alcap counters [ alcap-service alcap_svc_name [ aal2-node aal2_node_name [ aal2-path aal2_path_id ] ] ] [ { grep grep_options | more } ]
```

- **name alcap_svc_name**
  Specifies the name of the ALCAP service for which ALCAP protocol session counters are to be displayed.

- **aal2-node aal2-node**
  Specifies the name of the ATM Adaptation Layer 2 (AAL2) node for which protocol session counters will be filtered.

- **aal2-path aal2_path_id**
  Specifies the identity number of the AAL2 path on a specific ATM Adaptation Layer 2 (AAL2) node for which ALCAP protocol counters will be filtered.

- ```grep grep_options | more ```
  Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
  For details on the usage of the `grep` and `more` commands, refer to the Regulating a Command’s Output section in Command Line Interface Overview chapter.

Usage

This command is used to display the sessions statistics and counters for ALCAP service.

Example

The following command displays the ALCAP protocol session counters for ALCAP service named as `alcap_hnb_svc1`:

```plaintext
show alcap counters alcap-service alcap_hnb_svc1
```

**Important:** Output descriptions for commands are available in the Statistics and Counters Reference.
show alcap-service

Displays the Access Link Control Application Part (ALCAP) session statistics of an ALCAP service associated with a Home-NodeB Gateway (HNB-GW) service instance configured and running on a system.

Product
HNB-GW

Privilege
Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show alcap-service { all | name alcap_svc_name [ aal2-node aal2_node_name [ aal2-path aal2_path_id [ aal2-channel aal2_channel_num ] ] | endpoint aal2_endpoint_name ] } [ | { grep grep_options | more } ]

name alcap_svc_name
Specifies the name of the ALCAP service for which service statistics are to be displayed.

aal2-node aal2-node
Specifies the name of the ATM Adaptation Layer 2 (AAL2) node that will be used to filter the display of the ALCAP service statistics.

aal2-path aal2_path_id
Specifies the identity number of the AAL2 path on a specific ATM Adaptation Layer 2 (AAL2) node that will be used to filter the display of the ALCAP service statistics.

aal2-channel aal2_channel_num
Specifies the AAL2 channel number of the AAL2 path on a specific ATM Adaptation Layer 2 (AAL2) node that will be used to filter the display of the ALCAP service statistics.

endpoint atm_endpoint_name
Specifies the ATM endpoint name that will be used to filter the display of the ALCAP service statistics for a specific ATM endpoint.

Usage
This command is used to clear the sessions statistics and counters for ALCAP service.

Example
The following command displays the service statistics of ALCAP service named as alcap_hnb_svc1:

    show alcap-service name alcap_hnb_svc1
**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show alcap statistics

Displays the session statistics related to Access Link Control Application Part (ALCAP) protocol sessions associated with a Home-NodeB Gateway (HNB-GW) service instance configured and running on a system.

Product

HNB-GW

Privilege

Inspector

Mode

Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show alcap statistics [ alcap-service alcap_svc_name [ aal2-node aal2_node_name [ aal2-path aal2_path_id ] ] ] [ verbose ] [ | { grep grep_options | more } ]

| name alcap_svc_name
| Specifies the name of the ALCAP service for which statistics are to be displayed.

| aal2-node aal2-node
| Specifies the name of the ATM Adaptation Layer 2 (AAL2) node for which ALCAP service related statistics will be displayed.

| aal2-path aal2_path_id
| Specifies the identity number of the AAL2 path on a specific ATM Adaptation Layer 2 (AAL2) node for which ALCAP service statistics counters will be displayed.

| | { grep grep_options | more }
| Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
| For details on the usage of the grep and more commands, refer to the Regulating a Command’s Output section in Command Line Interface Overview chapter of the Command Line Interface Reference.

Usage

This command is used to display the sessions statistics and counters for ALCAP service.

Example

The following command displays the service session statistics counters for ALCAP service named as alcap_hnb_svc1:

show alcap counters alcap-service alcap_hnb_svc1

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show apn

Displays configuration information for either a specific or all configured Access Point Names (APNs).

Product
GGSN
P-GW
SAEGW

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show apn { all | name apn_name } [ | { grep grep_options | more } ]

| all
| Displays information on all APNs configured on the system.
| name apn_name
| Displays information for an APN specified as an alphanumeric string of 1 through 62 characters that is case sensitive.
| | { grep grep_options | more }
| Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of grep and more options, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage
This command is used to verify the configuration of one or all APNs for monitoring or troubleshooting purposes. The output is a concise listing of APN parameter settings.
If this command is executed from within the local context with the all keyword, information for all APNs configured on the system will be displayed.

Example
The following command displays configuration information for all APNs:

show apn all

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show apn counters ip-allocation

Displays cumulative statistics of IP allocation method for calls set up so far, per Access Point Name (APN) basis.

Product
- GGSN
- P-GW
- SAEGW

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec
The following prompt is displayed in the Exec mode:
[local]host_name#

Syntax
show apn counters ip-allocation [ all | name apn_name ] [ | { grep grep_options | more } ]

| all |
| Displays statistics for all APNs. |

| name apn_name |
| Displays statistics for the APN specified as an alphanumeric string of 1 through 63 characters that is case sensitive. |

| { grep grep_options | more } |
| Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent. For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter. |

Usage
This command is used to display the cumulative IP allocation counters on a per APN basis. Output of this command gives the user clear idea of how many sessions in each APN have used a particular type of ip-allocation method.
If this command is issued from within the local context, the statistics displayed will be cumulative for all APNs configured on the system regardless of context. If no APN name is specified and the command is executed from a context with multiple APNs configured, the output will be cumulative for all APNs in the context.

Example
The following command displays statistics for all APN on a system:

    show apn counter ip-allocation all
show apn counters ip-allocation

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show apn statistics

Displays statistics for either a specific Access Point Name (APN) or all configured APNs.

Product
GGSN
P-GW
SAEGW

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show apn statistics [ all | name apn_name ] [ | { grep grep_options | more } ]

| all
| Displays statistics for all APNs.

| name apn_name
| Displays statistics for the APN specified as an alphanumeric string of 1 through 63 characters that is case sensitive.

| { grep grep_options | more }
| Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage

This command is used to view statistics for one or all APNs within a context for monitoring or troubleshooting purposes.

If this command is issued from within the local context, the statistics displayed will be cumulative for all APNs configured on the system regardless of context. If no APN name is specified and the command is executed from a context with multiple APNs configured, the output will be cumulative for all APNs in the context.

Example

The following command displays statistics for an APN named isp2:

     show apn statistics name isp2

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show apn-profile

Displays information for configured Access Point Name (APN) profiles.

Product
- MME
- SGSN

Privilege
Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show apn-profile { all | full { all | name apn_name } | name apn_name } [ | { grep grep_options | more } ]

| Syntax |
|---------|---------------------------------|
| all     | Lists all APN profiles configured on the system. |
| full { all | name apn_name } | full: Displays all information in the APN profile(s). `<all>`: Displays full information for all APN profiles configured on the system. `<name apn_name>`: Displays full information for an APN profile specified as an alphanumeric string of 1 through 64 characters. |
| name apn_name | Displays information for an APN profile specified as an alphanumeric string of 1 through 64 characters. |
| [ | { grep grep_options | more } | Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent. For details on the usage of `grep` and `more`, refer to the `Regulating a Command’s Output` section of the `Command Line Interface Overview` chapter. |

Usage

Use this command to display information for APN profiles configured on the system. APN profiles are configured through the global configuration mode and in the APN profile configuration mode. For more information regarding APN profile commands, refer to the `APN Profile Configuration Mode Commands` chapter.

Example

The following command displays all available information for an APN profile named `apn-prof3`:

show apn-profile full name apn-prof3
show apn-remap-table

Displays information for Access Point Name (APN) remap tables configured on the system.

**Syntax**

```
show apn-remap-table { all | full { all | name remap_table_name } | name remap_table_name } [ | { grep grep_options | more } ]
```

- **all**
  
  Lists all APN remap tables configured on the system.

- **full { all | name remap_table_name }**
  
  - **full**: Displays a full set (all) of available information for the configured APN remap table(s).
  - **all**: Displays the full set of available information for all APN remap tables configured on the system.
  - **name remap_table_name**: Displays the full set of available information for an existing APN remap table specified as an alphanumeric string of 1 through 64 characters.

- **name remap_table_name**
  
  Displays information for an existing APN remap table specified as an alphanumeric string of 1 through 64 characters.

  | { grep grep_options | more }

  Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

  For details on the usage of **grep** and **more**, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter.

**Usage**

Use this command to display information for APN remap tables configured on the system. APN remap tables are configured through the Global Configuration mode and in the APN remap table configuration mode. For more information regarding APN remap table commands, refer to the *APN Remap Table Configuration Mode Commands* chapter.

**Example**

The following command displays all available information for an APN remap table named *remap-table12*:
show apn-remap-table full name remap-table12
show aps

Displays information for configured Automatic Protection Switching (APS) parameters.

Product
SGSN

Privilege
Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show aps { all | card-stats slot_number [ clear ] | info slot_number/port_number | port-stats slot_number/port_number [ clear ] | port-status } [ | { grep grep_options | more } ]

all
Lists APS information for all cards configured with APS.

card-stats slot_number [ clear ]
Displays the APS statistics for the identified card. If the clear keyword is included with the command, the APS statistics for the specified card are cleared (reset to zero).

slot_number is an integer that identifies the chassis slot holding the card.

info slot_number/port_number
Displays APS information for a specific port.

slot_number/port_number: The first number must be an integer that identifies the chassis slot holding the specified card. The slot number must be followed by a slash ‘/’, which must be followed immediately by the port number - an integer from 1 to 4 depending upon the type of card.

port-stats slot_number/port_number [ clear ]
Displays APS statistics for a specific port. If the clear keyword is included with the command then the APS statistics for the specified port are cleared (reset to zero).

slot_number/port_number: The first number must be an integer from 1 to 48 to identify the chassis slot holding the specified card. The slot number must be followed by a slash ‘/’, which must be followed immediately by the port number - an integer from 1 to 4 depending upon the type of card.

port-status slot_number/port_number
Displays APS status information for a specific port.

slot_number/port_number: The first number must be an integer from 1 to 48 to identify the chassis slot holding the specified card. The slot number must be followed by a slash ‘/’, which must be followed immediately by the port number - an integer from 1 to 4 depending upon the type of card.
show aps

| { grep grep_options | more }

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

**Usage**

Use this command to display APS redundancy configuration, APS card and port status, and APS card and port statistics. APS is configured at the card level. For details on configuring APS, refer to the Card Configuration Mode Commands chapter in this reference.

**Important:** APS is only relevant for the CLC2 and OLC2 line cards supporting SONET/SDH.

**Example**

The following command displays all available APS configuration information for a specific port 1 on the line card in slot 27:

```
show aps info 27/1
```
show asngw-service

Displays information about selected Access Service Network Gateway (ASN-GW) calls/services.

Product
ASN-GW

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show asngw-service { all | name service_name | session | statistics } [ bs-status { address ip_address | filter { all | icmp-monitored | no-calls | summary | up } ] [ | { grep grep_options | more } ]

| all |
|Name service_name|
|session|
|statistics|

all
Displays information for all configured ASN-GW services.

database service_name
Displays information only for an existing ASN-GW service in the current context specified as an alphanumeric string of 1 through 63 characters.

session
Displays information about configured ASN-GW sessions. See the show asngw-service session command

statistics
Total of collected information for specific protocol since the last restart or clear command.

bs-status { address ip_address | filter { all | icmp-monitored | no-calls | summary | up } ]
Displays the ASN base station (BS) status based on IP address and various filters.
address ip_address specifies the IP address of ASN base station whose status is requested. ip_address must be entered in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.
filter { all | icmp-monitored | no-calls | summary | up }: Filters the requested BS’s status on the basis of following criteria:
- all: Displays the status of all ASN base stations.
- icmp-monitored: Displays the status of ASN base stations that are monitored through ICMP ping messages.
- no-calls: Displays the status of an ASN base station that has no active calls.
- summary: Displays a summary of the status of requested ASN base stations.
- **up**: Displays the status of ASN base stations that are in active state.

```bash
| { grep grep_options | more }
```

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent. For details on the usage of `grep` and `more`, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter.

### Usage

Use this command to view information for selected configured ASN-GW services.

### Example

The following command displays available information for all active ASN-GW services.

```bash
show asngw-service all
```

**Important**: Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show asngw-service session

Displays statistics for specific Access Service Network Gateway (ASN-GW) sessions.

Product
ASN-GW

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show asngw-service session [ all | anchor-only [ full ] | callid call_id | counters | full | ip-address ipv4_address | msid msid_number | non-anchor-only [ full ] | peer-address ipv4_address | summary | username user_name ] [ [ grep grep_options | more ] ]

all
Displays all related information for all active ASN-GW service sessions.

anchor-only
Displays all available information for all active ASN-GW service sessions on an anchor ASN-GW only.

callid call_id
Displays available information for the call identification number specified as an 8-digit hexadecimal number.

full
Displays all available information for the associated display or filter keyword.

ip-address ipv4_address
Specifies the IP address of the subscriber in IPv4 dotted-decimal notation.

msid msid_number
Displays available information for the specific mobile station identification number (MSID).

non-anchor-only
Displays all available information for all active ASN-GW service sessions on a non-anchor ASN-GW only.

peer-address ipv4_address
Specifies the IP address of an IP peer in dotted-decimal notation.
show asngw-service session

**summary**
Displays summary of available information for associated display or filter keyword (previous keyword).

**username user_name**
Specifies the name of a user within current context as an alphanumeric string of 1 through 127 characters.

```
| { grep grep_options | more }
```
Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of `grep` and `more`, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter.

**Usage**
Use this command to view configuration information for an ASN-GW session.

**Example**
The following command displays all available ASN-GW sessions.

```
show asngw-service session all
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference.*
show asngw-service session counters

Displays statistics for specific Access Service Network Gateway (ASN-GW) sessions.

**Product**
ASN-GW

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Mode**
Exec
The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
show asngw-service session counters [ [ function-type { auth-relay | context-transfer | data-path | handoff | im-operation | ms-state-change | paging | qos } ] | [ anchor-only | callid call_id | ip-address ipv4_address | msid msid_number | non-anchor-only | peer-address ipv4_address | username user_name ] [ r4-only | r6-only | verbose ] ] | [ [ grep grep_options | more ]
```

**anchor-only**
Displays all available information for all active anchor sessions in an ASN-GW service.

**callid call_id**
Displays available information for the call identification number specified as an 8-digit hexadecimal number.

**function-type { auth-relay | context-transfer | data-path | handoff | im-operation | ms-state-change | paging | qos }**
Displays the counters for specific type of functions in an ASN-GW session.

**auth-relay:** Displays information about authentication relay messages.

**context-transfer:** Displays information about context-transfer messages.

**data-path:** Displays information about data-path registration messages.

**handoff:** Displays information about hand-off messages.

**im-operations:** Displays information about idle mode state operation messages.

**ms-state-change:** Displays information about MS state change messages.

**paging:** Displays information about paging messages.

**qos:** Displays information about RR messages.

**ip-address ipv4_address**
Specifies the IP address of the subscriber in IPv4 dotted-decimal notation.

**msid msid_number**
Displays available information for the specific mobile station identification (MSID) number.
**show asngw-service session counters**

---

**non-anchor-only**
Displays all available information for all active non-anchor sessions in an ASN-GW service.

**peer-address ipv4_address**
Specifies the IP address of an IP peer in IPv4 dotted-decimal notation.

**r6-only**
Displays all available counters for R6 interface in an ASN-GW session.

**r4-only**
Displays all available counters for R4 interface in an ASN-GW session.

**username user_name**
Displays available session information for the specific WiMAX user in ASN-GW service session. 
*user_name* is an alphanumeric string of 1 through 127 characters.

**verbose**
Indicates the output should provide as much information as possible. If this option is not specified then the output will be the standard level which is the concise mode.

```
| { grep grep_options | more }
```
Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of *grep* and *more*, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter.

---

**Usage**
Use this command to view the counters of an ASN-GW session.

**Example**
The following command displays the counters for data path type function.

```
show asngw-service session counters function-type data-path
```

---

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference.*
show asngw-service statistics

Displays statistics for all Access Service Network Gateway (ASN-GW) sessions.

Product

ASN-GW

Privilege

Security Administrator, Administrator, Operator, Inspector

Mode

Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show asngw-service statistics [ function-type { auth-relay | context-transfer | data-path
| handoff | im-operations | ms-state-change | paging | qos | capability } ] [ name
service_name | r4-only | r6-only | verbose | peer-address ipv4_address ] [ peer-id id ][
verbose ] [ [ grep grep_options | more ] ]

function-type

Displays information about selected function type on R4 or R6 interface.

function-type { auth-relay | context-transfer | data-path
| handoff | im-operations | ms-state-change | paging | qos | capability } [ r4-only | r6-only ]

Displays the counters for specific type of functions in an ASN-GW session.

auth-relay: Displays information about authentication relay messages.

context-transfer: Displays information about context-transfer messages.

data-path: Displays information about data-path registration messages.

handoff: Displays information about hand-off messages.

im-operations: Displays information about idle mode state operation messages.

ms-state-change: Displays information about MS state change messages.

paging: Displays information about paging messages.

qos: Displays information about RR messages.

capability: Displays the capability negotiation between the ASNGW and the base station.

r4-only: Displays information about selected function on R4 interface.

r6-only: Displays information about selected function on R6 interface.

name service_name

Displays information for an existing service specified as an alphanumeric string of 1 through 63 characters.

r4-only

Displays statistics of R4 interface in ASN-GW services.

r6-only

Displays statistics of R6 interface in ASN-GW services.
**show asngw-service statistics**

**peer-address ipv4_address**

Specifies the IP address of an IP Peer in IPv4 dotted-decimal notation.

**peer-id < id >**

Display the statistics based on the 6-byte BSID or ASNGW ID in addition to the IPv4 address.

**verbose**

Specifies that the output should display all available information. If this option is not specified then the output will be the standard level which is the concise mode.

```
| { grep grep_options | more }
```

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent. For details on the usage of `grep` and `more`, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter.

**Usage**

Use this command to display ASN-GW statistics.

**Example**

The following command displays information about selected MS-State-Change function.

```
show asngw-service statistics function-type ms-state-change
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*. 

---

Cisco ASR 5x00 Command Line Interface Reference

4162
show asnpc-service

Displays information about selected Access Service Network Paging Controller and Location Registry (ASN PC/LR) services.

Product
ASN-GW

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show asnpc-service { all | id | name service_name | session | statistics } [ | { grep grep_options | more }] 

| all |
| Displays information for all configured ASN PC services. |

| paging-group |
| Displays all the configured paging-groups and associated paging nodes, and the offset count. For a specific paging group, enter the paging group id number. |

| name service_name |
| Displays information only for an existing ASN PC service specified as an alphanumeric string of 1 through 63 characters. |

| session |
| Displays information about configured ASN PC sessions. |

| statistics |
| Total of collected information for specific protocol since last restart or clear command. |

| { grep grep_options | more } |
| Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent. For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter. |

Usage
Use this command to view information for selected configured ASN PC services.

Example

Use this command to view information for selected configured ASN PC services.
The following command displays available information for all active ASN PC services.

```
show asnpc-service all
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference.*
show asnpc-service session

Displays statistics for specific Access Service Network Paging Controller (ASN PC) service sessions.

**Product**
ASN-GW

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Mode**
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

**Syntax**

```
show asnpc-service session [ all | callid call_id | counters | full | msid msid_number | peer-address ipv4_address | summary ] [ | { grep grep_options | more } ]
```

- **all**
  Displays all related information for all active ASN PC service sessions.

- **callid call_id**
  Displays available information for the call identification number specified as an 8-digit hexadecimal number.

- **full**
  Displays all available information for the associated display or filter keyword.

- **msid msid_number**
  Displays available information for the specific mobile station identification (MSID) number.

- **peer-address ipv4_address**
  Specifies the IP address of an IP peer in IPv4 dotted-decimal notation.

- **summary**
  Displays summary of available information for associated display or filter keyword (previous keyword).

| { grep grep_options | more } |
|-----------------------------|

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter.

**Usage**
Use this command to view configuration information for an ASN PC session.
Example

The following command displays all available ASN PC session counters in verbose mode.

```bash
show asnpc-service session all
```

The following command displays full ASN PC session counters in verbose mode.

```bash
show asnpc-service session full
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*. 

---
show asnpc-service session counters

Displays session counters for Access Service Network Paging Controller (ASN PC) service sessions.

**Product**
ASN-GW

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
show asngw-service session counters [ all | callid call_id | msid msid_number | peer-address ipv4_address | verbose ] [ | { grep grep_options | more } ]
```

- `all` Displays all available counters for all ASN PC service sessions.
- `callid call_id` Displays available information for the call identification number specified as an 8-digit hexadecimal number.
- `msid msid_number` Displays available information for the specific mobile station identification (MSID) number.
- `peer-address ipv4_address` Specifies the IP address of an IP peer in IPv4 dotted-decimal notation.
- `verbose` Indicates the output should provide as much information as possible. If this option is not specified then the output will be the standard level which is the concise mode.
- `| { grep grep_options | more }` Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent. For details on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

**Usage**

Use this command to view the counters of an ASN PC session.

**Example**

The following command displays the counters for ASN PC service sessions in verbose mode.
show asnpc-service session counters verbose

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference.*
show asnpc-service session counters verbose

Displays session counters for Access Service Network Paging Controller (ASN PC) service sessions in complete detail.

Product
ASN-GW

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show asngw-service session counters verbose [ function-type { context-transfer | im-operations | ms-state-change | paging } ] [ all | callid call_id | msid msid_number | peer-address ipv4_address ] ] [ | { grep grep_options | more } ]

all
Displays all available counters for all ASN PC service sessions in verbose mode.

callid call_id
Displays full information for the call identification number specified as an 8-digit hexadecimal number.

function-type { context-transfer | im-operations | ms-state-change | paging }
Displays the counters for specific type of functions in an ASN-GW session.
context-transfer: Displays information about context-transfer messages.
im-operations: Displays information about idle mode state operation messages.
ms-state-change: Displays information about MS state change messages.
paging: Displays information about paging messages.

msid msid_number
Displays full information for the specific mobile station identification (MSID) number.

peer-address ipv4_address
Specifies the IP address of an IP peer IPv4 dotted-decimal notation.

r4-only
Displays statistics of R4 interface in ASN PC services in verbose mode.

r6-only
Displays statistics of R6 interface in ASN PC services in verbose mode.
show asnpc-service session counters verbose

| { grep grep_options | more }

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage

Use this command to view the counters of an ASN PC session in verbose mode.

Example

The following command displays the counters for data path type function.

```
show asnpc-service session counters verbose
```

**Important:** Output descriptions for commands are available in the Statistics and Counters Reference.
show asnpc-service statistics

Displays statistics for all ASN PC service sessions.

Product
ASN-GW

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show asnpc-service statistics [ name service_name | peer-address ipv4_address | verbose ] [ r4-only | r6-only [ | { grep grep_options | more } ]

name service_name
Specifies an existing service name as an alphanumeric string of 1 through 63 characters.

peer-address ipv4_address
Specifies the IP address of an IP peer in IPv4 dotted-decimal notation.

verbose
Indicates the output should provide as much information as possible. If this option is not specified then the output will be the standard level which is the concise mode.

| { grep grep_options | more }
Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage
Use this command to display ASN PC statistics.

Example
The following command displays information about ASN PC service in verbose mode.

    show asnpc-service statistics verbose

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show asnpc-service statistics verbose

Displays statistics for all Access Service Network Paging Controller (ASN PC) service in verbose mode.

**Product**
ASN-GW

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```shell
show asnpc-service statistics verbose [ function-type { context-transfer | ms-state-change | paging } ] | all | r4-only | r6-only ] [ | { grep grep_options | more }
```

**function-type { context-transfer | ms-state-change | paging }
**

Displays the statistics for specific type of functions in an ASN PC service in verbose mode.

- **context-transfer**: Displays information about context-transfer messages.
- **im-operations**: Displays information about idle mode state operation messages.
- **ms-state-change**: Displays information about MS state change messages.
- **paging**: Displays information about paging messages.

**all**

Displays statistics of all ASN PC services in verbose mode.

**r4-only**

Displays statistics of R4 interface in ASN PC services.

**r6-only**

Displays statistics of R6 interface in ASN PC services.

| { grep grep_options | more }

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of `grep` and `more`, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter.

**Usage**

Use this command to display ASN PC service statistics in verbose mode.

**Example**

The following command displays information about selected MS-State-Change function.
show asnp-service statistics verbose function-type ms-state-change

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*.
show banner

Displays the configured banner message for the current context.

**Product**

All

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Mode**

Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

**Syntax**

```plaintext
show banner { all | charging-service | motd | lawful-intercept | pre-login } [ | { grep grep_options | more } ]
```

- **all**
  - Displays all banners configured for a service in a system including the enhanced charging service (ECS).

- **charging-service**
  - Displays banner message configured for an enhanced charging service in the current context.

- **motd**
  - Display the banner message that is configured for the current context.

- **lawful-intercept**
  - Refer to the *Lawful Intercept Configuration Guide* for a description of this command.

    | { grep grep_options | more }

  Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent. For details on the usage of `grep` and `more`, refer to the Regulating a Command's Output section of the Command Line Interface Overview chapter.

**Usage**

Show the configured banner to verify the message of the day contents for possible change

**Example**

```plaintext
show banner
```
show bcmcs counters

Displays Broadcast and Multicast Service (BCMCS)-specific counters and statistics.

Product
PDSN

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show bcmcs counters { all | callid call_id | flow-id flow_id }

- **all**
  Displays BCMCS-specific counters and statistics for all multicast sessions.

- **callid call_id**
  Displays BCMCS-specific counters and statistics for a specific call ID.

- **flow-id flow_id**
  Displays BCMCS-specific counters and statistics for a specific BCMCS flow, defined by a flow ID.

Usage
Use this command to view BCMCS-specific statistics. You may narrow the results of the command output by specifying a specific call ID or flow ID.

Example

    show bcmcs counters all

**Important:** Output descriptions for commands are available in the Statistics and Counters Reference.
show bcmcs statistics

Displays Broadcast and Multicast Service (BCMCS)-specific statistics for the current PDSN-service.

Product
PDSN

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show bcmcs statistics [ pdsn-service service_name ]

pdsn-service service_name

Defines a specific PDSN service from which to gather BCMCS-specific statistics.

Usage

Shows several sets of BCMCS-specific statistics, and may be configured to show statistics only for a certain PDSN service.

Example

show bcmcs statistics pdsn-service service_name

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show boot

Displays information on the current boot image in use.

**Product**
All

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local] host_name#
```

**Syntax**

```
show boot [ initial-config | { grep grep_options | more } ]
```

- `initial-config`
  Identifies the OS image, configuration file, and boot priority used during the initial start up of the system.

  | { grep grep_options | more }
  Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

  For details on the usage of `grep` and `more`, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter.

**Usage**

Show the boot information in preparing for maintenance activities by verifying current boot data. The boot image in use may not be the same as the boot image stored on the SMC due to upgrades and pending reboots. **show boot initial-config** displays the actual boot image and configuration file loaded during boot. This may or may not be the highest priority image and makes this command useful when comparing the loaded image to the priority list.

**Important:** This command is not supported on all platforms.

**Example**

The following command displays the boot system configuration priority list:

```
show boot
```

The following command displays the initial configuration after a system boot:

```
show boot initial-config
```
show bssap+ statistics

Displays Base Station system Application Part (BSSAP+) protocol statistics for the Gs interface between the SGSN and the Mobile services Switching Centre, Visitor Location Register (MSC/VLR).

Product
SGSN

Privilege
Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show bssap+ statistics [ gs-service gs_svc_name ] [ vlr { isdn-number ISDN_Num| name vlr_name } ] [ verbose ] [ | { grep grep_options | more } ]

| gs-service gs_svc_name
| Specifies the name of a specific Gs service to filter the BSSAP+ information as an alphanumeric string of 1 through 63 characters that is case sensitive.

| vlr { isdn-number ISDN_Num| name vlr_name }
| Identifies a specific VLR (by name or ISDN number) to filter BSSAP+ information.
vlr_name is the configured name of the VLR expressed.
VLR_num is the configured E.164-type ISDN number for the VLR. Enter a numerical string of 1 to 15 digits.

| verbose
| Indicates the output should provide as much information as possible. If this option is not specified then the output will be limited to a concise summary.

| | { grep grep_options | more }
| Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage

Use this command to display the BSSAP+ statistics for the SGSN’s Gs interface(s). Based on how the command is entered, this command displays collected BSSAP+ protocol statistics for the entire SGSN or for a specified Gs interface. Using the keywords of this command, the interface can be identified by defining a specific VLR connected to the SGSN or by identifying the Gs service to which the interface has been configured.

Example
The following command displays all BSSAP+ information for the Gs interface configured for the Gs service named gssvcl.

```
show bssap+ statistics gs-service gssvcl verbose
```

**Important:** Descriptions for show command outputs are available in the *Statistics and Counters Reference*. 
show bssgp statistics

Displays base station subsystem GPRS protocol statistics for traffic between the base station subsystem (BSS) and the SGSN over the Gb interface.

Product
SGSN

Privilege
Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local] host_name#

Syntax

show bssgp statistics [ gprs-service gprs_svc_name | nse nse_id [ bvc bvc_id [ sessmgr | verbose ] ] | [ verbose ] [ | { grep grep_options | more } ] ]

gprs-service gprs_svc_name
Specifies the name of an existing GPRS service for which the BSSGP information will be filtered as an alphanumeric string of 1 through 63 characters that is case-sensitive.

nse nse_ID
Enter this keyword to display the BSSGP statistics for the network service entity (NSE) specified as an integer from 0 through 65535.

bvc bvc_ID
Enter this keyword to display the BSSGP statistics for the BSSGP virtual connection (BVC) specified as an integer from 0 through 6500.

sessmgr instance sessmgr_instance_number
Enter this keyword to display the BSSGP statistics for a session manager instance specified as an integer from 1 through 4294967295.

verbose
Indicates the output should provide as much information as possible. If this option is not specified then the output will be the standard level which is the concise mode.

| { grep grep_options | more }

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.
show bssgp statistics

Usage
Use this command to display the BBSGP statistics for a particular GPRS service or NSEI.

Example
The following command displays BSSGP statistics for the GPRS service named gprs1.

    show bssgp statistics gprs-service gprs1

Important: Descriptions for show command outputs are available in the Statistics and Counters Reference.
show bssgp status

Displays the traffic status through the BSSGP (base station subsystem GPRS protocol) layer between the base station subsystem (BSS) and the SGSN over the Gb interface.

**Product**
SGSN

**Privilege**
Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

**Syntax**

```
show bssgp status { bvc-bucket nsei nse_id bvci bvc_id | bvc-stat nsei nse_id bvci bvc_id } [ | { grep grep_options | more } ]
```

**bvc-bucket nsei nse_id bvci bvc_id**

Displays traffic status for a specific BVC bucket identified by the NSEI (network service entity ID) and BVCI (BSSGP virtual connection ID).

- *nsei* is an integer from 0 through 65535.
- *bvc_id* is an integer from 0 through 65000.

**bvc-stat nsei nse_id bvci bvc_id**

Displays traffic status for a BVC identified by the NSEI (network service entity ID) and BVCI (BSSGP virtual connection ID).

- *nsei* is an integer from 0 through 65535.
- *bvc_id* is an integer from 0 through 65000.

| { grep grep_options | more } |

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of *grep* and *more*, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter.

**Usage**

Use this command to display BVC status of the BBSGP layer for specified NSEI and BVCI.

**Example**

The following command displays BSSGP traffic status for the BVC bucket for NSEI 2556 BVCI 241.

```
show bssgp status bvc-bucket nsei 2556 bvci 241
```

**Important:** Descriptions for show command outputs are available in the *Statistics and Counters Reference*. 
show bulkstats

Displays the information on bulk statistics.

**Product**
All

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
show bulkstats [ [ data ] | [ schemas ] | [ variables [ schema_name ] [ obsolete ] ] ] [ | { grep grep_options | more } ] ]
```

- **data**
  Displays collected bulk statistical data.

- **schema**
  Displays the configuration of the statistics to be collected on a per-schema basis.

**Important:** For information on available schemas, refer to the *Bulk Statistics Configuration Mode Commands* chapter.

```
variables schema_name
```

Displays all valid bulkstat schema statistics, or only the statistics for the specified schema.  

*schema_name* specifies the name of the schemas available on system. The following is the list of available schemas in this release.

- aal2
- alcap
- apn
- asngw
- asnpc
- bcmcs
- card
- closedrp
- common
- context
show bulkstats

- cs-network-ranap
- cs-network-rtp
- cs-network-sccp
- csef
- cscfintf
- dcca
- dcca-group
- diameter-acct
- diameter-auth
- diameter-acct
- dcli-util
- dpca
- ecs
- egtpc
- epdg
- fa
- fng
- gprs
- gtpc
- gtpp
- gtpu
- ha
- hnbgw-access
- hnbgw-network
- hnbgw-hnbap
- hnbgw-hnbap-access-closed
- hnbgw-hnbap-access-hybrid
- hnbgw-hnbap-access-open
- hnbgw-iubc-sabp
- hnbgw-iubc-tcp
- hnbgw-ranap
- hnbgw-ranap-access-closed
- hnbgw-ranap-access-hybrid
- hnbgw-ranap-access-open
• hnbgw-rtp
• hnbgw-rtp-access-closed
• hnbgw-rtp-access-hybrid
• hnbgw-rtp-access-open
• hnbgw-rua
• hnbgw-rua-access-closed
• hnbgw-rua-access-hybrid
• hnbgw-rua-access-open
• hnbgw-sabp
• hnbgw-sabp-access-closed
• hnbgw-sabp-access-hybrid
• hnbgw-sabp-access-open
• hnbgw-sctp
• hsgw
• hss
• icsr
• imsa
• ippool
• ipsg
• lac
• lcs
• lma
• lns
• mag
• map
• mipv6ha
• mme
• mvs
• nat-realm
• p2p
• pcc-af
• pcc-policy
• pcc-service
• pcc-sp-endpt
show bulkstats

- pdg
- pdif
- pgw
- phsgw
- phspc
- port
- ppp
- ps-network-gtpu
- ps-network-ranap
- ps-network-sccp
- radius
- radius-group
- rlf
- rlf-detailed
- rp
- samog
- sccp
- sgs
- sgs-vlr
- sgsn
- sgtp
- sgw
- ss7link
- ss7rd
- system
- vlan-npu
- vpn

**obsolete**

This keyword shows the obsolete (but still available) schema variables. An asterisk (*) is displayed next to schema variables that have been obsoleted.

| { grep grep_options | more }

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For information on usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.
**Usage**

This command is used to display information on bulk statistics supported by the system.

The `variable` keyword can be used to list statistics supported by the system either for all schemas, or for an individual schema.

The `schema` keyword can be used to display the configuration of settings for bulk statistics, including the schema.

The `data` keyword can be used to display bulk statistic data collected up to that point.

**Example**

The following command displays the bulk statistics data:

```
show bulkstats data
```

The following command displays the bulk statistics schema configuration:

```
show bulkstats data schemas
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference.*
**show ca-certificate**

Displays information for Certificate Authority (CA) digital certificates configured on this system.

**Product**
All

**Privilege**
Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
show ca-certificate { all | name name }
```

- **all**
  Displays information about all the configured CA certificates.

- **name name**
  Displays information about an existing configured CA certificate name specified as an alphanumeric string of 1 through 128 characters.

**Usage**

View information for CA certificates configured on this system.

**Example**

The following command displays information for a CA certificate named `cert-1`:

```
show ca-certificate name cert-1
```

**Important:** Output descriptions for some commands are available in the *Statistics and Counters Reference*. 
show ca-crl

Displays information for Certificate Authority (CA) Certificate Revocation List (CRL) configured on this system.

Product
All

Privilege
Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show ca-crl { all | name name }

- **all**
  Displays information about all the configured CA-CRLs.

- **name name**
  Displays information about an existing CA-CRL name specified as an alphanumeric string of 1 through 128 characters.

Usage

View information for CA-CRLs on this system.

Example

The following command displays information for a CA-CRL named crl-5:

```
show ca-crl name crl-5
```

**Important:** Output descriptions for some commands are available in the Statistics and Counters Reference.
show cae-group server

Displays configuration information, including the name of the associated CAE group, for all CAEs or for a specific CAE. The CAE (Content Adaptation Engine) is an optional component of the Mobile Videoscape.

**Product**

MVG

**Privilege**

Security Administrator, Administrator

**Mode**

Exec

The following prompt is displayed in the Exec mode:

[local]\host_name#

**Syntax**

```
show cae-group server { all | name cae_name }
```

- **all**
  
  Shows the configuration information, including the associated CAE group, for all CAEs.

- **name cae_name**
  
  Shows the configuration information for a specific CAE.

**Usage**

Use this command to display configuration information for all CAEs or for a specific CAE. This command can be issued from either the local context or the context in which the associated CAE group is defined.

**Example**

The following command displays configuration information for the CAE named `server_1`:

```
show cae-group server name server_1
```
show call-control-profile

Displays information for call control profiles configured on the system.

Product
- MME
- SGSN

Privilege
- Inspector

Mode
- Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

```
show call-control-profile { all | full { all | name profile_name } | name profile_name } [ | { grep grep_options | more } ]
```

- **all**
  - Lists all call-control profiles configured on the system.

- **full { all | name profile_name }**
  - **full**: Displays a full set (all) of available information in the call-control profile.
  - **all**: Displays a full set of available information for all call-control profiles configured on the system.
  - **name profile_name**: Displays full information for an existing call-control profile specified as an alphanumeric string of 1 through 64 characters.

- **name profile_name**
  - Displays information for an existing call-control profile specified as an alphanumeric string of 1 through 64 characters.

  | { grep grep_options | more } |
  - Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
  - For details on the usage of `grep` and `more`, refer to the `Regulating a Command’s Output` section of the `Command Line Interface Overview` chapter.

Usage

Use this command to display information for call-control profiles configured on the system. Call-control profiles are configured through the global configuration mode and in the call-control profile configuration mode. For more information regarding call-control profile commands, refer to the `Call-Control Profile Configuration Mode Commands` chapter.

Example

The following command displays all available information for a call-control profile named `call-prof2`:
show call-control-profile full name call-prof2
show call-home

Displays information for Smart Call Home settings configured on the system.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show call-home [ alert-group | detail | mail-server status | profile [ all | name profile_name ] | statistics [ | { grep grep_options | more } ] ]

alert-group
Displays information for all alert groups configured on the system. It also indicates if an alert-group has been disabled by the user.

detail
Displays general information and alert-group settings for all configured call-home profiles.

mail-server status
Displays status information for call-home mail servers that are configured on the system.

profile { all | name profile_name }
Displays all available information for all call-home profiles on the system or a specified call-home profile.
all: Displays all available information for all call-home profiles configured on the system.
name profile_name: Displays all available information for an existing call-home profile specified as an alphanumeric string of 1 through 31 characters.

name profile_name
Displays information for a call-home profile specified as an alphanumeric string of 1 through 31 characters.

statistics
Displays statistical information for call-home statistics configured on the system.

| { grep grep_options | more }
Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.
show call-home

Usage

Use this command to display profile and notification policy information associated with the call-home profiles configured on the system. Call-home profiles are configured through the Context Configuration Mode and in the Call-home Configuration Mode. For more information regarding call-home commands, refer to the Call Control Profile Configuration Mode Commands chapter.

Example

The following command displays all available information for a call-home profile named call-home-prof1:

```
show call-home profile name call-home-prof1
```
show camel-service

Displays configuration details for Customized Applications for Mobile networks Enhanced Logic (CAMEL) services configured for this SGSN.

**Product**
SGSN

**Privilege**
Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

[local]host_name$

**Syntax**

```
show camel-service { all | name service_name } [ | grep grep_options | more ]
```

- **all**
  Displays the configuration details for all configured CAMEL services.

- **name**
  Displays the configuration details for an existing CAMEL service specified as an alphanumeric string of 1 through 63 characters.

  ```
  | { grep grep_options | more }
  ```

  Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

  For details on the usage of `grep` and `more`, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter.

**Usage**
View configuration information for CAMEL services.

**Example**

The following command displays the configuration information for a CAMEL service identified as `camel4sgsnTO`:

```
show camel-service name camel4sgsnTO
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*.
show card

Displays various types of information for a card or all cards in the system.

**Product**
All

**Privilege**
Security Administrator, Administrator, Operator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
show card [ diag [ slot# ] | hardware [ slot# ] | info [ slot# ] | mappings | table [ all ] ] [ | { grep grep_options | more } ]
```

- **diag**
  Displays diagnostic results for a specific card or all cards.

- **hardware**
  Displays information about installed hardware.

- **info**
  Displays detailed information for a specific card or all cards

- **mappings**
  Displays mappings between front-installed application cards and rear-installed interface cards.

**Important:** This keyword is only supported on the ASR 5000.

- **table [all]**
  Displays information about each card in tabular output. The all option includes empty slots in the output.

- **slot#**
  Specifies the slot number for a card as an integer from 1 through 48.

- | { grep grep_options | more }

  Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

  For details on the usage of **grep** and **more**, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter.
Usage

Use this command to view various types of information for all cards or a specified card.

Example

The following command displays diagnostic information for the card in slot 1:

```
show card diag 1
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference.*
show cbs counters

This command displays the counters for CBS service.

Product
HNBGW

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec
The following prompt is displayed in the Exec mode:
[local]host_name#

Syntax
show cbs counters [ cbs-service cbs_service_name ] [ | { grep grep_options | more } ]

cbs-service cbs_service_name
Displays information for specific CBS service. cbs_service_name is a string of size 1 through 63.

| { grep grep_options | more }
Pipes (sends) the output of this command to the specified command. You must specify a command to which
the output of this command will be sent.
Refer to Regulating a Command’s Output section of the Command Line Interface Overview chapter for
details on the usage of grep and more.

Usage
Use this command to display the counters for CBS service

Example
The following command displays the counters for CBS with cbs-service as my_service:

show cbs counters cbc-service my_service
show cbs sessions

This command displays the information for CBS sessions.

Product
HNBGW

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show cbs sessions [ all ] [ cbc-address cbc_address | cbs-service cbs_service_name ] [ [ full | summary ] [ cbc-address cbc_address | cbs-service cbs_service_name ] ] [ | { grep grep_options | more } ]

all
Displays all CBS sessions.

cbc-address cbc_address
Designates address of CBC. This must be followed by cbc_address, IPv4 address, using dotted-decimal notation.

cbs-service cbs_service_name
Displays information for specific CBS service. cbs_service_name is a string of size 1 through 63.

full
Displays all available information for associated display or filter keyword (previous keyword).

summary
Displays summary information for CBS sessions

| { grep grep_options | more }

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent. Refer to Regulating a Command’s Output section of the Command Line Interface Overview chapter for details on the usage of grep and more.

Usage
Use this command to display the information for CBS sessions.

Example
The following command displays the full sessions for CBS with cbc-address as 101.102.109.211: 
show cbs sessions full  cbc-address 101.102.109.211
show cbs statistics

This command displays the statistics for CB service.

**Product**
HNBGW

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
show cbs statistics [ cbc-address cbc_address | cbs-service cbs_service_name ] [ sabp-only | tcp-only | verbose ] [ | { grep grep_options | more } ]
```

### `cbc-address cbc_address`
Designates address of CBC. This must be followed by `cbc_address`, IPv4 address, using dotted-decimal notation.

### `cbs-service cbs_service_name`
Displays information for specific CBS service. `cbs_service_name` is a string of size 1 through 63.

### `sabp-only`
Displays SABP statistics for selected CBS Service.

### `tcp-only`
Displays TCP statistics for selected CBS Service.

### `verbose`
Displays CBS statistics with more detailed statistics breakup.

| { grep grep_options | more } |
Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent. Refer to [Regulating a Command’s Output](#) section of the [Command Line Interface Overview](#) chapter for details on the usage of `grep` and `more`.

**Usage**

Use this command to display the statistics for CB service.

**Example**

The following command displays the SABP statistics for CBS with `cbc-address` as 101.102.109.211:
show cbs statistics cbc-address 101.102.109.211 sabp-only
show cbs-service

This command displays the information for all / specific CBS service.

Product
HNBGW

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show cbs-service { all | name cbs_service_name } [ status ] [ | { grep grep_options | more } ]

- all
  Displays all CBS services.

- name cbs_service_name
  Displays information for specific CBS service name. cbs_service_name is a string of size 1 through 63.

- status
  Display detailed status.

  | { grep grep_options | more }

  Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
  Refer to Regulating a Command’s Output section of the Command Line Interface Overview chapter for details on the usage of grep and more.

Usage

Use this command to display the information for all / specific CBS service.

Example

The following command displays the detailed status of a CBS service with name my_service:

show cbs-service name my_service status
show cdr

Displays files space used by the Event Data Record (EDR) and Usage Data Record (UDR) and their file information.

Product
ACS

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec
The following prompt is displayed in the Exec mode:
[local]host_name#

Syntax

```
show cdr { file-space-usage | statistics } [ | { grep grep_options | more } ]
```

- **file-space-usage**
  Displays the file space used by Charging Data Record (CDR) and Event Data Record (EDR) files.

- **statistics**
  Displays EDR and UDR file statistics.

  | { grep grep_options | more }

  Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
  For details on the usage of **grep** and **more**, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter.

Usage
Use this command to view CDR flow control information.

Example
The following command displays EDR and UDR files statistics:

```
show cdr statistics
```

The following command displays the file space used by the EDR and UDR files:

```
show cdr file-space-usage
```

**Important:** Output descriptions for commands are available in the Statistics and Counters Reference.
show certificate

Displays information of certificates configured on this system.

Product
All

Privilege
Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show certificate { all | name name }

all
Displays information about all the configured certificates on this system.

name name
Displays information of a specified certificate configured.
name must be the name of an existing certificate, and must be an alphanumeric string of 1 through 128 characters.

Usage

View information for local node certificates on this system.

Example

The following command displays information for a node certificate named certificate-3:

show certificate name certificate-3

Important: Output descriptions for some commands are available in the Statistics and Counters Reference.
show cgw-service

Displays configuration and/or statistical information for CGW services on this system.

Product
SaMOG

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

show cgw-service { all | name name | statistics { all [ verbose ] [ | { grep grep_options | more } ] | name name} } [ | { grep grep_options | more } ]

- all
  Displays all CGW services.

- name name
  Displays information for specific CGW service name.
  name is a string of size 1 to 63.

- statistics
  Displays Node level Statistics for CGW.

- verbose
  Specifies Detailed statistics.

  | { grep grep_options | more }

  Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
  For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage
Use this command to displays configuration and/or statistical information for CGW services on this system.

Example

```
show cgw-service all
```
show cli

Displays current command line interface (CLI) users and associated session information.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

```
show cli { configuration-monitor | history | session } [ | { grep grep_options | more } ]
```

configuration-monitor
Displays information related to the cli configuration-monitor command, including the number of seconds remaining until the next configuration monitor check is performed.

history
Displays CLI command history for this CLI session.

session
Displays information about the current CLI session.

| { grep grep_options | more }

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage
Show current command line interface sessions when there is some unexpected output from a chassis and a check of current CLI users may reveal other activities in progress.

Example

```
show cli
```
**show clock**

Displays the current system data and time.

**Product**
All

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Mode**
Exec
The following prompt is displayed in the Exec mode:

```
[local]host_name# 
```

**Syntax**

```
show clock [ universal ] [ | { grep grep_options | more } ]
```

- **universal**
  Displays the date and time in universal coordinated time (UTC/GMT) format.

- `| { grep grep_options | more }`
  Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
  For details on the usage of `grep` and `more`, refer to the *Regulating a Command Output* section of the *Command Line Interface Overview* chapter.

**Usage**

Check the current time of a chassis to compare with network wide time or for logging purposes if network accounting and/or event records appear to have inconsistent timestamps.

---

**Important:** This command is not supported on all platforms.

**Example**

The following displays the system time in local time and UTC, respectively.

```
show clock

show clock universal
```
show cmp history

Displays historical information for the last 100 Certificate Management Protocol v2 transactions.

Product

All products supporting IPSec CMPv2 features

Important: This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

Privilege

Security Administrator

Mode

Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show cmp history

Usage

Display historical information for the last 100 Certificate Management Protocol v2 transactions.

Example

The following command displays CMPv2 transaction history:

    show cmp history
show cmp outstanding-req


Product
All products supporting IPSec CMPv2 features

Important: This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

Privilege
Security Administrator

Mode
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show cmp outstanding-req

Usage

Example
The following command displays outstanding CMPv2 requests:

show cmp outstanding-req
show cmp statistics


Product
All products supporting IPSec CMPv2 features

**Important:** This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

Privilege
Security Administrator

Mode
Exec

The following prompt is displayed in the Exec mode:

```
[local]\host_name#
```

Syntax

```
show cmp statistics
```

Usage

Example

The following command displays CMPv2 statistics:

```
show cmp statistics
```
show configuration

Displays current configuration information for various subcomponents of the system.

**Product**

All

**Privilege**

Security Administrator, Administrator, Operator

**Mode**

Exec

The following prompt is displayed in the Exec mode:

```
[local] host_name#
```

**Syntax**

```
show configuration [ apn apn_name | card card_num | checksum | context name | obsolete-encryption | port slot/port | rohc | showsecrets | srp | url url | verbose ] [ { grep grep_options | more } ]

show configuration apn apn_name [ obsolete-encryption | showsecrets | verbose ]

show configuration card card_num [ obsolete-encryption | showsecrets | verbose ]

show configuration checksum [ obsolete-encryption | showsecrets | verbose ]

show configuration context name [ obsolete-encryption | radius | showsecrets | verbose ]

show configuration obsolete-encryption

show configuration port slot/port [ obsolete-encryption | showsecrets | verbose ]

show configuration rohc [ all | profile-name name ] [ verbose ]

show configuration showsecrets [ obsolete-encryption ]

show configuration srp [ checksum [ obsolete-encryption ] | showsecrets [ obsolete-encryption ] | verbose ]

show configuration url url

show configuration verbose [ obsolete-encryption | showsecrets [ obsolete-encryption ] ]
```

---

**apn apn_name**

Specifies an APN to display the configuration information for the requested APN. All contexts are searched for this APN, and if a match found, the system returns configuration of this APN.

---

**card card_num**

Specifies a card for which configuration information is to be displayed as an integer from 1 through 48 for the ASR 5000 or 1 through 20 for the ASR 5500.
**checksum**
Generates and displays a checksum value for the configuration data.

**context** name
Specifies an existing context for which configuration information is to be displayed as an alphanumeric string of 1 through 79 characters.

**obsolete-encryption**
Shows encrypted values using a weaker, obsolete encryption method (prior to release 12.2).

**port** slot/port
Displays configuration information for a port identified by its slot and port numbers.

**rohc** [ all | profile-name** name**
Specifies that information for all robust header compression (RoHC) profiles or the named profile is to be displayed.

**showsecrets**
Displays encrypted and unencrypted secret keys saved in the configuration. If this keyword is not specified, secret keys are not displayed.

**Important:** The `showsecrets` keyword is restricted to Administrator privilege or higher.

**srp**
Shows the Service Redundancy Protocol (SRP) configuration used for Interchassis Session Recovery (ICSR) deployments.

**url** url
Default: configuration which is currently in use.
This keyword is not available to users with Operator level permissions. Specifies the location of the configuration data to use for information display. The `url` may refer to a local or a remote file and must be entered in the following format:
For the ASR 5000:

```plaintext
[ file: ]{ /flash | /pcmcia | /hd }[ /directory ]/file_name
tftp://[ host[ :port# ] ]{ /directory ]/file_name
```

For the ASR 5500:

```plaintext
[ file: ]{ /flash | /usb1 | /hd }[ /directory ]/file_name
tftp://[ host[ :port# ] ]{ /directory ]/file_name
```
show configuration

| { http: | ftp: | sftp: }@ [ username[ :password ]@ ] { host }[ :port# ]{ directory }/file_name

**Important:** Do not use the following characters when entering a string for the field names below: “/” (forward slash), “:” (colon) or “@” (at sign).

directory is the directory name.
filename is the actual file of interest.

**Important:** Configuration files should be named with a .cfg extension.

username is the user to be authenticated.
password is the password to use for authentication.
host is the IP address or host name of the server.
port# is the logical port number that the communication protocol is to use.

| { grep grep_options | more } |
|___|___|
Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of **grep** and **more**, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter.

**Usage**
View the current configuration to analyze recent changes. For additional information, refer to the Administration Guides for products installed on your ASR 5x00 system.

**Example**
The following command displays the local in-use port configuration information for port 24/1 in verbose mode.

```
show configuration port 24/1 verbose
```

The following command displays the local in-use port configuration information for port 5/11 in verbose mode.

```
show configuration port 5/11 verbose
```

The following command displays the card configuration for card 17 on host remoteABC stored in the configuration file in /pub/config.cfg.

```
show configuration card 17
```

The following command displays the card configuration for card 5 on host remoteABC stored in the configuration file in /pub/config.cfg.

```
show configuration card 5
```
The following command displays the configuration of all RADIUS server groups configured in context `local`.

```
show configuration context local radius group all
```

The following command shows the configuration for a context named PDIF.

```
show configuration context pdif
```

The following command shows the configuration for a context named PGW.

```
show configuration context pgw
```
show configuration errors

Displays current configuration errors and warning information for the target configuration file as specified for a service.

Product
All

Privilege
Security Administrator, Administrator, Operator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local] host_name#

Syntax

```
show configuration errors [ section section_name ] [ verbose ] [ | { grep grep_options | more } ]
```

```
section {section_name}
```

Specifies the services and section for which to display and validate a configuration.

The following services and sections are supported:

- **aaa-config**: Displays configuration errors/warnings for the AAA service(s) configured on the system.
- **active-charging**: Displays configuration errors/warnings for the Enhanced Charging Service(s) and the Personal Stateful Firewall service(s) configured on the system.
- **alcap-service**: Displays configuration errors/warnings for Access Link Control Application Part (ALCAP) on HNB-GW for IuCS-over-ATM support towards CS core network.
- **apn**: Displays configuration errors/warnings for the APN configuration(s) on the system.
- **apn-profile**: Displays configuration errors/warnings for the APN Profile configuration(s) on the system.
- **apn-remap-table**: Displays configuration errors/warnings for the APN Remap Table configuration(s) on the system.
- **asngw-service**: Displays configuration errors/warnings for the Access Service Network Gateway (ASN-GW) Service configured in a specific context for which configuration errors/warnings is to be displayed.
- **asnpc-service**: Displays configuration errors/warnings for the ASN Paging Controller and Location Registry (ASN PC-LR) Service(s) configured on the system.
- **call-control-profile**: Displays configuration errors/warnings for the Call Control Profile configuration(s) on the system.
- **camel-service**: Displays configuration errors/warnings for the Customised Applications for Mobile networks Enhanced Logic (CAMEL) Service configuration(s) on the system.
- **cs-network**: Displays configuration errors/warnings for the circuit switched (CS) network configuration(s) on the system.
show configuration errors

- **cscf-service**: Displays configuration errors/warnings for the Call Session Control Function (CSCF) service(s) configured on the system.
- **diameter**: Displays configuration errors/warnings for the Diameter configuration(s) on the system.
- **dns-client**: Displays configuration errors/warnings for the DNS client configuration(s) on the system.
- **egtp-service**: Displays configuration errors/warnings for the evolved GPRS Tunneling Protocol (eGTP) service configuration(s) on the system.
- **event-notif**: Displays configuration errors/warnings for the event notification (SNMP) interface client.
- **fa-service**: Displays configuration errors/warnings for the Foreign Agent (FA) service(s) configured on the system.
- **fng-service**: Displays configuration errors/warnings for the Femto Network Gateway (FNG) configuration(s) on the system.
- **ggsn-service**: Displays configuration errors/warnings for the Gateway GPRS Support Node (GGSN) service(s) configured on the system.
- **gprs-service**: Displays configuration errors/warnings for the General Packet Radio Service (GPRS) service(s) configured on the system.
- **gs-service**: Displays configuration errors/warnings for the Gs service(s) configured on the system. The Gs interface between the SGSN and the MSC (VLR) uses the BSSAP+ protocol.
- **ha-service**: Displays configuration errors/warnings for the Home Agent (HA) service(s) configured on the system.
- **henbgw-network-service**: Displays configuration errors/warnings for the Home Evolved Node B Gateway (HNB-GW) network service configuration(s) on the system.
- **hnbgw-service**: Displays configuration errors/warnings for the Home Evolved Node B Gateway (HNB-GW) Service configuration(s) on the system.
- **hsgw-service**: Displays configuration errors/warnings for the HRPD Serving Gateway (HSGW) service(s) configured on the system.
- **imei-profile**: Displays configuration errors/warnings for the International Mobile Equipment Identity (IMEI) Profile configuration(s) on the system.
- **imsa-config**: Displays configuration errors/warnings for the IMS Authorization (IMSA) configuration(s) on the system.
- **imssh-service**: Displays configuration errors/warnings for the IMS Sh (IMSSh) service(s) configured on the system.
- **imsue-service**: Displays configuration errors/warnings for the IMS UE service(s) configured on the system.
- **ipms**: Displays configuration errors/warnings for the Intelligent Packet Monitoring System (IPMS) service(s) configured on the system.
- **ipne**: Displays configuration errors/warnings for the IP Network Enabler (IPNE) facility configured on the system.
- **ipsg-service**: Displays configuration errors/warnings for the IP Security Gateway (IPSG) service(s) configured on the system.
• **iups-service**: Displays configuration errors/warnings for the IuPS service(s) configured on the system.

• **lac-service**: Displays configuration errors/warnings for the Layer 2 Tunneling Protocol (L2TP) Access Concentrator (LAC) service(s) configured on the system.

• **lns-service**: Displays configuration errors/warnings for the L2TP Network Server (LNS) service(s) configured on the system.

• **local-policy**: Displays configuration errors/warnings for the Local Policy configuration(s) on the system.

• **map-service**: Displays configuration errors/warnings for the SS7 Mobile Application Part (MAP) service(s) configured on the system.

• **mme-service**: Specifies the configuration errors for a Mobility Management Entity (MME) service configured in a specific context for which configuration errors/warnings are to be displayed.

• **operator-policy**: Displays configuration errors/warnings for the Operator Policy configuration(s) on the system.

• **pcc-policy-service**: Displays configuration errors/warnings for the Policy and Charging Control (PCC) Policy Service configuration(s) on the system.

• **pcc-service**: Displays configuration errors/warnings for the PCC Service configuration(s) on the system.

• **pdg-service**: Displays configuration errors/warnings for the Packet Data Gateway (PDG) Service configuration(s) on the system.

• **pdif-service**: Displays configuration errors/warnings for the Packet Data Interworking Function (PDIF) service(s) configured on the system.

• **pdsn-service**: Displays configuration errors/warnings for the Packet Data Serving Node (PDSN) service(s) configured on the system.

• **pgw-service**: Displays configuration errors/warnings for the PDN-Gateway (P-GW) service configuration(s) on the system.

• **phsgw-service**: Displays configuration errors/warnings for the Payload Header Suppression (PHS) Gateway service(s) configured on the system.

• **policy-grp-config**: Displays configuration errors/warnings for the Policy Group configuration(s) on the system.

• **ps-network**: Displays configuration errors/warnings for the packet switched (PS) network configuration(s) on the system.

• **saegw-service**: Displays configuration errors/warnings for the System Architecture Evolution Gateway (SAE-GW) Service configuration(s) on the system.

• **sccp-network**: Displays configuration errors/warnings for the Signaling Connection Control Part (SCCP) network configuration(s) on the system.

• **sgs-service**: Displays configuration errors/warnings for the SGs Service configuration(s) on the system. The SGs interface connects the databases in the VLR and the MME.

• **sgsn-mode**: Displays configuration errors/warnings for the Serving GPRS Support Node (SGSN) mode configuration(s) on the system.

• **sgsn-service**: Displays configuration errors/warnings for the SGSN service(s) configured on the system.
• `sgtp-service`: Displays configuration errors/warnings for the SGSN GPRS Tunneling Protocol (SGTP) service(s) configured on the system.

• `sgw-service`: Displays configuration errors/warnings for the Serving Gateway (S-GW) service configuration(s) on the system.

• `subscriber-config`: Displays configuration errors/warnings for the subscriber configuration(s) on the system.

• `subscriber-map`: Displays configuration errors/warnings for the Subscriber Map configuration(s) on the system.

**verbose**

Indicates the output should provide as much information as possible. If this option is not specified then the output will be the standard level which is the concise mode.

```
| { grep grep_options | more }
```

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For more information on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

### Usage

Use this command to view the current configuration errors and warning to review recent changes. For additional information, refer to the Administration Guides for products installed on your ASR 5x00 system.

The following command displays configuration errors and warnings for all services configured in a context/system:

```
show configuration errors verbose | more
```

The following command displays configuration errors and warnings for Active Charging service and Personal Stateful Firewall service configured in a context:

```
show configuration errors section active-charging verbose
```

The following command displays configuration errors and warnings for QoS-configuration in a context:

```
show configuration errors section qos-marking verbose
```

---

**Example**

The following command displays configuration errors and warnings for all services configured in a context:

```
show configuration errors verbose | more
```

The following command displays configuration errors and warnings for Active Charging service and Personal Stateful Firewall service configured in a context:

```
show configuration errors section active-charging verbose
```

The following command displays configuration errors and warnings for QoS-configuration in a context:

```
show configuration errors section qos-marking verbose
```
show congestion-control

Displays information pertaining to congestion control functionality on the system

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show congestion-control { configuration | statistics { manager [ all | instance task_instance ] } [ | { grep grep_options | more } ]

show congestion-control statistics mme { critical | full | major | minor } [ | { grep grep_options | more } ]

configuration
Displays congestion control configuration information including threshold parameters and policy settings for the configured services.

statistics
Displays congestion control statistics for manager services.

manager
Specifies the name of the service/session manager for which statistics are displayed. The following types of manager services are supported:

• allmgr: Specifies that statistics are displayed for PDSN services.
• asngwmgmgr: Specifies that statistics are displayed for ASN-GW services.
• asnpcmcmgr: Specifies that statistics are displayed for ASN PC-LR services.
• bindmux: Specifies that statistics are displayed for Bindmux Manager used by PCC service.
• egtpinmgmgr: Specifies that statistics are displayed for EGTP ingress demuxmgr.
• gtpcmcmgr: Specifies that statistics are displayed for GGSN services.
• hamgr: Specifies that statistics are displayed for HA services.
• hnbmgmgr: Specifies that statistics are displayed for HNB Manager used by HNB-GW service.
• imsimgr: Specifies that statistics are displayed for IMSI managers.
• ipsecmgmgr: Specifies that statistics are displayed for IPSec managers.
• ipsgmgmgr: Specifies that statistics are displayed for IPSG managers.
• **l2tpmgr**: Specifies that statistics are displayed for L2TP managers.

```
statistics mme { critical | full | major | minor }
```

Displays the statistics based on the current state of all instances of the specified task.

- **critical**: Specifies that statistics are displayed for the critical congestion policy for MME services.
- **full**: Specifies that statistics are displayed for all congestion policies for MME services.
- **major**: Specifies that statistics are displayed for the major congestion policy for MME services.
- **minor**: Specifies that statistics are displayed for the minor congestion policy for MME services.

```
all
```

Displays the statistics based on the current state of all instances of the specified task.

```
instance task_instance
```

Displays statistics for a specified software task instance. `task_instance` can be configured to an integer from 1 to 128.

> **Important:** The `inst` column of the `show task table` command output displays the instance of a particular task.

```
| { grep grep_options | more }
```

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of `grep` and `more`, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter.

**Usage**

This command displays congestion control configuration information or statistics for a particular service type. When the all keyword is used, the system compares the current state of all instances of the specified task. The state is based on whether or not any congestion control thresholds have been exceeded. If one or more instances are experiencing congestion, the state is displayed as “Applied”, and the various thresholds that have been crossed are indicated.

**Example**

The following command displays congestion control statistics for a PDSN service using an `allmgr` task with an instance of 2:

```
show congestion-control statistics allmgr instance 2
```

The following command displays congestion control statistics for an ASN-GW service using an `asngwmgr` task with an instance of 2:

```
show congestion-control statistics asngwmgr instance 2
```

The following command displays congestion control statistics for an ASN PC-LR service using an `asnpcmgr` task with an instance of 2:

```
show congestion-control statistics asnpcmgr instance 2
```
**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*.
**show connectedapps**

Displays information about the current Connected Apps (CA) configuration.

**Product**
SecGW (WSG)

**Privilege**
Security Administrator, Administrator

**Mode**
Exec
The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
show connectedapps
```

**Usage**
Displays information about the current Connected Apps (CA) configuration between the CA client on the ASR 9000 VSM and IOS-XR.

**Example**
This command displays Connected Apps configuration information:

```
show connected apps
```
show content-filtering category database

Displays details of the specified category based content filtering database for content filtering application configured in a system/service.

**Product**

CF

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Mode**

Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

**Syntax**

```
show content-filtering category database [ active | all | facility srdbmgr { all | instance instance_number } ] [ url url_string ] [ verbose ] [ | { grep grep_options | more } ]
```

- **active**
  Displays the information about all active databases, for example databases in memory. This is the default setting for category database information.

- **all**
  Displays the information about all active databases, for example, databases in memory and all saved databases on a system.

- **facility**
  Displays logged events for a specific facility.

- **srdbmgr { all | instance instance_number }**
  Displays logged events for all static rating database managers or for all or for a specific instance.
  - **all**: Displays the logged events for all Static Rating Database (SRDB) Manager instances.
  - **instance instance_number**: Displays events logged for a specific SRDB Manager instance specified as an integer from 1 through 8.

- **url url_string**
  Displays the information of the database located at the URL that specifies the name/location of the category database from which to retrieve information as an alphanumeric string of 1 through 512 characters.

- **verbose**
  This option enables the detailed mode for additional information display for specific database.
show content-filtering category database

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.
For details on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage

Use this command to display information of database for category based content filtering application in a service.

Example

The following command displays a detailed information for all active databases in memory.

```
show content-filtering category database active all
```

The following command displays the CF database status of all running SRDB managers.

```
show content-filtering category database facility srdbmgr all
```

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show content-filtering category policy-id

Displays Content Filtering category policy definitions.

Product
CF

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show content-filtering category policy-id { all | id cf_policy_id } [ | { grep grep_options | more } ]

all
Displays definitions of all Content Filtering category policies.

id cf_policy_id
Displays definitions of an existing Content Filtering category policy ID specified as an integer from 1 through 4294967295.

| { grep grep_options | more }
Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.
For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage
Use this command to view Content-Filtering Category definitions for a specific/all Policy IDs.

Example
The following command displays Content Filtering category definitions for policy ID 3:

    show content-filtering category policy-id id 3

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show content-filtering category statistics

Displays statistics for the category-based Content Filtering application configured in a system/service.

Product

CF

Privilege

Security Administrator, Administrator, Operator, Inspector

Mode

Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show content-filtering category statistics [ facility srdbmgr { all | instance instance_number } ] [ | { grep grep_options | more } ]

- **facility**: Displays logged events for a specific facility.

- **srdbmgr { all | instance instance_number }**: Displays logged events for all Static Rating Database (SRDB) Manager instances or for the specified instance.
  - **all**: Displays events logged for all SRDB Manager instances.
  - **instance instance_number**: Displays events logged for the SRDB Manager instance specified as an integer from 1 through 8.

- **| { grep grep_options | more }**
  Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.
  For details on the usage of **grep** and **more**, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage

Use this command to view the statistics of Category Based Content Filtering application in a service. This command’s output also indicates capability of the system to perform Content Filtering and Dynamic Content Filtering if configured.

**Important**: Content filtering cannot be performed if less than two PSCs are activated. Dynamic Content Filtering cannot be performed if less than three PSCs are activated.

Example

The following command displays the detailed statistics of configured category based content filtering application:
show content-filtering category statistics

The following command displays the detailed statistics of configured category based content filtering application based on running SRDB Manager instance1.

```
show content-filtering category statistics facility srdbmgr instance instance1
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show content-filtering category url

Displays the information about the categories of the database at the specific URL configured for the category-based content filtering application in a system/service.

Product
CF

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show content-filtering category url url_string [ policy-id cf_policy_id | rulebase rulebase_name ] [ verbose ] [ | { grep grep_options | more } ]

url url_string
Displays the category information of the URL specified as an alphanumeric string of 1 through 512 characters.

policy-id cf_policy_id
Displays the category information of a URL configured with an existing content filtering category policy ID specified as an integer from 0 through 65535.

rulebase rulebase_name
Displays the category information of a URL configured in ACS Configuration Mode for category-based content filtering in specific rulebase.

rulebase_name must be the name of an existing rulebase, and must be an alphanumeric string of 1 through 15 characters.

verbose
Enables the detailed mode for additional information display for a specific database.

| { grep grep_options | more }

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.

For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage

Use this command to display information of a database URL for category based content filtering application in a service.
Example

The following command displays a detailed information for all active databases in memory.

```
show content-filtering category url /cf_server/cf/optcmd.bin verbose
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show content-filtering server-group

Displays information for Content Filtering Server Group (CFSG) configured in the service.

Product
CF

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show content-filtering server-group [ name cfsg_name | statistics ] [ | { grep grep_options | more } ]

name cfsg_name

Displays information for an existing CFSG specified as an alphanumeric string of 1 through 63 characters.

statistics

Displays statistical information for all configured CFSGs.

| { grep grep_options | more } |

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output will be sent.

For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage

Use this command to display information for Content Filtering Server Group configured in a service.

Example

The following command displays a detailed information for all charging actions:

show content-filtering server-group statistics

The following command displays a details of a specific charging action:

show content-filtering server-group name test123

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show context

Displays information for currently configured contexts.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:
[local]host_name#

Syntax

```plaintext
show context [ all | name context_name ] [ | { grep grep_options | more } ]
```

- **all**: Displays information for all currently configured contexts.
- **name context_name**: Displays information for an existing context specified as an alphanumeric string of 1 through 79 characters.

| { grep grep_options | more } |

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter.

Usage

View configured contexts. This may be useful in verifying configuration or troubleshooting the system.

Example

The following command displays information for the configured context named `sampleContext`:

```plaintext
show context name sampleContext
```

The following command displays information for all contexts:

```plaintext
show context all
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*. 

---

Cisco ASR 5x00 Command Line Interface Reference
show cpu

Displays information on system CPUs.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show cpu { info [ card card_num [ cpu cpu_num ] ] [ graphs ] [ verbose ] | table } [ | { grep grep_options | more } ]

- `info [ card card_num [ cpu cpu_num ] ] [ graphs ] [ verbose ]`: Displays information for an entire card or a specific CPU.
  - `card card_num`: Specifies the card for which to display associated information. `card_num` must be a value in the range 1 through 48 on the ASR 5000 or 1 through 20 on the ASR 5500 and must refer to an installed card.
  - `cpu cpu_num`: Optionally selects a specific CPU on the card of interest to display specific information. `cpu_num` must be a value in the range 0 through 3 and must refer to an installed CPU.
- `graphs`: In addition to textual CPU information display CPU utilization information in graphs.
- `verbose`: Output is to display all information available.
- `table`: Display, in tabular format, all cards and CPUs.
- `{ grep grep_options | more }`: Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

Usage

View CPU statistics to aid in diagnosing service problems for the case of overload conditions.

Important: This command is not supported on all platforms.

Example

The following command displays the CPU information in tabular format for all CPUs on all installed cards:

show cpu table
The following command displays CPU information for card 8 in verbose mode:

```
show cpu info card 8 verbose
```

The following command displays information for CPU 0 on card 1:

```
show cpu info card 1 cpu 0
```

**Important**: Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show crash

Displays software crash events records and associated dump files (minicore, NPU or kernel) for all crashes or a specified crash event.

**Product**
All

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
show crash

all | list | number crash_num
```

- **all**: Displays the dump files for all crash event records in the crash log.
- **list**: Displays a list of recent crash event records. This is the contents of the crashlog2 file.
- **number crash_num**: Displays the dump file for an existing crash number. The crash number can be displayed using the **list** keyword.

```
| { grep grep_options | more }
```

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter.

**Usage**

View the crash list to determine frequency of crashes or if crashes occur at some specific time of day. To aid in troubleshooting, this command may also be used to view the dump file for a specific crash.

For additional information refer to the *System Logs* section of the *System Administration Guide*.

**Example**

The following displays the list of crash event records on the active management card.

```
show crash list
```

The following command will display the dump file for crash number 11.

```
show crash number 11
```
show credit-control sessions

Displays credit control sessions information.

Product
PDSN

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

```plaintext
show credit-control session [ all | callid | full | mdn | nai | summary ] [ | { grep grep_options | more } ]
```

 session [ all | callid | full | mdn | nai | summary ]
Displays the credit control session status based on the following keywords:
all: Displays all available information for Credit Control sessions
callid: Displays the Credit Control Session Call ID
full: Displays All available information for the associated display or the filter keyword
mdn: Displays the Credit Control Message Delivery Notification (MDN) information.
nai: Displays the Credit Control NI
summary: Displays the summary of Credit Control session information

| { grep grep_options | more } |
Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
Please refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter for details on the usage of `grep` and `more`.

Usage
Use this command to show active credit control application for service sessions.

Example

The following command shows the configured Credit Control application sessions:

```plaintext
show credit-control sessions
```
show credit-control statistics

Displays credit control statistics.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
show credit-control statistics cc-service name[ | { grep grep_options | more } ]
```

*cc-service*

Specifies the Credit Control Service.

*name* must be the name of a Credit Control Service, and must be an alphanumeric string of 1 through 63 characters.

```
| { grep grep_options | more }
```

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

Please refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter for details on the usage of *grep* and *more*.

**Usage**

Use this command to show active credit control statistics.

**Example**

The following command shows the configured credit control statistics for a service named *service1*:

```
show credit-control statistics cc-service service1
```
show crypto blacklist file

Displays the contents of the blacklist (access denied) file.

**Product**

All products supporting IPSec blacklisting

---

**Important:** This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

**Privilege**

Security Administrator

**Mode**

Exec

The following prompt is displayed in the Exec mode:

```
[local]\host_name#
```

**Syntax**

```
show crypto blacklist file
```

**Usage**

Use this command to display the current contents of the blacklist file.

**Example**

The following command displays the contents of the blacklist file:

```
show crypto blacklist file
```
show crypto group

Displays information pertaining to configured crypto groups.

Product
- ePDG
- FA
- GGSN
- HA
- HeNGBGW
- HNBGW
- HSGW
- MME
- P-GW
- PDSN
- S-GW
- SAEGW
- SCM
- SecGW
- SGSN

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

```
show crypto group [ name group_name | summary ]
```

**name group_name**
Displays information for an existing crypto group specified as an alphanumeric string of 1 through 127 characters.

**summary**
Displays state and statistical information for configured crypto groups in this context.

Usage
Use this command to display information and statistics pertaining to one or all configured crypto groups within the current context.
If the `summary` keyword is not used, detailed information is displayed.

Example

The following command displays detailed information for a crypto group called `group1`:

```
show crypto group name group1
```
show crypto ikev1

Displays pre-shared key information for peer security gateways configured within the context.

Product
- ePDG
- FA
- GGSN
- HA
- HeNBGW
- HNBGW
- HSGW
- MME
- P-GW
- PDSN
- S-GW
- SAEGW
- SCM
- SecGW
- SGSN

Privilege
- Security Administrator, Administrator, Operator, Inspector

Mode
- Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show crypto ikev1 { keys | policy [ preference ] | security-associations [ summary ] }

- **keys**
  Displays the IKE pre-shared key information based on the peer security gateway.

- **policy [ preference ]**
  Displays configuration information for the Internet Exchange Key (IKE) policy priority specified as an integer from 1 through 100. If no preference is specified, information will be displayed for all configured policies.

- **security-associations [ summary ]**
  Displays information for established IPSec security associations (SAs).
Usage
Use this command to:

- Display pre-shared key information. This information can be used to verify configuration and/or for troubleshooting.
- Verify the configuration of IKE policies within the context.
- Display established IPSec SA information. This information can be used for troubleshooting.

Example
The following command lists the pre-shared keys received from peer security gateways as part of the Diffie-Hellman exchange:

```
show crypto ikev1 keys
```

The following command displays information for an IKE policy with a preference of 1:

```
show crypto ikev1 policy 1
```

The following command displays the currently established SAs:

```
show crypto ikev1 security-associations summary
```
show crypto ikev2-ikesa security-associations

Displays a summary view of Internet Key Exchange v2 (IKEv2) IKE Security Associations (IKE SAs).

Product

- ePDG
- FA
- GGSN
- HA
- HeNBGW
- HNBGW
- HSGW
- MME
- P-GW
- PDSN
- S-GW
- SAEGW
- SCM
- SecGW
- SGSN

Privilege

Administrator, Security Administrator

Mode

Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show crypto ikev2-ikesa security-associations peer ipv4/v6_address [ | { grep grep_options | more } ]

show crypto ikev2-ikesa security-associations summary [ cookies ] [ distribution ] [ | { dpd ] [ ipsecmgr instance instance_value ] [ natt [ remote-gw ipv4/v6_address ] [ spi ] [ | { grep grep_options | more } ]]

show crypto ikev2-ikesa security-associations tag crypto_map [ | { grep grep_options | more } ]

peer ipv4/v6_address

Specifies the crypto map peer IP address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.
**summary**

Displays SA summary information only. This information can be one of the following:

- **cookies**: Display IKE cookies for connections.
- **distribution**: Display summary distribution.
- **dpd**: Display DPD (Dead Peer Detection) information for connections.
- **ipsecmgr instance instance_value**: Display ipsecmgr instance information. *instance_value* is an integer from 177 through 352.
- **natt [[ remote-gw ipv4/v6_address ]**: Display NAT-T information for connections or a specified remote gateway.

**tag tag_name**

Specifies a crypto map name as an alphanumeric string of 1 through 127 characters.

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent. Refer to *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter for details on the usage of *grep* and *more*.

**Usage**

Shows the information of the of the SAs configured for a crypto template. It shows the total configured SA lifetime in seconds and the number of seconds left on the timer.

**Example**

Use this command to display the SA summary:

```
show crypto ikev2-ikesa security-associations summary
```

**Important**: Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show crypto ikev2-ikesa transform-set

Displays IKEv2/IKESA (Internet Key Exchange v2/IKE Security Association) transform set configuration information.

**Product**
- ePDG
- FA
- GGSN
- HA
- HeNBGW
- HNBGW
- HSGW
- MME
- P-GW
- PDSN
- S-GW
- SAEGW
- SCM
- SecGW
- SGSN

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
show crypto ikev2-ikesa transform-set transform_set_name [ | { grep grep_options | more }
```

```
show crypto ikev2-ikesa transform-set transform_set_name
```

Specifies the name of an existing IKEv2/IKSA transform set for which to display information as an alphanumeric string of 1 through 127 characters that is case sensitive.

```
|{ grep grep_options | more }
```

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

Refer to *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter for details on the usage of *grep* and *more*.
show crypto ikev2-ikesa transform-set

Usage
Use this command to verify the configuration of IKEv2/IKESA transform sets within the context. If no keyword is specified, information will be displayed for all IKEv2/IKESA transform sets configured within the context.

Example
The following command displays information for an IKEv2/IKESA transform set named *test1*:

```
show crypto ikev2-ikesa transform-set test1
```
show crypto ipsec security-associations

Displays IPSec security associations (SAs) configured within or facilitated by the context and can optionally display statistics for them.

Product
- ePDG
- FA
- GGSN
- HA
- HeNBGW
- HNBGW
- HSGW
- MME
- P-GW
- PDSN
- S-GW
- SAEGW
- SCM
- SecGW
- SGSN

Privilege
- Security Administrator, Administrator, Operator, Inspector

Mode
- Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show crypto ipsec security-associations [ map-type { ikev2-ipv4-cfg | ikev2-ipv4-node | ikev2-ipv6-cfg | ikev2-ipv6-node | ipsec-dynamic | ipsec-ikev1 | ipsec-ikev2-subscriber | ipsec-l2tp | ipsec-manual | ipsec-mobile-ip } | summary [ distribution | ipsecmgr | map-type ] | [ | { grep grep_options | more } ] | [ tag tag_name ] | [ | { grep grep_options | more } ]]

map-type { ikev2-ipv4-cfg | ikev2-ipv4-node | ikev2-ipv6-cfg | ikev2-ipv6-node | ipsec-dynamic | ipsec-ikev1 | ipsec-ikev2-subscriber | ipsec-l2tp | ipsec-manual | ipsec-mobile-ip }

Specifies that information for all crypto maps of a specific type configured within the context will be displayed. The following types can be specified:

*ikev2-ipv4-cfg: IKEv2 IPv4 IPSec configured (ACL) Tunnel
show crypto ipsec security-associations

- **ikev2-ipv4-node**: IKEv2 IPv4 IPSec spawned node Tunnel
- **ikev2-ipv6-cfg**: IKEv2 IPv6 IPSec configured (ACL) Tunnel
- **ikev2-ipv6-node**: IKEv2 IPv6 IPSec spawned node Tunnel
- **ipsec-dynamic**: Dynamic IPSec Tunnel
- **ipsec-ikev1**: IKEv1 IPSec Tunnel
- **ipsec-ikev2-subscriber**: IKEv2 Subscriber Tunnel
- **ipsec-l2tp**: L2TP IPSec Tunnel
- **ipsec-manual**: Manual (Static) IPSec Tunnel
- **ipsec-mobile-ip**: Mobile IP IPSec Tunnel

**summary [ distribution | ipsecmgr | map-type ]**
Displays only security association summary information.

**distribution**: Show IPSec Manager SA distribution information.

**ipsecmgr ipsec_mgr_id**: Displays summary SA information for the IPSec manager instance ID specified as an integer from 1 through 200.

**map-type map_type**: Displays summary SA information for the specified type of crypto map. The following types can be specified:
- **ikev2-ipv4-cfg**: IKEv2 IPv4 IPSec configured (ACL) Tunnel
- **ikev2-ipv4-node**: IKEv2 IPv4 IPSec spawned node Tunnel
- **ikev2-ipv6-cfg**: IKEv2 IPv6 IPSec configured (ACL) Tunnel
- **ikev2-ipv6-node**: IKEv2 IPv6 IPSec spawned node Tunnel
- **ipsec-dynamic**: Dynamic IPSec Tunnel
- **ipsec-ikev1**: IKEv1 IPSec Tunnel
- **ipsec-ikev2-subscriber**: IKEv2 Subscriber Tunnel
- **ipsec-l2tp**: L2TP IPSec Tunnel
- **ipsec-manual**: Manual (Static) IPSec Tunnel
- **ipsec-mobile-ip**: Mobile IP IPSec Tunnel

**tag tag_name**
Displays the SAs for an existing crypto map specified as an alphanumeric string of 1 through 127 characters that is case sensitive.

```bash
| ( grep grep_options | more )
```
Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

Refer to *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter for details on the usage of `grep` and `more`.

**Usage**
Use this command to display IPSec SA information and statistics. This information can be used for performance monitoring and/or troubleshooting.
The displayed information categorizes control signal and data statistics. Data statistics are further categorized according to the encapsulation method, either GRE or IP-in-IP.

Example

The following command displays summary SA statistics for all IPSec managers.

```
show crypto ipsec security-associations summary
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show crypto ipsec transform-set

Displays IPSec transform set configuration information.

**Product**
- ePDG
- FA
- GGSN
- HA
- HeNBGW
- HNBGW
- HSGW
- MME
- P-GW
- PDSN
- S-GW
- SAEGW
- SCM
- SecGW
- SGSN

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]\host_name#
```

**Syntax**

```
show crypto ipsec transform-set [ transform_name ]
```

- `transform_name`
  Displays information for the IPSec transform set specified as an alphanumeric string of 1 through 127 characters that is case sensitive.

**Usage**

Use this command to verify the configuration of IPSec transform sets within the context. If no keyword is specified, information will be displayed for all IPSec transform sets configured within the context.
Important: This command is used in PDIF Release 8.3 only.

Example

The following command displays information for an IPSec transform set named `test1`:

```
show crypto ipsec transform-set test1
```
**show crypto isakmp keys**

Displays pre-shared key information (Internet Security Association and Key Management Protocol, ISAKMP) for peer security gateways configured within the context.

**Product**
- PDSN
- GGSN

**Privilege**
- Security Administrator, Administrator, Operator, Inspector

**Mode**
- Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
show crypto isakmp keys
```

**Usage**

Use this command to display pre-shared key information based on the peer security gateway. This information can be used to verify configuration and/or for troubleshooting.

**Example**

The following command lists the pre-shared keys received from peer security gateways as part of the Diffie-Hellman exchange:

```
show crypto isakmp keys
```

---

*Important:* Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show crypto isakmp policy

Displays Internet Security Association and Key Management Protocol (ISAKMP) policy configuration information.

Product

PDSN
GGSN

Privilege

Security Administrator, Administrator, Operator, Inspector

Mode

Exec

The following prompt is displayed in the Exec mode:

[local]\host_name#

Syntax

show crypto isakmp policy [ preference ]

preference

Displays configuration information for the ISAKMP policy priority specified as an integer from 1 through 100.

Usage

Use this command to verify the configuration of ISAKMP policies within the context. If no preference is specified, information will be displayed for all configured policies.

Example

The following command displays information for an ISAKMP policy with a preference of 1:

    show crypto isakmp policy 1
show crypto isakmp security-associations

Displays currently established Internet key Exchange (IKE) security associations (SAs) facilitated by the context.

Product
PDSN
GGSN

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec
The following prompt is displayed in the Exec mode:

[local] host_name#

Syntax
show crypto isakmp security-associations [ cookies ]

cookies
Specifies that cookies should be displayed.

Usage
Use this command to display established IPSec SA information. This information can be used for troubleshooting.

Example
The following command displays the currently established SAs:

show crypto isakmp security-associations

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show crypto managers

Displays statistics per IPSec Manager.

Product
- ePDG
- FA
- GGSN
- HA
- HeNBGW
- HNBGW
- HSGW
- MME
- P-GW
- PDSN
- S-GW
- SAEGW
- SCM
- SecGW
- SGSN

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show crypto managers [ context context_id | crypto-map map_name | instance instance_num | summary [ distribution | ike-stats | ikev2-stats | ipsec-sa-stats | npu-stats ] | | { grep grep_options | more } ]

context context_id
Displays IPSec manager statistics for an existing context specified as an alphanumeric string of 1 through 80 characters.

crypto-map map_name
Displays IPSec Managers for an existing crypto map specified as an alphanumeric string of 1 through 128 characters.
instance instance_num

Displays statistics for the IPSec manager instance specified as an integer from 1 through 366.

summary [ distribution | ike-stats | ipsec-3gpp-cscf-stats | ikev2-stats | demux-stats | ipsec-sa-stats | npu-stats ]

Shows statistics per service IP address for each manager.

distribution: Displays a summary list of IPSec manager distribution.
ike-stats: Displays a summary list of IPSec IKE statistics for each IPSec manager.
ipsec-3gpp-cscf-stats: Displays CSCF IPSec Statistics on each IPSec Manager.
ikev2-stats: Displays IKEv2 Statistics on each IPSec Manager.
demux-stats: Displays session demux statistics on each IPSec Manager.
ipsec-sa-stats: Displays a summary list of IPSec Security Association (SA) statistics for each IPSec Manager.
npu-stats: Displays NPU statistics on each IPSec Manager.

| { grep grep_options | more }

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
Refer to Regulating a Command’s Output section of the Command Line Interface Overview chapter for details on the usage of grep and more.

Usage

Use this command to view statistics relating to IPSec managers.

Example

The following command displays summary information for all IPSec managers:

```
show crypto managers summary
```

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show crypto map

Displays crypto map configuration information.

Product

- ePDG
- FA
- GGSN
- HA
- HeNNGW
- HNBGW
- HSGW
- MME
- P-GW
- PDSN
- S-GW
- SAEGW
- SCM
- SecGW
- SGSN

Privilege

Security Administrator, Administrator, Operator, Inspector

Mode

Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show crypto map [ map-type [ ikev2-ipv4-cfg | ikev2-ipv4-node | ikev2-ipv6-cfg | ikev2-ipv6-node | ipsec-ikev1 | ipsec-ikev2-subscriber | ipsec-l2tp | ipsec-manual | ipsec-mobile-ip | | { grep grep_options | more } ] | [ summary ] | [ tag tag_name ] | | |{ grep grep_options | more } ]

map-type [ ikev2-ipv4-cfg | ikev2-ipv4-node | ikev2-ipv6-cfg | ikev2-ipv6-node | ipsec-ikev1 | ipsec-l2tp | ipsec-manual | ipsec-mobile-ip | | { grep grep_options | more } ]

Specifies that information for all crypto maps of a specific type configured within the context will be displayed. The following types can be specified:

- *ikev2-ipv4-cfg*: IKEv2 IPv4 IPSec configured (ACL) Tunnel
- *ikev2-ipv4-node*: IKEv2 IPv4 IPSec spawned node Tunnel
- *ikev2-ipv6-cfg*: IKEv2 IPv6 IPSec configured (ACL) Tunnel
show crypto map

- **ikev2-ipv6-node**: IKEv2 IPv6 IPSec spawned node Tunnel
- **ipsec-ikev1**: IKEv1 IPSec Tunnel
- **ipsec-ikev2 Subscriber**: IKEv2 Subscriber Tunnel
- **ipsec-l2tp**: L2TP IPSec Tunnel
- **ipsec-manual**: Manual (Static) IPSec Tunnel
- **ipsec-mobile-ip**: Mobile IP IPSec Tunnel

**summary**
Displays summary information for all crypto maps configured in the context.

**tag map_name**
Specifies the name of an existing crypto map in the current context for which to display configuration information as an alphanumeric string of 1 through 127 characters that is case sensitive.

```bash
| ( grep grep_options | more )
```
Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent. Refer to *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter for details on the usage of `grep` and `more`.

**Usage**
Use this command to verify the configuration of crypto maps within the context. If no keyword is specified, information will be displayed for all maps configured within the context regardless of type.

**Example**
The following command displays configuration information for a dynamic crypto map named `test_map3`:

```bash
show crypto map tag test_map3
```
show crypto statistics

Displays Internet Protocol Security (IPSec) statistics.

Product
ePDG
FA
GGSN
HA
HeNBGW
HNBGW
HSGW
MME
P-GW
PDSN
S-GW
SAEGW
SCM
SecGW
SGSN

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show crypto statistics [ ikev1 | ikev2 [ service-ip-address ip-address ] [ service-name name ] | srtp [ service-ip-address ip-address ] [ service-name name ] | [ | { grep grep_options | more } ]

ikev1
Displays global ikev1 statistics for this context.

ikev2 [ service-ip-address ip-address ] [ service-name name ]
Displays global ikev2 statistics for this context.

service-ip-address ip-address: Specifies the Packet Data Interworking Function (PDIF) service IP address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

service-name name: Specified PDIF service name, a string of size 1 through 63.
**show crypto statistics**

```bash
srtp [ service-ip-address ip-address ] [ service-name name ]
```

Displays global SRTP (Secure Real-time Transport Protocol) statistics for this context.

- `service-ip-address ip-address`: Specifies the CSCF service IP address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.
- `service-name name`: Specifies the CSCF service name, a string of size 1 through 63.

```bash
| { grep grep_options | more }
```

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

Refer to *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter for details on the usage of `grep` and `more`.

### Usage

Use this command to display statistics for IPSec tunnels facilitated by the context. This information can be used for performance monitoring and/or troubleshooting.

### Example

The following command displays cumulative IPSec statistics for the current context:

```bash
show crypto statistics
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show crypto template

Displays information about crypto templates.

Product

ePDG
FA
GGSN
HA
HeNBGW
HNBGW
HSGW
MME
P-GW
PDSN
S-GW
SAEGW
SCM
SecGW
SGSN

Privilege

Security Administrator, Administrator, Operator, Inspector

Mode

Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show crypto template [ map-type [ ikev2-dynamic | ipsec-dynamic ] | summary | tag map_name ] [ | { grep grep_options | more }

map-type [ ikev2-dynamic | ipsec-dynamic ]
Specifies a specific map type.

summary
Displays summary information for all templates.

tag map_name
Specifies a crypto map name as an alphanumeric string of 1 through 127 characters.
show crypto template

| \ `{ grep grep_options \ | more \ } |

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent. Refer to Regulating a Command’s Output section of the Command Line Interface Overview chapter for details on the usage of `grep` and `more`.

Usage

Use this command to display statistics for crypto templates. This information can be used for performance monitoring and/or troubleshooting.

Example

The following command displays summary information for all crypto templates:

```
show crypto template summary
```
show crypto whitelist file

Displays the contents of the whitelist (access granted) file.

**Product**
All products supporting IPSec whitelisting

**Important:** This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

**Privilege**
Security Administrator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
show crypto blacklist file
```

**Usage**
Use this command to display the current contents of the whitelist file.

**Example**
The following command displays the contents of the whitelist file:

```
show crypto whitelist file
```
show cs-network

Displays statistics for the Circuit Switched (CS)-network(s) instance configured on a chassis for HNB-GW service sessions.

**Product**
HNB-GW

**Privilege**
Security Administrator, Administrator, Operator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
show cs-network { all | name cs_name } [ status ] [ | { grep grep_options | more }]
```

- **all**
  Displays status counters for all CS (circuit switched) networks configured for HNB-GW service sessions on a chassis.

- **name cs_name**
  Displays status counters for a CS network configured for HNB-GW service specified as an alphanumeric string of 1 through 127 characters that is case sensitive

  | { grep grep_options | more }

  Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent. Refer to *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter for details on the usage of `grep` and `more`.

**Usage**

Use this command to display the status of any or all CS-network(s) instance configured on a chassis for HNB-GW service sessions.

**Example**

The following command displays the output for CS network instance status named `cs_1_hnb`:

```
show cs-network name cs_1_hnb status
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference.*
show cs-network counters

Displays the session counter information for an HNB-CS Network associated with Home-NodeB Gateway (HNB-GW) services configured and running on a system.

Product
HNB-GW

Privilege
Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show cs-network counters [ name cs_svc_name [ msc msc_point_code ] ] [ | { grep grep_options | more } ]

name cs_svc_name
Filters the counter display based on an existing HNB-CS Network service name associated with an HNB-GW service running on system. cs_svc_name is an alphanumeric string of 1 through 63 characters.

msc msc_point_code
Filters the counter display filtered on the basis of MSC address provided in the SS7 point code that is connected to a particular HNB-CS Network service. msc_point_code must be the address of an MSC in SS7 point code notation.

| { grep grep_options | more }

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of the grep and more commands, refer to the Regulating a Command’s Output section in Command Line Interface Overview chapter.

Usage

Use this command to view the session counter information for HNB-CS Network services configured and MSCs connected on a system.

Example

The following command displays the counters for the HNB-CS Network service named hnb_cs_svc1:

show cs-network counters name hnb_cs_svc1

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show cs-network statistics

Displays the Circuit Switched session statistics for Home-NodeB Gateway (HNB-GW) services configured and running on this system.

Product

HNB-GW

Privilege

Inspector

Mode

Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show cs-network statistics [ name cs_svc_name [ msc msc_point_code]] [ ranap-only | rtp-only | sccp-only ] [ | { grep grep_options | more } ]

name cs_svc_name

Filters the session statistics display based on an existing HNB-CS Network service name that is associated with an HNB-GW service running on this system. cs_svc_name is an alphanumeric string of 1 through 63 characters.

msc msc_point_code

Filters the counter display filtered on the basis of MSC address provided in the SS7 point code that is connected to a particular HNB-CS Network service. msc_point_code must be the address of an MSC in SS7 point code notation.

ranap-only

Filters the session statistics to display only Radio Access Network Application Protocol (RANAP) traffic for an HNB-CS Network service which is configured and associated with an HNB-GW service running on this system.

rtp-only

Filters the session statistics to display only Realtime Streaming Protocol (RTP) and Realtime Streaming Control Protocol (RTCP) traffic for the specified HNB-CS Network service which is configured and associated with an HNB-GW service running on this system.

sccp-only

Filters the session statistics to display only Signaling Connection Control Part (SCCP) traffic for the specified HNB-CS Network service which is configured and associated with an HNB-GW service running on this system.
Exec Mode show Commands (A-C)

show cs-network statistics

| { grep grep_options | more }

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of the `grep` and `more` commands, refer to the Regulating a Command’s Output section in Command Line Interface Overview chapter of the Command Line Interface Reference.

Usage

Use this command to view the session statistics for overall session or in selected part of user session for HNB-GW services configured and running on this system.

Example

The following command displays the session statistics for RTP and RTCP part of session for the HNB-CS Network service named `hnb_cs1`:

```
show cs-network statistics name hnbcs1 rtp-only
```

**Important:** Output descriptions for commands are available in the Statistics and Counters Reference.
show cscf ifc

Displays the Initial Filter Criteria (iFC) for shared iFC functionality.

Product
SCM (S-CSCF, SIP Proxy)

Privilege
Security Administrator, Administrator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

```
show cscf ifc { all | id fc_id } [ | { grep grep_options | more } ]
```

- `all`: Displays all iFC.
- `id fc_id`: Displays information for an existing iFC specified as an alphanumeric string of 1 through 200 characters.

| | { grep grep_options | more } |
|---|---|
| Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent. |
| Refer to *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter for details on the usage of `grep` and `more`. |

Usage

Use this command to display configuration information for any or all iFC on this system.

Example

The following command displays the configuration information for all iFC on this system:

```
show cscf ifc all
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show cscf nat

Displays the Call Session Control Function (CSCF) mapping created for each of the media streams present in an established dialog.

Product
SCM (P-CSCF, A-BG)

Privilege
Security Administrator, Administrator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax
show cscf nat media mapping { all | aor aor } [ | { grep grep_options | more } ]

media mapping { all | aor aor }
    all: Displays the UE/Network origins and destinations, including their IP addresses/port numbers and associated contexts.
    aor aor: Displays information for an Address of Record (AoR) specified as an alphanumeric string of 1 through 79 characters.

| { grep grep_options | more }
    Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
    Refer to Regulating a Command’s Output section of the Command Line Interface Overview chapter for details on the usage of grep and more.

Usage
Use this command to display the status of configured Network Address Translation (NAT) support.

Example
The following command displays the status of the mapping created for each of the media streams present on this system:

    show cscf nat media mapping all

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show cscf npdb-servers

Displays the connection status of NPDB (Number Portability Data Base) servers in S-CSCF service.

Product
SCM (S-CSCF)

Privilege
Security Administrator, Administrator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local] host_name#

Syntax

show cscf npdb-servers service service_name [ | { grep grep_options | more } ]

service service_name

Specifies the name of an existing CSCF service for which the statistics will be displayed as an alphanumeric string of 1 through 63 characters.

| { grep grep_options | more }

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
Refer to Regulating a Command's Output section of the Command Line Interface Overview chapter for details on the usage of grep and more.

Usage
Use this command to display the connection status of NPDB servers in S-CSCF service.

Example
The following command displays the connection status of NPDB servers for the S-CSCF service named scscf1:

    show cscf npdb-servers service scscf1

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show cscf peer-servers

Displays name, IP address, and status of configured Call Session Control Function (CSCF) peer servers visible to the system.

Product
SCM

Privilege
Security Administrator, Administrator, Operator

Mode
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show cscf peer-servers { all | full | name service_name [ server-name server_name ] } [ | { grep grep_options | more } ]

all | full | name service_name [ server-name server_name ]
all: Displays the peer server list names and the servers within those lists including their IP addresses/port numbers and domain names.
full: Displays additional details regarding the peer servers within the configured lists on the system.
name service_name [ server-name server_name ]: Displays the same information as the full keyword output, but for a peer server list or an existing peer server specified as an alphanumeric string of 1 through 80 characters.

| { grep grep_options | more }

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
Refer to Regulating a Command’s Output section of the Command Line Interface Overview chapter for details on the usage of grep and more.

Usage
Use this command to display the status of configured peer servers.

Example
The following command displays the status of a peer server named icscf3 that is a member of peer server list cscf-main:

    show cscf peer-servers name cscf-main server-name icscf3

The following command displays the status of all peer servers in configured peer server groups in this context:

    show cscf peer-servers full
**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference.*
show cscf peer-servers-group

Displays the status of peer-servers-lists inside peer-servers groups.

Product
SCM

Privilege
Security Administrator, Administrator, Operator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show cscf peer-servers-group { all | full | name group_name [ servers-list-name list_name ] } [ | { grep grep_options | more } ]

all | full | name service_name [ server-name server_name ]

all: Displays information for all peer-servers-groups.
full: Displays all available peer servers.
name group_name [ servers-list-name list_name ]: Displays information for peer-server-list (Active/Standby) in the peer-servers-group.
group_name must be an existing peer-servers-group specified as an alphanumeric string of 1 through 80 characters.
[ servers-list-name list_name ] must be an existing peer-server-list specified as an alphanumeric string of 1 through 80 characters.

| { grep grep_options | more } |

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
Refer to Regulating a Command’s Output section of the Command Line Interface Overview chapter for details on the usage of grep and more.

Usage

Use this command to display the status of peer-servers-lists inside peer-servers groups.

Example

The following command displays the status of a peer-server-list named psl3 that is a member of peer-servers-group psg2:

    show cscf peer-servers-group name psg2 servers-list-name psl3

The following command displays the status of all peer-servers-groups in this context:

    show cscf peer-servers-groups all
show cscf service

Displays configuration and/or statistical information for Call Session Control Function (CSCF) services on this system.

Product
SCM

Privilege
Security Administrator, Administrator, Operator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show cscf service { all [ counters ] | diameter { location-info statistics service-name service_name [ vpn-name name ] | policy-control statistics service-name service_name [ vpn-name name ] } | grey-list name name | li-packet-cable statistics service-name service_name | location-info statistics service-name service_name [ vpn-name name ] | policy-control statistics service-name service-name [ vpn-name name ] } | grey-list name name | li-packet-cable statistics service-name service_name | performance-counters name service-name | statistics name service-name [ all | atcf | calls | eatf equip-id | eatf-statistics | ip-security | message | npdb [ all | instance id ] | package-name { message-summary | presence | reg | winfo } | registrations | sigcomp | tcp { msrp | sip } ] | subscription name service-name } [ | { grep grep_options | more } ]

all [ counters ]
Displays configuration information for all CSCF services configured on this system.

counters: Displays statistics with the configuration information for all CSCF services configured on the system.

diameter { location-info statistics service-name service_name [ vpn-name name ] | policy-control statistics service-name service_name [ vpn-name name ] } | grey-list name name | li-packet-cable statistics service-name service_name | location-info statistics service-name service_name [ vpn-name name ] | policy-control statistics service-name service-name [ vpn-name name ] } | grey-list name name | li-packet-cable statistics service-name service_name | performance-counters name service-name | statistics name service-name [ all | atcf | calls | eatf equip-id | eatf-statistics | ip-security | message | npdb [ all | instance id ] | package-name { message-summary | presence | reg | winfo } | registrations | sigcomp | tcp { msrp | sip } ] | subscription name service-name } [ | { grep grep_options | more } ]

location-info statistics: Displays Diameter statistics on the E2 interface with the location information.
policy-control statistics: Displays Diameter (DPECA) statistics on the CSCF Rx interface with the configuration information.
service-name service_name: Specifies the name of an existing CSCF service for which the statistics will be displayed as an alphanumeric string of 1 through 63 characters.

vpn-name name: Specifies the name of an existing context in which all statistics for all services will be displayed as an alphanumeric string of 1 through 79 characters.

grey-list name name
Displays an existing list of run-time grey-listed users and their remaining barred period for the specified CSCF service as an alphanumeric string of 1 through 63 characters.

li-packet-cable statistics service-name service_name
Refer to the Lawful Intercept Configuration Guide for a description of this command.
name service_name [ counters ]
Displays configuration information for an existing CSCF service specified as an alphanumeric string of 1 through 63 characters.

counters: Displays statistics with the configuration information for the specific CSCF service.

performance-counters name service_name
Displays performance counters (3GPP TS 32.409) for an existing CSCF service specified as an alphanumeric string of 1 through 63 characters.

statistics name service_name [ all | atcf | calls | eatf equip-id | eatf-statistics | ip-security | message | npdb [ all | instance id ] | package-name { message-summary | presence | reg | winfo } | registrations | sigcomp | tcp { msrp | sip } ]
Displays service statistics for an existing CSCF service specified as an alphanumeric string of 1 through 63 characters.

- all: Displays all CSCF service statistics.
- atcf: Displays statistics related to ATCF access transfers.
- calls: Displays session statistics related to CSCF calls.
- eatf equip-id: Displays the list of all equipment IDs under an E-CSCF service.
- ip-security: Displays session statistics related to CSCF IPSec.
- message: Displays session statistics for the SIP method MESSAGE.
- npdb: Displays NPDB message statistics for the specific S-CSCF service. These statistics are associated with the various messages in the NPDB call flow, such as BIND, PING_PONG, REL_REQ, and ERRREP.
  - all: Displays statistics related to NPDB across all instances.
  - instance id: Displays NPDB statistics for an existing instance. id must be an integer from 1 through 65535.
- package-name: Displays session statistics for the associated event package.
  - presence: Displays session statistics for the “presence” event package.
  - reg: Displays session statistics for the “reg” event package.
  - winfo: Displays session statistics for the “watcher-info” event package.
- registrations: Displays session statistics related to CSCF registrations, re-registrations, and de-registrations.
- sigcomp: Displays session statistics related to CSCF sigcomp.
- tcp: Displays session statistics related to CSCF TCP.
  - msrp: Displays statistics related to CSCF TCP MSRP statistics.
  - sip: Displays statistics related to CSCF TCP SIP statistics.

Important: This keyword must be followed by another statistics-related keyword.

subscription name service_name
Displays service level subscription information for an existing CSCF service specified as an alphanumeric string of 1 through 63 characters.
show cscf service

| { grep grep_options | more }

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage
Use this command to display configuration information and/or statistics for any or all CSCF services on this system.

Example
The following command displays service statistics for the CSCF service named `cscf1`:

```
show cscf service statistics name cscf1
```

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show cscf sessions

Displays statistics for Call Session Control Function (CSCF) sessions on this system.

Product
SCM

Privilege
Security Administrator, Administrator, Operator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show cscf sessions { counters { calls { duration | first-response-time | invite-processing-time | post-answer-delay | post-dial-delay | service service_name | session-release-delay | session-setup-delay } service service_name | subscription { duration | service service_name | setup-time } service service_name } | duration | full { callleg-id id | from-aor aor | service service_name | session-id id | to-aor aor } [ media-type type ] | summary { from-aor aor | service service_name | session-id id | to-aor aor } } [ | { grep grep_options | more } ]

counters { calls { duration | first-response-time | invite-processing-time | post-answer-delay | post-dial-delay | service service_name | session-release-delay | session-setup-delay } service service_name | subscription { duration | service service_name | setup-time } service service_name }

Displays counters for all CSCF sessions matching the filter criteria.
calls: Counters associated with calls in CSCF service.

• duration: Displays the call duration time.
  • first-response-time: Displays the time interval for the first response received for INVITE.
  • invite-processing-time: Displays the INVITE message processing time in CSCF.
  • post-answer-delay: Displays the time interval for post answer delay.
  • post-dial-delay: Displays the time interval for the ringing or success response for INVITE.
  • service service_name: Displays counters for an existing CSCF service specified as an alphanumeric string of 1 through 63 characters.

Important: This keyword may be used alone with the counters keyword or following any other counters-specific keyword.

• session-release-delay: Displays the time interval for releasing the call.
• session-setup-delay: Displays the time interval for session setup.
• subscription: Counters associated with subscriptions in CSCF service.
  • duration: Displays the SIP Subscription duration time.
show cscf sessions

• service service_name: Displays specific service. service_name must be an existing CSCF service and be from 1 to 63 alphanumeric characters.

  Important: This keyword may be used alone with the subscription keyword or following any other subscription-specific keyword.

• setup-time: Displays the SIP Subscription setup time.

duration
Displays the call duration for all CSCF sessions.

full [ callleg-id id | from-aor aor | service service_name | session-id id | to-aor aor ] [ media-type type ]
Displays all the session information for the active CSCF sessions matching the filter criteria.
callleg-id id: Displays session statistics for an existing call-leg ID, and must be an alphanumeric string of 1 through 63 characters.
from-aor aor: Displays session statistics for sessions originating from an existing Address of Record (AoR) specified as an alphanumeric string of 1 through 79 characters.
service service_name: Displays session statistics for sessions using an existing CSCF service specified as an alphanumeric string of 1 through 63 characters.
session-id id: Displays session statistics for sessions with an existing ID specified as an alphanumeric string of 1 through 63 characters.
to-aor aor: Displays session statistics for sessions sent to an existing AoR specified as an alphanumeric string of 1 through 79 characters.
media-type type: Displays information about an existing media type specified as an alphanumeric string of 1 through 9 characters.

summary [ from-aor aor | service service_name | session-id id | to-aor aor ]
Displays session summary information for sessions matching the filter criteria.
from-aor aor: Displays session statistics for sessions originating from an existing AoR specified as an alphanumeric string of 1 through 79 characters.
service service_name: Displays session statistics for sessions using an existing CSCF service specified as an alphanumeric string of 1 through 63 characters.
session-id id: Displays session statistics for sessions with an existing ID specified as an alphanumeric string of 1 through 63 characters.
to-aor aor: Displays session statistics for sessions sent to an existing AoR specified as an alphanumeric string of 1 through 79 characters.

| { grep grep_options | more }
 Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
Refer to Regulating a Command’s Output section of the Command Line Interface Overview chapter for details on the usage of grep and more.

Usage
Use this command to display session information for any or all CSCF sessions.

Example
The following command displays the output for CSCF session duration:

```bash
show cscf sessions duration
```
show cscf sessions duration

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show cscf sip

Displays Session Initiation Protocol (SIP) statistics for a specific Call Session Control Function (CSCF) service configured on this system.

Product
SCM

Privilege
Security Administrator, Administrator, Operator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show cscf sip statistics name service_name [ interface { domain { list | name domain_name } } | ip { address ip_address | list } ] [ vpn-name name ] [ | { grep grep_options | more } ]

statistics name service_name

Specifies the name of an existing CSCF service as an alphanumeric string of 1 through 63 characters.

[ interface { domain { list | name domain_name } } | ip { address ip_address | list } ]

SIP statistics will be displayed for this interface.

domain list: Displays list of interfaces associated with the CSCF service.
domain name domain_name: Specifies an existing domain associated with the CSCF service as an alphanumeric string of 1 through 80 characters.
ip address ip_address: Specifies the destination or source IP address associated with the CSCF service in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.
ip list: Displays a list of interfaces associated with the CSCF service.

vpn-name name

Specifies the name of an existing VPN as an alphanumeric string of 1 through 79 characters.

| { grep grep_options | more }

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

Refer to Regulating a Command’s Output section of the Command Line Interface Overview chapter for details on the usage of grep and more.

Usage

Use this command to display SIP statistics for a specific CSCF service.
Important: This command displays counters for SIP statistics for a specified CSCF service. Counters are incriminated when SIP messages are sent (Tx) or received (Rx). SIP Request, Response, and Error counters are maintained at various levels in the SIP stack. These values are dependent on the packet flow. For example, if packets are dropped at an initial stage of parsing and error detection, the counters may not increment. All 2xx Response counters for individual requests are maintain outside the SIP layer and will not track re-transmissions and erroneous packets that are dropped. All other counters do keep track of re-transmissions.

Example

The following command displays SIP statistics for the CSCF service named cscf1:

```
show cscf sip statistics name cscf1
```

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
**show cscf tcp**

Displays TCP connection information for a specific Call Session Control Function (CSCF) service configured on this system.

**Product**

SCM

**Privilege**

Security Administrator, Administrator, Operator

**Mode**

Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

**Syntax**

```
show cscf tcp connections service service_name [ facility { cscfmgr | sessmgr } ] [ full ] [ msrp ] [ remote-ip ip_address ] [ remote-port port_number ] [ sip ] [ | { grep grep_options | more } ]
```

- **connections service service_name**
  Specifies the name of an existing CSCF service as an alphanumeric string of 1 through 63 characters.

- **facility { cscfmgr | sessmgr }**
  Facility type for which connection details have to be retrieved.
  - `cscfmgr`: Facility type cscfmgr.
  - `sessmgr`: Facility type sessmgr.

- **full**
  Displays detailed information related to each connection.

- **msrp**
  Displays statistics related to CSCF TCP Message Session Relay Protocol (MSRP) statistics.

- **remote-ip ip_address**
  Specifies the remote IP address to match the connection in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

- **remote-port port_number**
  Specifies the remote port to match the connection an integer from 1 through 65534.

- **sip**
  Displays statistics related to CSCF TCP SIP statistics.
Usage

Use this command to display TCP connection information for a specific CSCF service.

Important: More than one optional keyword may be used per command.

Example

The following command displays TCP connections for the CSCF service named cscf1:

```
show cscf tcp connections service cscf1
```

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show css delivery-sequence

In StarOS 9.0 and later releases, this command is deprecated.
show css server

In StarOS 9.0 and later releases, this command is deprecated.
show css service

In StarOS 9.0 and later releases, this command is deprecated.
Chapter 128
Exec Mode show Commands (D-G)

This section includes the commands `show dhcp` through `show gtpu-service`.

The Exec Mode is the initial entry point into the command line interface system. Exec mode `show` commands are useful in troubleshooting and basic system monitoring.

Mode

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
show dhcp

Displays counter information pertaining to Dynamic Host Configuration Protocol IPv4 (DHCP) functionality based on specific criteria.

Product

- GGSN
- ASN-GW
- P-GW
- SAEGW

Privilege

- Security Administrator
- Administrator
- Operator
- Inspector

Mode

Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show dhcp [ counters | full | summary ] [ all | apn apn_name | callid id | chaddr mac_address | dhcp-service svc_name | imsi imsi | msid msid | server server_address | statistics [ dhcp-service svc_name | server server_address ] | status [ dhcp-service svc_name | server server_address ] | user-address address | username name | [wf1] [ | { grep grep_options | more } ]

counters

Displays DHCP counter information.

full

Displays all available information pertaining to the criteria specified.

summary

Displays a summary of the DHCP statistics.

all

Displays counter information for each active PDP context.

apn apn_name

Displays information based on an existing Access Point Name (APN) specified as an alphanumeric string of 1 through 63 characters that is case sensitive.

callid id

Displays information for an existing call identification number specified as a 4-digit hexadecimal number.
Exec Mode show Commands (D-G)

```bash
chaddr mac_address
Displays information for a mobile node specified by its MAC address.

dhcp-service svc_name
Displays information for an existing DHCP service specified as an alphanumeric string of 1 through 63 characters that is case sensitive.

imsi imsi
Displays information for an International Mobile Subscriber Identity (IMSI) specified as a string of 1 to 15 digits.

msid msid
Displays information for a Mobile Subscriber Identity (MSID) specified as a string of 1 to 15 digits.

server server_address
Displays information for a DHCP server specified by its IP address in IPv4 dotted-decimal notation.

statistics [ dhcp-service svc_name | server server_address ]
Displays DHCP statistics for either a specific or for all DHCP services and servers configured.

dhcp-service svc_name: Displays statistics for a DHCP service specified as an alphanumeric string of 1 through 63 characters that is case sensitive.

server server_address: Displays statistics for a DHCP server specified by its IP address in IPv4 dotted-decimal notation.

status [ dhcp-service svc_name | server server_address ]
Displays configuration information for either a specific or for all DHCP services and servers configured.

dhcp-service svc_name: Displays statistics for a DHCP service specified as an alphanumeric string of 1 through 63 characters that is case sensitive.

server server_address: Displays statistics for a DHCP server specified by its IP address in IPv4 dotted-decimal notation.

user-address address
Displays information for a DHCP-assigned user IP address specified in IPv4 dotted-decimal notation.

username name
Displays information for a subscriber specified as an alphanumeric string of 1 through 127 characters (including wildcards “$” and “*”) that is case sensitive.

wf1
Displays all available information for associated filter keyword in wide-format number 1.

| { grep grep_options | more }
Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference.
```
Usage
Counters pertaining to DHCP functionality can be displayed as cumulative values or for specific APNs, PDP contexts, servers, or DHCP services.

Example
The following command displays DHCP counter information for a DHCP service called \textit{DHCP-Gi}:

\begin{verbatim}
show dhcp dhcp-service DHCP-Gi
\end{verbatim}

The following command displays DHCP counter information for a DHCP Call ID \textit{01ca11a2}:

\begin{verbatim}
show dhcp call-id DHCP-Gi
\end{verbatim}

The following command displays DHCP information for the specified mobile node:

\begin{verbatim}
show dhcp chaddr 00:05:47:00:37:44
\end{verbatim}

\textbf{Important:} Output descriptions for commands are available in the \textit{Statistics and Counters Reference}. 
show dhcp-service

Displays information for either a specific or for all Dynamic Host Configuration Protocol IPv4 (DHCP) services.

**Product**
GGSN
ASN-GW
P-GW
SAEGW

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Mode**
Exec
The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
show dhcp-service { all | name svc_name } [ | { grep grep_options | more } ]
```

- **all**
  Displays information for all configured DHCP services.

- **name svc_name**
  Displays information for a DHCP service name specified as an alphanumeric string of 1 through 63 characters that is case sensitive.

- **| { grep grep_options | more }**
  Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of `grep` and `more`, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

**Usage**
This command is used to verify the configuration of one or all DHCP services for monitoring or troubleshooting purposes. The output is a concise listing of DHCP service parameter settings.

If this command is executed from within the local context with the all keyword, information for all DHCP services configured on the system will be displayed.

**Example**
The following command displays configuration information for a DHCP service called dhcp1:

```
show dhcp-service name dhcp1
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show dhcpv6

Displays counter information pertaining to Dynamic Host Configuration Protocol IPv6 (DHCPv6) functionality based on specific criteria.

Product
GGSN
ASN-GW
P-GW
SAEGW

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show dhcpv6 [ counters | full | summary ] [ all | callid id | server server_address | service svc_name | statistics [ dhcp-service svc_name | server server_address ] | status [ dhcp-service svc_name | server server_address ] [ | { grep grep_options | more } ] ]

counters
Displays DHCPv6 counter information.

full
Displays all available information pertaining to the criteria specified.

summary
Displays a summary of the DHCPv6 statistics.

all
Displays counter information for each active PDP context.

callid id
Displays information for an existing call identification number specified as an 8-digit hexadecimal number.

server server_address
Displays information for a DHCPv6 server specified by its IP address in IPv6 colon-separated-hexadecimal notation.

Important: In StarOS 15.0 and later releases, this option is deprecated
statistics [ dhcp-service svc_name ]
Displays DHCPv6 statistics for either a specific or for all DHCPv6 services.
dhcp-service svc_name: Displays statistics for a DHCPv6 service specified as an alphanumeric string of 1 through 63 characters that is case sensitive.
server server_address: Displays statistics for a DHCPv6 server specified by its IP address in IPv6 colon-separated-hexadecimal notation.

Important: In StarOS 15.0 and later releases, this option is deprecated

status [ dhcp-service svc_name ]
Displays configuration information for either a specific or for all DHCPv6 services and servers configured.
dhcp-service svc_name: Displays statistics for a DHCPv6 service specified as an alphanumeric string of 1 through 63 characters that is case sensitive.
server server_address: Displays statistics for a DHCPv6 server specified by its IP address in IPv6 colon-separated-hexadecimal notation.

Important: In StarOS 15.0 and later releases, this option is deprecated

| { grep grep_options | more } |
Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference.

Usage
Counters pertaining to DHCP IPv6 functionality can be displayed as cumulative values or for specific APNs, PDP contexts or DHCPv6 services.

Example
The following command displays DHCPv6 status information for a DHCPv6 service called DHCPv6-Gi:

show dhcpv6 status service DHCPv6-Gi

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show dhcpv6-client-profile

Displays configuration information for a specific or all Dynamic Host Configuration Protocol IPv6 (DHCPv6) client profiles.

Product
GGSN
ASN-GW
P-GW
SAEGW

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show dhcpv6-client-profile [ all | name profile_name ] | { grep grep_options | more }

all
Displays configuration information for all DHCPv6 client profiles.

name profile_name
Displays profile configuration information for an existing DHCPv6 client profile specified as an alphanumeric string of 1 through 63 characters.

| { grep grep_options | more }

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference.

Usage
Use this command to display configuration information for one or all DHCPv6 client profiles.

Example
The following command displays all DHCPv6 client profiles:

show dhcpv6-client-profile all
show dhcpv6-server-profile

Displays configuration information for a specific or all Dynamic Host Configuration Protocol IPv6 (DHCPv6) server profiles.

Product

GGSN
ASN-GW
P-GW
SAEGW

Privilege

Security Administrator, Administrator, Operator, Inspector

Mode

Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show dhcpv6-server-profile { all | name profile_name } | { grep grep_options | more }

all
Displays configuration information for all DHCPv6 server profiles.

name profile_name
Displays profile configuration information for an existing DHCPv6 server profile specified as an alphanumeric string of 1 through 63 characters.

| { grep grep_options | more }
Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference.

Usage

Use this command to display configuration information for one or all DHCPv6 server profiles.

Example

The following command displays all DHCPv6 server profiles:

show dhcpv6-server-profile all
show dhcpv6-service

Displays service information and configuration counters for a specific or all Dynamic Host Configuration Protocol IPv6 (DHCPv6) services.

Product

GGSN
ASN-GW
P-GW
SAEGW

Privilege

Security Administrator, Administrator, Operator, Inspector

Mode

Exec

The following prompt is displayed in the Exec mode:

[local] host_name#

Syntax

show dhcpv6-service [ all | name svc_name ] | { grep grep_options | more }

all
Displays configuration information and counters for all DHCPv6 services.

name svc_name
Displays configuration information and counters for an existing DHCPv6 service specified as an alphanumeric string of 1 through 63 characters.

| { grep grep_options | more }

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference.

Usage

Use this command to display configuration information and counters for one or all DHCPv6 services.

Example

The following command displays all DHCPv6 services:

show dhcpv6-service all
show diameter aaa-statistics

Displays Diameter Authentication, Authorization and Accounting (AAA) statistics.

Product

All

Privilege

Security Administrator, Administrator, Operator, Inspector

Mode

Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show diameter aaa-statistics [ all | group group_name [ server server_name ] | server server_name ] [ | { grep grep_options | more } ]

- **all**
  - Displays all available Diameter server statistics.

- **group group_name [ server server_name ]**
  - Displays all Diameter server statistics within an existing AAA group specified as an alphanumeric string of 1 through 64 characters.
  - *server_name* must be the name of a Diameter server, expressed as an alphanumeric string of 1 through 64 characters.

- **server server_name**
  - Displays Diameter server statistics for the Diameter server name specified as an alphanumeric string of 1 through 64 characters.

| { grep grep_options | more } |

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of *grep* and *more*, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

Usage

Use this command to view Diameter AAA statistics.

Example

The following command displays all available Diameter server statistics:

```
show diameter aaa-statistics all
```
show diameter accounting servers aaa-group

Displays Diameter accounting server information for an Authentication, Authorization and Accounting (AAA) group.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show diameter accounting servers [ aaa-group group_name ] [ | { grep grep_options | more } ]

aaa-group group_name
Specifies the name of an existing AAA group as an alphanumeric string of 0 through 64 characters.

| [ grep grep_options | more ]
Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference.

Usage
Use this command to view Diameter accounting server information for an AAA group.

Example

The following command displays Diameter accounting server information for an AAA group named in group12:

show diameter accounting servers aaa-group group12
show diameter authentication servers aaa-group

Displays Diameter Authentication server information for a specified AAA group.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show diameter authentication servers [ aaa-group group_name ]

aaa-group group_name
Specifies the name of an existing AAA group as an alphanumeric string of 0 through 64 characters.

Usage
Use this command to view Diameter authentication server information for an AAA group.

Example
The following command displays Diameter authentication server information for an AAA group named group12:

    show diameter authentication servers aaa-group group12
show diameter dynamic-dictionary

Displays the contents of Diameter dictionary that is loaded dynamically at run time.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show diameter dynamic-dictionary { { all [ contents ] } | { name dict_name [ contents | { full facility { aaamgr | diamproxy | sessmgr instance instance_no } ] } } | { grep grep_options | more } }

all
Displays, in text format, the information for all dynamically loaded dictionaries configured in the Global Configuration mode. Displays up to 10KB buffered text from each dictionary file.

name dict_name
Displays detailed information for an existing dynamically loaded dictionary specified as an alphanumeric string of 1 through 15 characters. Displays up to 10KB buffered text from the specified dictionary file.

full facility { aaamgr | diamproxy | sessmgr }
Displays all available information for the specified instance associated with one of the following facilities:
• aaamgr — Accounting and authentication Manager
• diamproxy — Diameter Proxy
• sessmgr — Session Manager

instance instance_no
Specifies the instance number from which dynamic dictionary details to be fetched, is an integer value between 0 through 4294967295.

| { grep grep_options | more }
Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference.
Usage

Use this command to view the contents of dynamically loaded Diameter dictionaries. For more details on the dynamic configuration of Diameter dictionary, refer to the `diameter dynamic-dictionary` command in the Global Configuration Mode Commands chapter.

Example

The following command displays the contents of dynamically loaded Diameter dictionary file named `dyn1`:

```
show diameter dynamic-dictionary name dyn1
```
show diameter endpoint

This command has been deprecated, and is replaced by the show diameter endpoints command.
show diameter endpoints

This command displays the status of Diameter client endpoint(s).

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show diameter endpoints { all | endpoint endpoint_name } [ | { grep grep_options | more } ]

all
Displays status of all Diameter client endpoints.

endpoint endpoint_name
Displays status of an existing Diameter client endpoint specified as an alphanumeric string of 1 through 63 characters.

| { grep grep_options | more }
Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference.

Usage
Use this command to view the status of Diameter client endpoints.
If you are in the local context, then all contexts are searched for the specified endpoint(s). Specify all to see all endpoints; otherwise, just the named endpoint will be displayed. If no argument is provided, a summary of all endpoints is displayed.
Default value: N/A

Example
The following command displays status of all Diameter client endpoints.

    show diameter endpoints all

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show diameter message-queue

Displays Diameter message queue statistics.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

`show diameter message-queue counters { inbound | outbound } [ endpoint endpoint_name [ peer-host peer_id [ peer-realm realm_id ] ] | session-id session_id ] [ | { grep grep_options | more } ]`

counters { inbound | outbound }
Specifies the message counters:
inbound: Specifies Diameter inbound messages
outbound: Specifies Diameter outbound messages

endpoint endpoint_name
Specifies the Diameter endpoint as an alphanumeric string of 1 through 63 characters.

peer-host peer_id
Specifies the Diameter peer host as an alphanumeric string of 1 through 63 characters.

peer-realm realm_id
Specifies the Diameter peer realm as an alphanumeric string of 1 through 127 characters.

session-id session_id
Specifies the session ID as an alphanumeric string of 1 through 127 characters.

| { grep grep_options | more }
Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of `grep` and `more`, refer to the Regulating a Command's Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference.

Usage

Use this command to view the count of the messages in the Diameter message queue for specific counter type, session ID, or endpoint, peer host, and peer realm.
Example

The following command displays message queue statistics for outbound messages specific to the Diameter endpoint named `asr5k.testnetwork.com`:

```
show diameter message-queue counters outbound endpoint asr5k.testnetwork.com
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show diameter peers

Displays Diameter peer information.

Product

All

Privilege

Security Administrator, Administrator, Operator, Inspector

Mode

Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

```
show diameter peers [ full | summary ] [ all | [ endpoint endpoint_name ] [ peer-host peer_id ] [ peer-realm realm_id ] ] [ | { grep grep_options | more } ]
```

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>full</code></td>
<td>Displays full details of all or specified Diameter peers.</td>
</tr>
<tr>
<td><code>summary</code></td>
<td>Displays summary details of all or specified Diameter peer(s).</td>
</tr>
<tr>
<td><code>all</code></td>
<td>Displays details of all Diameter peers.</td>
</tr>
<tr>
<td><code>endpoint endpoint_name</code></td>
<td>Displays details of the origin Diameter endpoint specified as an alphanumeric string of 1 through 255 characters.</td>
</tr>
<tr>
<td><code>peer-host peer_id</code></td>
<td>Displays details of the Diameter peer host specified as an alphanumeric string of 1 through to 63 characters.</td>
</tr>
<tr>
<td><code>peer-realm realm_id</code></td>
<td>Displays details of the Diameter peer realm ID specified as an alphanumeric string of 1 through 127 characters.</td>
</tr>
<tr>
<td>`</td>
<td>{ grep grep_options</td>
</tr>
</tbody>
</table>
**Usage**

Use this command to view the details of Diameter peers.
If you are in the local context, then all contexts are searched for the specified peer(s).
This is similar to the `show subscribers` CLI command and supports multiple filter options specified at the same time.
If filter options are specified (e.g., `all`, `endpoint`, etc.), the default is for one line of output to be displayed per peer. Use `full` to get detailed information per peer, or `summary` to get summarized information about all matching peers.
If no filter options are specified, a summary output for all peers is displayed. Use the `full` option to get detailed information about every peer.
Default value: N/A

**Example**

The following command details of the Diameter endpoint named `endpoint12`:

```
show diameter peers endpoint endpoint12
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show diameter route status

Displays Diameter route health status information.

**Product**
All

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
show diameter route status [ endpoint endpoint_name | full [ endpoint endpoint_name ] ] [ host host_name [ peer peer_id ] ] [ | { grep grep_options | more } ]
```

- **full**
  Displays information about which Diameter clients are using which peer/host combinations.

- **endpoint endpoint_name**
  Displays detailed information for the Diameter client endpoint specified as an alphanumeric string of 1 through 63 characters.

- **host host_name**
  Displays information for the Diameter host specified as an alphanumeric string of 1 through 63 characters.

- **peer peer_id**
  Displays information for the Diameter peer host specified as an alphanumeric string of 1 through 63 characters.

| { grep grep_options | more } |

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

**Usage**

Use this command to view the Diameter route health status. The route status displays status of peer/host combinations. Refer to the **route-failure** CLI command in Diameter Endpoint Configuration mode. When no options are specified, the display will give one line per peer/host combination, indicating how many Diameter clients are using each combination, and for how many clients the combination is available or failed. Specify **full** to see which Diameter clients are using which
peer/host combinations. Specify **host** or **peer** to see just combinations with the named host or peer. Specify **endpoint** to see detailed information about the named Diameter client.

Default value: N/A

**Example**

The following command displays route health status details of the Diameter client endpoint named `endpoint12`:

```
show diameter route status endpoint endpoint12
```
show diameter route table

Displays the Diameter routing table.

**Product**
All

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
show diameter route table [ wide ] [ endpoint endpoint_name ] [ | { grep grep_options | more } ]
```

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>wide</code></td>
<td>Displays the route table information in wide-format.</td>
</tr>
<tr>
<td><code>endpoint endpoint_name</code></td>
<td>Displays the Diameter routing table for the Diameter endpoint specified as an alphanumeric string of 1 through 63 characters.</td>
</tr>
<tr>
<td>`</td>
<td>{ grep grep_options</td>
</tr>
</tbody>
</table>

**Usage**

Use this command to view the status of Diameter client endpoints. If you are in the local context, then the route information used by Diameter endpoints in all chassis contexts will be used in the display. The route table displays all static and dynamic routes. Refer to the route-entry CLI command in Diameter Endpoint Configuration Mode. Default value: N/A

**Example**

The following command displays status of the Diameter client endpoint named `endpoint12`.

```
show diameter route table endpoint endpoint12
```
**show diameter statistics**

Displays Diameter peer statistics.

**Product**
All

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
show diameter statistics { [ proxy ] endpoint endpoint_name [ peer-host peer_id [ peer-realm realm_id ] ] [ | { grep grep_options | more } ] }
```

- **endpoint endpoint_name**
  Displays statistics for the Diameter endpoint specified as an alphanumeric string of 1 through 63 characters.

- **peer-host peer_id**
  Displays statistics for the Diameter host peer specified as an alphanumeric string of 1 through 255 characters.

- **peer-realm realm_id**
  Displays statistics for the Diameter peer realm specified as an alphanumeric string of 1 through 127 characters.

- **proxy**
  Displays proxy related statistics.

- **| { grep grep_options | more }**
  Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of `grep` and `more`, refer to the *Regulating a Command’s Output* section of the Command Line Interface Overview chapter in the Command Line Interface Reference.

**Usage**

Use this command to view Diameter statistics for the specified endpoint or proxy.

**Example**

The following command displays Diameter peer statistics for the endpoint named `endpoint12`:

```
show diameter statistics endpoint endpoint12
```
show diameter-service

Displays information about configured Diameter services.

**Product**
All

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
show diameter-service { all | lte-s6a trace-id { all | user-name user_name } | name service_name | statistics name service_name [ vpn-name vpn_context_name ] } [ | { grep grep_options | more } ]
```

- **all**
  Displays full information for all configured Diameter services.

- **lte-s6a trace-id { all | user-name user_name }**
  Displays user trace ID information for an LTE/S6a application.
  - **all**: Displays full information.
  - **user-name user_name**: Displays information for the user specified an alphanumeric string of 1 through 79 characters.

- **name service_name**
  Displays information for the Diameter service name specified as an alphanumeric string of 1 through 79 characters.

- **statistics name service_name [ vpn-name vpn_context_name ]**
  Displays statistics for the Diameter service name specified as an alphanumeric string of 1 through 79 characters.
  - **vpn-name vpn_context_name**: Specifies the name of VPN context as an alphanumeric string of 1 through 79 characters.

- **| { grep grep_options | more }**
  Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.
  For details on the usage of **grep** and **more**, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*. 
Usage
Use this command to view information on configured Diameter services.

Example
The following command displays statistics for the Diameter service named ggsn12:

```
show diameter-service name ggsn2
```
show dns-client

Displays cache and/or statistics for a specified Domain Name System (DNS) client.

Product
- ePDG
- P-CSCF, SIP Proxy
- SGSN
- HSGW
- MME
- P-GW
- SAEGW

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec
The following prompt is displayed in the Exec mode:

[local] host_name#

Syntax

show dns-client { cache client name [ query-name name | query-type { A | AAAA | NAPTR | SRV } ] | statistics client name } [ | [ grep grep_options | more ] ]

cache client name [ query-name name | query-type { A | AAAA | NAPTR | SRV } ]
displays statistics for the cache of an existing DNS client specified as an alphanumeric string of 1 through 255 characters.

query-name name: Filters DNS results based on the domain name specified as an alphanumeric string of 1 through 255 characters. name is the domain name used to perform the DNS query. It is different from the actual domain name which is resolved. For example, to resolve the SIP server for service.com, the query name is _sip._udp.service.com and the query type is SRV.

query-type:
- A: Filters DNS results based on 32-bit domain IPv4 address records (A records).
- AAAA: Filters DNS results based on 128-bit domain IPv6 address records (AAAA resource records).
- NAPTR: Filters DNS results based on Naming Authority Pointer records.
- SRV: Filters DNS results based on service locator records (SRV records).

statistics client name
Displays statistics for an existing DNS client specified as an alphanumeric string of 1 through 255 characters.

| { grep grep_options | more }
Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of `grep` and `more`, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter.

**Usage**

Use this command to display DNS cache and/or statistics for a specified DNS client.

**Example**

The following command displays statistics for a DNS client named `domain1.com`:

```
show dns-client statistics client domain1.com
```

**Important**: Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show dynamic-policy statistics

Displays policy control and charging (PCC) statistics from the interface communicating with the Policy and Charging Rules Function (PCRF) via Gx(x).

Product
HSGW
PDSN
SAEGW
S-GW

Privilege
Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local] host_name#

Syntax

show dynamic-policy statistics { hsgw-service name | pdsn-service name | sgw-service name }

hsgw-service name
Displays policy control and charging statistics from the Gxa interface communicating with the PCRF. name must be an existing HSGW service name and be from 1 to 63 alphanumeric characters.

pdsn-service name
Displays policy control and charging statistics from the Gx interface communicating with the PCRF. name must be an existing PDSN service name and be from 1 to 63 alphanumeric characters.

sgw-service name
Displays policy control and charging statistics from the Gxc interface communicating with the PCRF. name must be an existing S-GW service name and be from 1 to 63 alphanumeric characters.

Usage
Use this command to display PCC statistics for the specified service and its Gx interface communicating with the PCRF.

Example
The following command displays HSGW statistics for an HSGW service named hsgw4:

    show dynamic-policy statistics hsgw-service hsgw4

The following command displays PCC statistics for a PDSN service named cdma4:

    show dynamic-policy statistics pdsn-service cdma4
The following command displays S-GW statistics for an S-GW service named `sgw4`:

```
show dynamic-policy statistics sgw-service sgw4
```
**show egtpc peers**

Displays information about eGTP-C peers.

**Product**
- ePDG
- MME
- P-GW
- SAEGW
- S-GW

**Privilege**
Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local] host_name# 
```

**Syntax**

```
show egtpc peers [ address ip_address | egtp-service name ] | interface { epdg-egress | mme | pgw-ingress | sgsn | sgw-egress | sgw-ingress } [ address ip_address ] [ wf1 ] | { grep grep_options | more } |
```

- **address ip_address**
  Displays information about a eGTP-C peer specified by its IP address in IPv4 dotted-decimal notation or IPv6 colon-separated-hexadecimal notation.

- **egtp-service name [ address ip_address ]**
  Displays information about eGTP-C peers associated with an existing egtp-service name specified as an alphanumeric string of 1 through 63 characters.
  
  **address ip_address**: Additionally, the results can be filtered based on the IP address associated with an existing eGTP-C peer service specified in IPv4 dotted-decimal notation or IPv6 colon-separated-hexadecimal notation.

- **interface { epdg-egress | mme | pgw-ingress | sgsn | sgw-egress | sgw-ingress } [ address ip_address ] [ wf1 ]**
  Displays information about eGTP-C peers associated with the service interface configured on this system.
  
  **epdg-egress**: Displays ePDG's egress EGTP interface.
  
  **mme**: Displays information about eGTP-C MME peers associated with the service interface configured on this system. Additionally, the results can be filtered based on the IP address associated with the MME peer.
  
  **pgw-ingress**: Displays information about eGTP-C P-GW ingress peers associated with the service interface configured on this system. Additionally, the results can be filtered based on the IP address associated with the P-GW ingress peer.
  
  **sgsn**: Displays information about eGTP-C SGSN peers associated with the S4 service interface configured on this system. Additionally, the results can be filtered based on the IP address associated with the SGSN peer.
**sgw-egress**: Displays information about eGTP-C S-GW egress peers associated with the service interface configured on this system. Additionally, the results can be filtered based on the IP address associated with the S-GW egress peer.

**sgw-ingress**: Displays information about eGTP-C S-GW ingress peers associated with the service interface configured on this system. Additionally, the results can be filtered based on the IP address associated with the S-GW ingress peer.

**address ip_address**: Specifies the IP address of the selected peer in IPv4 dotted-decimal notation or IPv6 colon-separated-hexadecimal notation.

**wf1**: Specifies that the output is to be displayed in wide format number 1.

```
| { grep grep_options | more }
```

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.

For details on using the `grep` and `more` commands, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter.

**Usage**

Use this command to display information about eGTP-C peers associated with the service interface configured on this system. The output contains the following information about the peer:

- Status of the peer
- Echo status
- Restart counter status
- Peer restart counter knowledge
- Service ID
- Peer IP address
- Current sessions
- Maximum sessions

**Important**: The primary command, `show egtpc peers`, when entered without additional keywords, displays information for all peers associated with the service operating on this system.

**Example**

The following command returns an output for an eGTP-C S-GW egress peers associated with the service interface configured on this system with an IP address of 10.2.3.4:

```
show egtpc peers interface sgw-egress address 10.2.3.4
```

The following command returns an output for an eGTP-C MME peer associated with the service interface configured on this system with an IP address of 10.2.3.4:

```
show egtpc peers interface mme address 10.2.3.4
```
show egtpc sessions

Displays eGTP-C session information.

**Product**
ePDG
MME
P-GW
SAEGW
S-GW

**Privilege**
Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

**Syntax**

```
show egtpc sessions [ egtp-service name | interface { epdg-egress | mme | pgw-ingress | sgsn | sgw-egress | sgw-ingress } ] [ | { grep grep_options | more } ]
```

- **egtp-service name**
  Displays information about eGTP-C sessions associated with an existing egtp-service specified as an alphanumeric string of 1 through 63 characters.

- **interface { epdg-egress | mme | pgw-ingress | sgsn | sgw-egress | sgw-ingress }**
  Displays information about eGTP-C sessions associated with the service interface configured on this system.

  - **epdg-egress**: Displays information about ePDG egress associated with EGTP interface.
  - **mme**: Displays information about eGTP-C sessions associated with the MME interface configured on this system.
  - **pgw-ingress**: Displays information about eGTP-C sessions associated with the P-GW ingress interface configured on this system.
  - **sgsn**: Displays information about eGTP-C sessions associated with the SGSN eGTP-C S4 interface configured on this system.
  - **sgw-egress**: Displays information about eGTP-C sessions associated with the S-GW egress interface configured on this system.
  - **sgw-ingress**: Displays information about eGTP-C sessions associated with the S-GW ingress interface configured on this system.

- **| { grep grep_options | more }**
  Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.
  For details on using the **grep** and **more** commands, refer to the *Regulating a Command’s Output* section of the Command Line Interface Overview chapter.
Usage

Use this command to display session information for a specific eGTP service or for sessions associated with an interface type configured on this system.

Example

The following command displays eGTP-C session information for sessions associated with all P-GW ingress interfaces configured on this system:

```
show egtpc sessions interface pgw-ingress
```

The following command displays eGTP-C session information for sessions associated with all MME interfaces configured on this system:

```
show egtpc sessions interface mme
```
show egtpc statistics

Displays evolved GPRS Tunneling Protocol Control (eGTP-C) plane statistics for a specific service name or interface type.

**Product**
ePDG
MME
P-GW
SAEGW
S-GW

**Privilege**
Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local] host_name#
```

**Syntax**

```
show egtpc statistics [ demux-only | egtp-service name | epdg-address ip_address | event-statistics | header-decoder-errors | interface { epdg-egress | mme | pgw-ingress | sgsn | sgw-egress | sgw-ingress } | mme-address ip_address | path-failure-reasons | pgw-address ip_address | piggybacking-statistics | sessmgr-only | sgsn-address ip_address | sgw-address ip_address ] [ verbose ] [ | { grep grep_options | more } ]
```

---

**demux-only**
Displays entry point statistics at demux manager.

---

**egtp-service name**
Displays statistics for an existing eGTP service specified as an alphanumeric string of 1 through 63 characters.

---

**epdg-address ip_address**
Displays eGTP-C statistics for an existing ePDG IP address expressed in IPv6 colon-separated-hexadecimal notation.

---

**event-statistics**
Displays total eGTP-C events sent/received.

---

**header-decoder-errors**
Displays header decoding errors of incoming packets at eGTP-C stack/demux manager.
Exec Mode show Commands (D-G)

show egtpc statistics

interface { epdg-egress | mme | pgw-ingress | sgw-egress | sgw-ingress }

epdg-egress: Displays eGTP-C statistics for all ePDG egress interfaces.
mme: Displays eGTP-C statistics for all MME interfaces.
pgw-ingress: Displays eGTP-C statistics for all eGTP P-GW ingress interfaces.
sgsn: Displays eGTP-C statistics for all eGTP S4 SGSN interfaces.
sgw-egress: Displays eGTP-C statistics for all eGTP S-GW egress interfaces.
sgw-ingress: Displays eGTP-C statistics for all eGTP S-GW ingress interfaces.

mme-address ip_address
Displays eGTP-C statistics for an existing MME IP address expressed in IPv4 dotted-decimal notation or IPv6 colon-separated-hexdecimal notation.

path-failure-reasons
Displays breakup of reasons for path failure.

pgw-address ip_address
Displays eGTP-C statistics for an existing P-GW IP address expressed in IPv4 dotted-decimal notation or IPv6 colon-separated-hexdecimal notation.

piggybacking-statistics
Displays total piggybacked messages sent/received at eGTP-C stack.

sessmgr-only
Displays entry point statistics at sessmgr.

sgsn-address ip_address
Displays eGTP-C statistics for an existing SGSN S4 IP address expressed in IPv4 dotted-decimal or IPv6 colon-separated-hexdecimal notation.

sgw-address ip_address
Displays eGTP-C statistics for an existing S-GW IP address expressed in IPv4 dotted-decimal or IPv6 colon-separated-hexdecimal notation.

verbose
Displays the maximum amount of detail available for this commands output. If this option is not specified, the output is truncated to a more concise level.

| { grep \grep_options | more }
Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.
For details on using the grep and more commands, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.
show egtpc statistics

Usage

Use this command to display evolved GPRS Tunneling Protocol Control (eGTP-C) plane statistics for a specific service name or interface type.

Example

The following command displays eGTP-C statistics for interfaces configured as S-GW ingress interfaces:

```
show egtpc statistics interface sgw-ingress
```

The following command displays eGTP-C session information for sessions associated with all MME interfaces configured on this system:

```
show egtpc sessions interface mme
```
show egtp-service

Displays configuration information for evolved GPRS Tunneling Protocol (eGTP) services on this system.

Product
- ePDG
- MME
- P-GW
- SAEGW
- S-GW

Privilege
Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show egtp-service { all | name service_name } [ | { grep grep_options | more } ]

- **all**
  Displays configuration information for all eGTP services configured on this system.

- **name service_name**
  Displays configuration information for an existing eGTP service specified as an alphanumeric string of 1 through 63 characters.

  | { grep grep_options | more }
  Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.
  For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Reference Guide*.

Usage

Use this command to view configuration information for eGTP services on this system.

Example

The following command displays service statistics for the eGTP service named *egtp1*:

```
show egtp-service name egtp1
```
show epdg-service

Displays information about selected EPDG calls/services.

**Product**
ePDG

**Privilege**
Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
show epdg-service { all [ counters [ | { grep grep_options | more } ] ] | name epdg_service_name [ counters [ | { grep grep_options | more } ] ] | session [ all | callid call_id [ counters | full | ip-address { < ip_address | > ip_address | IP-ADDRESS | greater-than ip_address | less-than ip_address } | peer-address peer_address | [ summary ] | username user_name [ | { grep grep_options | more } ] ] } | statistics [ dns-stats ] [ name service_name [ peer-address peer_address ] [ | { grep grep_options | more } ] ] }
```

---

**all**

Displays information for all configured services.

**counters**

Displays counters associated with EPDG service.

**name epdg_service_name**

Displays specific service. This must be followed by service name `epdg_service_name`, which is a string of size between 1 and 63.

**session**

Displays information about configured EPDG sessions.

**callid call_id**

Specific Call Identification Number. This must be followed by `call_id`, an eight digit HEX number.

**full**

Displays all available information for associated display or filter keyword (previous keyword).

**ip-address**

Displays IP address of the subscriber. Must be followed by IPv4 address, in dotted decimal notation.
< ip_address | less-than ip_address
Specifies Less Than. Must be followed by IPv4 / IPV6 address, in dotted / (:) / (::) decimal notation.

> ip_address | greater-than ip_address
Specifies Greater Than. Must be followed by an IP address of IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

peer-address peer_address
Address of specific IP Peer. This must be followed by IPv4 address in dotted decimal notation or IPv6 address in colon-separated-hexadecimal notation.

summary
Displays the summary of available information for associated display or filter keyword (previous keyword).

username user_name
Displays the name of specific user within current context. This must be followed by user_name, which is a string between 1 and 127.

statistics
Displays the total of collected information for specific protocol since last restart or clear command.

dns-stats
Displays information related to DNS PGW selection.

name service_name
Displays specific service. Must be followed by service_name, which is a string of size between 1 and 63.

| { grep grep_options | more }
Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.
For details on using the grep and more commands, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage
Use this command to display information about selected EPDG calls/services.

Example
The following command displays ePDG counter information:

    show epdg-service all counters | grep 21
show event-notif server

Displays the counter information of configured Event Notification servers based on specific criteria.

Product
All

Privilege
Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show event-notif server all [ | { grep grep_options | more }]

---

all

Displays counter information for each active Event Notification server in this context.

| { grep grep_options | more }

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.

For details on using the grep and more commands, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

---

Usage

Use this command to display the counters pertaining to the Event Notification collection servers configured in a context.

Example

The following command displays the counter information for all Event Notification collection servers configured in a context:

show event-notif server all

---

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show event-notif statistics

Displays the statistical information collected over configured Event Notification interface based on specific criteria.

Product
All

Privilege
Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

```
show event-notif statistics [ | { grep grep_options | more }]
```

| | { grep grep_options | more }
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.</td>
</tr>
<tr>
<td>For details on using the <strong>grep</strong> and <strong>more</strong> commands, refer to the <em>Regulating a Command’s Output</em> section of the <em>Command Line Interface Overview</em> chapter.</td>
</tr>
</tbody>
</table>

Usage

Use this command to display the statistical information collected over configured Event Notification interface based on specific criteria.

Example

The following command displays the counter information for all Event Notification collection servers configured in a context:

```
show event-notif statistics
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show external-inline-servers

This command is obsolete.
**show fa-service**

Displays information on configured foreign agent (FA) services.

**Product**
- PDSN
- GGSN
- ASN-GW

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:
```
[local]host_name#
```

**Syntax**
```
show fa-service { all | name fa_name } [ | { grep grep_options | more } ]
```

- `all | name fa_name`
  - `all`: indicates information on all foreign agent services is to be displayed.
  - `name fa_name`: indicates only the information for the named FA service is to be displayed.

- `| { grep grep_options | more }`
  - Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.
  - For details on the usage of `grep` and `more`, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

**Usage**
Display foreign agent service configuration information.

**Example**

The following commands display information on the FA service `sampleService` and all services, respectively.

```
show fa-service name sampleService
show fa-service all
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show fa-spi-list

Displays Security Parameter Indices (FA-SPIs) for configured foreign agent (FA) services.

**Product**
- PDSN
- GGSN
- ASN-GW

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
show fa-spi-list { all | name fa_name } [ | { grep grep_options | more } ]
```

- `all`: indicates information on all foreign agent services is to be displayed.
- `name fa_name`: indicates only the information for the named FA service is to be displayed.

| Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent. For details on the usage of `grep` and `more`, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*. |

**Usage**
Display foreign agent SPI information.

**Example**
The following command displays SPI information for the FA service `sampleService`.

```
show fa-spi-list name sampleService
```

*Important:* Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show fans

Displays the current control status, speed, and temperature for the upper and lower fans in the system chassis.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show fans [ verbose ] [ | { grep grep_options | more } ]

verbose

ASR 5500 only: Displays additional information regarding the state of the fan trays.

| { grep grep_options | more }

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference.

Usage

View the fan information to verify system hardware status as necessary.

Example

The following command displays information regarding the cooling fans in the system:

show fans

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show file

Displays the contents of the file specified. The contents are paginated as if it were normal ASCII output.

**Product**

All

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Mode**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
show file url [ | { grep grep_options | more } ]
```

`url` specifies the location of a file to display. `url` may refer to a local or a remote file. `url` must be entered using the following format:

For the ASR 5000:

```
{ file: }{ /flash | /pcmcia1 | /hd }{ /directory }/file_name
```

```
tftp://{ host[ :port# ] }{ /directory }/file_name
```

```
/directory ]/file_name
```

For the ASR 5500:

```
{ file: }{ /flash | /usb1 | /hd }{ /directory }/file_name
```

```
tftp://{ host[ :port# ] }{ /directory }/file_name
```

```
/directory ]/file_name
```

**Important:** Use of the SMC hard drive is not supported in this release.

**Important:** Do not use the following characters when entering a string for the field names below: “/” (forward slash), “:” (colon) or “@” (at sign).

- `directory` is the directory name.
- `filename` is the actual file of interest.
- `username` is the user to be authenticated.
password is the password to use for authentication.
host is the IP address or host name of the server.
port# is the logical port number that the communication protocol is to use.

| { grep grep_options | more }

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage
Display the contents of files to view such information as log data, trace information, etc.

Example
The following will display the contents of the local file /pub/log.txt.

    show file //pcmcia1/pub/log.txt

The following command will display the contents of the file /pub/log.txt on remote host remoteABC.

    show file ftp://remoteABC/pub/log.txt
show firewall flows

This command is obsolete.
show firewall ruledef

This command is obsolete.
show firewall statistics

This command is obsolete.
show fng-service

Displays information about specified Femto Network Gateway (FNG) service configuration, status, and counters, and includes information about all the sessions currently maintained by the FNG.

Product
FNG

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show fng-service { all [ counters ] | name service_name | session | statistics }

| all |
| Displays information for all configured FNG services. |

| counters |
| Displays counters associated with the FNG service. |

| name service_name |
| Displays information only for an existing FNG service specified as an alphanumeric string of 1 through 63 characters. |

| session |
| Displays information about configured FNG sessions. |

**Important:** See show fng-service session for detailed options.

| statistics service_name |
| Total of collected information for specific protocol since the last restart or clear command. |

**Important:** See show fng-service statistics for detailed options.

| { grep grep_options | more } |
| Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent. |

For details on the usage of grep and more, refer to the section Regulating a Command’s Output in the chapter Command Line Interface Overview in the Command Line Interface Reference.
Usage
Use this command to view information for selected configured FNG services.

Example
The following command displays available information for all active FNG services.

```
show fng-service all
```

Important: Command output descriptions are available in the Statistics and Counters Reference.
show fng-service session

Displays statistics for specific Femto Network Gateway (FNG) sessions.

Product  
FNG

Privilege  
Security Administrator, Administrator, Operator, Inspector

Mode  
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show fng-service session [ all | callid call_id | counters | full [ all | callid call_id | ip-address ip-address | peer-address ip_address | username name ] | ip-address ip-address | peer-address ip_address | summary [ all | callid call_id | ip-address ip-address | peer-address ip_address | username name ] | username name ]

all
Displays all related information for all active FNG sessions.

callid
Displays PPP information for the call ID specified as a 4-digit hexadecimal number.

counters
Displays counters for the configured FNG sessions.

full
Displays all available information for the associated display or filter keyword.

ip-address ipv4_address
Displays information for the subscriber IP address specified in IPv4 dotted-decimal notation.

peer-address ipv4_address
Displays information for the IP peer specified by its IP address in IPv4 dotted-decimal notation.

summary
Displays summary information for FNG sessions.

username user_name
Displays information for a username within the current context specified as an alphanumeric string of 1 through 127 characters.
Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent. For details on the usage of `grep` and `more`, refer to the section Regulating a Command’s Output in the Command Line Interface Overview chapter.

Usage
Use this command to view configuration information for an FNG session.

Example
The following command displays all available FNG sessions.

```
show fng-service session all
```

**Important:** Command output descriptions are available in the Statistics and Counters Reference.
show fng-service statistics

Displays statistics for the FNG since the last restart or clear command. The output includes the number of each type of protocol message. For example, the output includes the various types of EAP messages.

Product
FNG

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show fng-service statistics [ name service_name | peer-address ipv4_address ]

name service_name
Displays statistics for an existing service name specified as an alphanumeric string of 1 through 63 characters.

peer-address ipv4_address
Displays statistics for an IP peer specified by its IP address in IPv4 dotted-decimal notation.

| { grep grep_options | more }

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of grep and more, refer to the section Regulating a Command’s Output in the Command Line Interface Overview chapter.

Usage

Use this command to display FNG statistics.

Important: You may use more than one keyword per command line.

Example

The following command displays information about the FNG service.

    show fng-service statistics

Important: Command output descriptions are available in the Statistics and Counters Reference.
show freeze-ptmsi imsi

Displays the P-TMSI (packet-temporary mobile subscriber identify) corresponding to the IMSI (international mobile subscriber identity) that has entered a frozen state after the purge timeout timer expires.

Product
SGSN

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show freeze-ptmsi imsi imsi_num

imsi imsi_num

Specifies the IMSI that has been frozen as a sequence of up to 15 digits. The first three digits are the MCC (mobile country code). The next two or three digits are the MNC (mobile network code). The remaining digits are the MSIN (mobile station identification number).

Usage
This command enables the operator to know whether a frozen IMSI has an associated P-TMSI.

Example
The following command displays the P-TMSI corresponding to a frozen IMSI:

show freeze-ptmsi imsi 262090426000194
show ggsn sessmgr

Displays session manager (SessMGR) statistics specific to the gGSN service.

Product
GGSN

Privilege
Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show ggsn sessmgr { all | instance smgr_inst }

- **all**
  
  Displays all SessMGR statistics specific to the system’s GGSN services.

- **instance smgr_inst**
  
  Displays the statistics for a session manager instance of the GGSN service specified as an integer between 1 and 10000000.

Usage

Use this command to display information for GGSN services.

Example

The following command displays GGSN SessMGR statistics for all GGSN services on the system:

```
show ggsn sessmgr all
```
show ggsn-service

Displays configuration information for Gateway GPRS Support Node (GGSN) services on the system.

Product
GGSN

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

```
show ggsn-service { all | name ggsn_svc_name } [ | { grep grep_options | more }]
```

- **all**
  Displays information for all GGSN services configured with the given context.

- **name ggsn_svc_name**
  Displays information for an existing GGSN service name specified as an alphanumeric string of 1 through 63 characters that is case sensitive.

- | { grep grep_options | more }
  Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.
  For more information on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Reference.

Usage

This command is used to verify the configuration of one or all GGSN services for monitoring or troubleshooting purposes. The output is a concise listing of GGSN service parameter settings.

If this command is executed from within the local context with the all keyword, information for all GGSN services configured on the system will be displayed.

Example

The following command displays configuration information for a GGSN service called `ggsnl`:

```
show ggsn-service name ggsnl
```
show ggsn-service sgsn-table

Lists all Serving GPRS Support Nodes (SGSNs) by IP addresses and shows the current number of subscribers to each SGSN.

Product
GGSN

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show ggsn-service sgsn-table

Usage
While there are existing commands to show SGSN subscriber information, this command is the only way to list all SGSNs by IP address and show the current number of subscribers to each SGSN.

Example
The following command will bring up a table showing the current active/inactive status, IP address, reboots/restarts and SGSN users.

    show ggsn-service sgsn-table

> Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show global-title-translation

Displays configuration information for Global Title Translation (GTT).

Product
SGSN

Privilege
Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show global-title-translation { address-map { all | instance instance } | association { all | instance instance } }

address-map { all | instance }

Displays configuration information for either the entire GTT address map database or for a specific instance of an address map. instance is an integer from 1 to 4096 which uniquely identifies the address map configuration.

association { all | instance }

Displays configuration information for either the entire database of GTT association lists for for a specific instance of GTT association configuration. instance is an integer from 1 to 16 which uniquely identifies the GTT association configuration.

Usage

This command displays the configuration for the GTT address maps and associations.

Example

The following command displays the address map 2047.

    show global-title-translation address-map 2047
show gmb statistics

Displays the collected statistics for the Gmb reference point. Gmb handles broadcast multicast service center (BM-SC) related signaling, which includes the user specific and bearer service messages for Multimedia Broadcast/Multicast Service (MBMS) service.

Product
GGSN

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show gmb statistics [ apn name | bmsc-profile profile_name ] [ | { grep grep_options | more }]

- **apn name**
  Displays only the Gmb information for the specified Access Point Name (APN) specified as an alphanumeric string of 1 through 62 characters.

- **bmsc-profile profile_name**
  Displays only the Gmb information for the specified BM-SC profile specified as an alphanumeric string of 1 through 79 characters.

- **| { grep grep_options | more }**
  Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.
  For more information on the usage of **grep** and **more**, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Reference*.

Usage

Use this command to display usage statistics for the Gmb reference point.

Example

The following command displays all Gmb statistics:

```
show gmb statistics
```
show gmm-sm statistics

Displays statistics for the GPRS Mobility Management and Session Management (GMM/SM) configuration of the system’s SGSN service. GMM/SM supports mobility to allow the SGSN to know the location of a Mobile Station (MS) at any time and to activate, modify and deactivate the PDP sessions required by the MS for user data transfer.

Product
SGSN

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local] host_name#

Syntax

show gmm-sm statistics [ gmm-only | gprs-service srvc_name | iups-service srvc_name | plmn-id mcc mcc mnc mnc [ access-type { gprs | umts } ] | sgsn-service srvc_name | sm-only ] [ verbose ] [ | { grep grep_options | more } ]

Keywords are presented below. Primary keywords are listed in the order of selection as shown in the syntax. Secondary or filtering keywords are presented alphabetically after the description of the primary keywords.

---

**gmm-only**
Displays only GPRS mobility management (GMM) information for other specified keyword parameters for the current context.

**gprs-service srvc_name**
Displays the statistics for an existing 2.5G GPRS service name specified as an alphanumeric string of 1 through 63 characters.
The display request can be narrowed by adding either the nsei or routing-area filter keywords.

**iups-service srvc_name**
Displays the statistics for an existing IuPS service specified as an alphanumeric string of 1 through 63 characters.
The display request can be narrowed by adding either the rnc or routing-area filter keywords.

**plmn-id mcc mcc mnc mnc [ access-type { gprs | umts } ]**
Filters the statistics display per PLMN.
Enter the access-type keyword to fine-tune the display of the GMM/SM statistics to an aggregate of the IuPS (select access-type UMTS) and/or the GPRS (select access-type GPRS) services belonging to the PLMN.
sgsn-service srvc_name
Displays the statistics for an existing 3G SGSN service specified as an alphanumeric string of 1 through 63 characters.
The display request can be narrowed by adding either the rnc or routing-area filter keywords.

sm-only
Displays only session management (SM) information for other specified keyword parameters for the current context.

access-type type
Filters the display of service statistics by 2.5G GPRS services or 3G IuPS services for UMTS:
• gprs
• umts
If this keyword is not included, then statistics for both access types are displayed.

lac lac_id
 Specifies the location area code (LAC) as part of the identification of the RNC or RA as an integer from 1 through 65535.

mcc mcc_id
 Specifies the mobile country code (MCC) as part of the identification of the RNC or RA an integer from 100 through 999.

mnc mnc_id
 Specifies the mobile network code (MNC) as part of the identification of the RNC or RA as a 2- or 3-digit integer from 00 through 999.

nsei nse_id
 Displays the GMM/SM session statistics for an existing network service entity (NSEI) specified as an integer from 0 to 65535.

rac rac_id
 Specifies the routing area code (RAC) as part of the identification of the RNC or RA as an integer from 1 through 255.

erce rnc_id
 Enter this keyword to fine-tune the display of the GMM/SM session statistics just for the radio network controller (RNC) specified as an integer from 0 through 4095.

routing-area mcc mcc_id mnc mnc_id lac lac_id rac rac_id
Enter the routing-area keyword to fine-tune the display of the GMM/SM statistics for a specified routing area (RA) identified by the MCC, MNC, LAC and RAC.

verbose
Displays all possible statistics for specified command or keyword.
show gmm-sm statistics

Usage

Use this command to display usage statistics for the GMM/SM session configurations for SGSN services, including a BSC attaches, activations, and throughput.

Example

The following command displays GMM/SM statistics for a specific routing area defined for the 2.5G SGSN’s GPRS service:

```
show gmm-sm statistics gprs-service gprsl routing-area mcc 123 mcc 131 lac 24 rac 11
```

The following command displays all possible information for GMM/SM statistics:

```
show gmm-sm statistics verbose
```

**Important:** Output descriptions for commands are available in the Statistics and Counters Reference.
show gprsns statistics

 Displays the statistics for the 2.5G SGSN’s GPRS NS layer (link level).

**Product**
SGSN

**Privilege**
Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

`[local]host_name#`

**Syntax**

```bash
show gprsns statistics { msg-stats { consolidated nse nse_id | nse nse_id } | sns-msg-stats } | { grep grep_options | more }
```

- **msg-stats**
  Displays the transmit (Tx) and receive (Rx) message statistics (except for SNS messages) in the statistics output.

- **consolidated nse nse_id**
  
  `nse_id`: Enter an integer from 0 to 65535.

- **nse nse_id**
  Display statistics for a NSE specified as an integer from 0 to 65535.

- **sns-msg-stats**
  Display subnetwork service (SNS) sublayer message statistics.

  ```bash
  | { grep grep_options | more }
  ```

  Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.

  For details on the usage of `grep` and `more`, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

**Usage**

This command is used to display Frame Relay statistics configured for the NSE/NSVC with the commands documented in the *Network Service Entity - Peer NSEI Configuration Mode Commands* chapter.

Collected statistics are cleared (deleted) with the `clear gprsns statistics` described in the *Exec Mode Commands (A-C)* chapter.

**Example**

Use the following command to display the collected message statistics for NSEI 1422:

```bash
[local]host_name# show gprsns statistics
```
show gprsns statistics msg-stats nse 1422

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference.*
show gprsns status

Displays the status of the network service virtual circuits (NSVC) for the GPRS NS layer (link level).

**Product**
SGSN

**Privilege**
Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
show gprsns status { nsvc-status-all nse nse_id | nsvc-status-consolidated nse nse_id | nsvc-status-per-bvci bvci bvc_id nse nse_id } | { grep grep_options | more }
```

- **nsvc-status-all nse { all | nse:nse_id }**
  Displays status information for all NSVCs included in the NSE specified as an integer from 0 to 65535.

- **nsvc-status-consolidated nse nse_id**

- **nsvc-status-per-bvci bvci bvc_id nse nse_id**
  - **bvc_id** is an integer from 0 to 65535.
  - **nse_id** is an integer from 0 to 65535.

  | { grep grep_options | more }

  Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.

  For details on the usage of **grep** and **more**, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference.

**Usage**

This command is used to display the status of the NSVC.

**Example**

Use the following command to display status of all NSVC for NSE 1422:

```
show gprsns status nsvc-status-all nse 1422
```

**Important:** Output descriptions for commands are available in the Statistics and Counters Reference.
show gprs-service

Displays the statistics for GPRS services.

Product
SGSN

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show gprs-service { all | name gprs_svc_name } [ nsei { all | id nse_id } | { grep grep_options | more } ]

all
Instructs the SGSN to display information for all GPRS services configured with this context.

name gprs_svc_name
Instructs the SGSN to display information for the specified GPRS service.
gprs_svc_name is a case-sensitive string of 1 to 63 characters, any combination of letters, digits, dots (.) and dashes (-) that identifies a specific GPRS service.

nsei { all | id }nse_id
Instructs the SGSN to display network service entity information for either a specific NSEI or for all NSEI configured for the specified GPRS service(s).
nse_id is an integer from 0 to 65535.

| { grep grep_options | more } |
Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.
For more information on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Reference.

Usage
This command is used to verify the configuration of one or all GPRS services for monitoring or troubleshooting purposes. The output is a concise listing of GPRS service parameter settings.
If this command is executed from within the local context with the all keyword, information for all GPRS services configured on the system will be displayed.

Example
The following command displays configuration information for all GPRS services configured in this context:

show gprs-service all
Use a command similar to the following to display statistics for NSEI 4257 for the GPRS service named London2:

```
show gprs-service name London2 nsei id 4257
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference.*
show gprsssf

Displays statistics for various 3GPP Customised Applications for Mobile network Enhanced Logic (CAMEL) service GPRS Service Switching Function (gprsSSF) entities.

Product
SGSN

Privilege
Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show gprsssf { counters | statistics } [ camel-service srvc_name | gprs [ 2g-sgsn-app | 3g-sgsn-app ] | gsmscf-address { address | all } | sms ] [ | { grep | more } ]

| counters
| Displays collected status counter information for CAMEL service entities.

| statistics
| Displays collected statistics for CAMEL service entities.

| camel-service srvc_name
| Filters the display of counters and statistics for an existing CAMEL service name in the SGSN configuration specified as an alphanumeric string of 1 through 63 characters that is case sensitive.

| gprs [ 2g-sgsn-app | 3g-sgsn-app ]
| Filters the counter/statistic output to display GPRS protocol information specific to either the 2.5G or 3G SGSN.

| gsmscf-address { address | all }
| The GSM service control function (gsmSCF) address is the ISDN address of the SCP where the CAMEL service resides. It is possible to display information for one or all of the configured CAMEL services. address is a standard ISDN E.164 address of 1 to 15 digits.

| sms
| Filters the display of counters and statistics for SMS protocol information.

| { grep grep_options | more }
| Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.
show gprsssf

For details on the usage of *grep* and *more*, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*.

**Usage**

Use this command to display CAMEL service status counter information and statistics collected since the last restart or clear command. If filters are not included with the command, then all statistics or counters are displayed for all CAMEL services in all contexts in which CAMEL services have been defined. Collected statistics are cleared (deleted) with the *clear gprsssf statistics* command described in the chapter *Exec Mode Commands (A-C)*.

**Example**

Use the following command to display the status counter totals of the GPRS Dialogue parameters for a 3G SGSN:

```
show gprsssf counter gprs 3g-sgsn-app
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show gs-service

Displays configuration information and statistics for Gs services configured on system.

Product
SGSN

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

`show gs-service { all | name svc_name } [ | { grep grep_options | more } ]`

- **all**
  Displays information for all Gs services configured with in the given context.

- **name svc_name**
  Displays information for an existing Gs service specified as an alphanumeric string of 1 through 63 characters that is case sensitive.

  | { grep grep_options | more }

  Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.

  For more information on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Reference.

Usage

This command is used to verify the configuration of one or all Gs services for monitoring or troubleshooting purposes.

If this command is executed from within the local context with the all keyword, information for all Gs services configured on the system will be displayed.

Example

The following command displays configuration information for all Gs services configured on a system:

```
show gs-service all
```

**Important:** Output descriptions for commands are available in the Statistics and Counters Reference.
show gtpc

Displays GPRS Tunnelling Protocol-Control (GTPC) information for GTPv0, GTPv1-C, GTPv1-U with filtering options.

Product
GGSN

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show gtpc [ full | counters | summary ] { all | apn apn_name | imsi imsi_value [ nsapi nsapi_value ] | callid callid | sgsn-address ip_address | ggsn-service ggsn_name | user-address ip_address | username username }

[ full | counters | summary ]
Specifies the level of information to be displayed. The following levels can be used:

•full: Indicates detailed information is to be displayed.
•counters: Indicates the output is to include the statistical counters.
•summary: Indicates only summary information is to be displayed.

{ all | apn apn_name | imsi imsi_value [ nsapi nsapi_value ] | callid callid | sgsn-address ip_address | ggsn-service ggsn_name | user-address ip_address | username username }
Specifies the filter criteria used when displaying GTP information. The following filters can be used:

•all: Specifies that all available information is to be displayed.

•apn apn_name: Specifies that GTP information for an APN specified as an alphanumeric string of 1 through 63 characters that is case sensitive.

•imsi imsi_value [ nsapi nsapi_value ]: Displays GTP information for an International Mobile Subscriber Identity (IMSI) specified as an integer from 1 through 15 characters. Optionally, the IMSI could be further filtered by specifying a particular PDP context using the Network Service Access Point Identifier (NSAPI) expressed as an integer from 5 through 15.

Important: In release 18.2 and later, this command option has been deprecated.

•callid callid: Displays GTP information for a call identification number specified as a 4-digit hexadecimal number.

Important: In release 18.2 and later, this command option has been deprecated.
show gtpc

- **sgsn-address ip_address**: Displays GTP information for an SGSN specified by its IP address in IPv4 dotted-decimal notation.

- **ggsn-service ggsn_name**: Displays GTP information for an existing GGSN service specified an alphanumeric string of 1 through 63 characters that is case sensitive.

- **user-address ip_address**: Displays GTP information for a user PDP context specified as an IP address in IPv4 dotted-decimal notation.

**Important**: In release 18.2 and later, this command option has been deprecated.

- **username username**: Displays GTP information for a username specified as an alphanumeric string of 1 through 127 characters (including wildcards ‘$’ and ‘*’) that is case sensitive.

**Important**: In release 18.2 and later, this command option has been deprecated.

**Usage**

This command displays statistics for every GTP message type based on the filter criteria. This information is useful for system monitoring or troubleshooting.

**Example**

The following command displays GTPC counters for a GGSN service named ggsn1:

```
show gtpc counters ggsn-service ggsn1
```

The following command displays GTPC full information:

```
show gtpc full
```

The following command displays GTPC summary information for a specific call identification number of 05f62f34:

```
show gtpc summary callid 05f62f34
```

**Important**: Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show gtpc statistics

Displays GTPv0, GTPv1-C, GTPv1-U statistics with filtering options.

Product
GGSN

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show gtpc statistics [ [ custom1 | custom2 ] [ apn apn_name | ggsn-service ggsn_service_name | mseg-service mseg_service_name | sgsn-address ipv4_address ] [ [ verbose ] format1 ] [ | { grep grep_options | more } ]]

custom1
Displays statistics of GTP-C messages for preservation mode and free of charge service. This keyword is customer specific and license enabled. For more information, contact your Cisco sales representative.

custom2
Displays statistics for GTP-C messages related to overcharging protection on loss of radio coverage for a GGSN service. This keyword is feature specific and license enabled. For more information, contact your Cisco sales representative.

apn apn_name
Displays GTP-C statistics for an existing APN specified as an alphanumeric string of 1 through 63 characters that is case sensitive.

ggsn-service ggsn_service_name
Displays GTP-C statistics for an existing GGSN service specified as an alphanumeric string of 1 through 63 characters that is case sensitive.

mseg-service mseg_service_name

Important: This keyword is not supported in this release.

sgsn-address ipv4_address
Displays GTP statistics for an SGSN specified by its IP address in IPv4 dotted-decimal notation.
show gtpc statistics

**verbose**
Displays detailed instead of concise statistics.

**format1**
Displays more detailed statistical breakouts.

```
| { grep grep_options | more }
```
Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

**Usage**
The information displayed by this command consists of session statistics such as the number of currently active sessions categorized by PDP context type, and statistics for every GTP message type. The statistics are cumulative.
If the verbose keyword is used, additional information will be displayed such as statistics for every type of error code.

**Example**
The following command displays verbose GTP statistics:

```
show gtpc statistics verbose
```

**Important:** Output descriptions for commands are available in the Statistics and Counters Reference.
show gtpp

Displays information on the GPRS Tunneling Protocol Prime (GTPP) for the selected charging gateway function (CGF) or GCDR storage server.

Product

- GGSN
- P-GW
- SAEGW
- SGSN

Privilege

Security Administrator, Administrator, Operator, Inspector

Mode

Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show gtpp { accounting | counters { all | cgf-address | group } | group { all | name } | statistics { cgf-address | group } | storage server { counters | group | local | statistics | status | streaming } } [ | { grep grep_options | more } ]

Usage

This command displays the GTPP related information for the selected CGF or the G-CDRs storage server. If this command is issued from within the local context, information for all GTPP accounting servers configured on the system is displayed regardless of context.

Example

The following command displays the GTPP counters for all the servers:

```
show gtpp counters all
```

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show gtp accounting

Displays information on the GPRS Tunneling Protocol Prime (GTPP) accounting server configuration.

Product
GGSN
P-GW
SAEGW
SGSN

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec
The following prompt is displayed in the Exec mode:

[local] host_name#

Syntax

show gtp accounting servers { group name group_name } [ | { grep grep_options | more } ]

Usage
This command is used to view the status of GTPP accounting servers configured within a context for monitoring or troubleshooting purposes.
If this command is issued from within the local context, information for all GTPP accounting servers configured on the system is displayed regardless of context.

Example
The following command displays the status of and information on configured GTPP accounting servers:

show gtp accounting servers

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show gtpp counters

Displays GTPP counters for configured charging gateway functions (CGFs) within the given context.

Product

GGSN
P-GW
SAEGW
SGSN

Privilege

Security Administrator, Administrator, Operator, Inspector

Mode

Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show gtpp counters { all { gcdrs } | cgf-address cgf_address | group name group_name } [ | { grep grep_options | more } ]

all
Displays counters for all CGFs configured within the context.

cgf-address cgf_address
Displays counters for a CGF specified by its IP address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

Usage

Counters for a single CGF can be viewed using the cgf-address keyword. Counters for all CGFs in the context can be viewed by entering the command with the all keyword.

If this command is issued from within the local context and no CGF-address is specified, the counters displayed will be cumulative for all CGFs configured on the system regardless of context.

Example

The following command displays counters for all CGF:

show gtpp counters all

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show gtpp group

Displays information pertaining to the configured GTPP storage server group.

Product

GGSN
P-GW
SAEGW
SGSN

Privilege

Security Administrator, Administrator, Operator, Inspector

Mode

Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show gtpp group { name gtpp_group_name | all } [ | { grep grep_options | more } ]

name gtpp_group_name

Displays information and CDR statistics for an existing GTPP server group name specified as an alphanumeric string of 1 through 64 characters.

all

Displays statistics for all configured GTPP storage server groups, including default group.

| { grep grep_options | more }

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent. For more information on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage

Use this command to display the CDR statistics on the basis of GTPP server groups. It shows the information for all or specific GTPP server group configured in the context from which this command is issued.

Example

The following command displays the status of the GTPP server group backup server configured in a context called GTPP_Group1:

show gtpp group name GTPP_Group1

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show gtpp statistics

Displays GTPP statistics for configured Charging Gateway Functions (CGFs) within the context.

Product
- ePDG
- GGSN
- P-GW
- SAEGW
- SGSN

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show gtpp statistics { cgf-address cgf_address | group name group_name } [ | { grep grep_options | more } ]

---

cgf-address cgf_address
Displays statistics for a CGF specified by its IP address expressed in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

---

group name group_name
Displays server statistics information of an existing GTPP server group name specified as an alphanumeric string of 1 through 64 characters.

---

| { grep grep_options | more } |
Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent. For more information on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference.

Usage
Statistics for a single CGF can be viewed by specifying its IP address. Statistics for all CGFs in the context can be viewed by not specifying an IP address. If this command is issued from within the local context, the statistics displayed will be cumulative for all CGFs configured on the system regardless of context.

Example
The following command displays statistics for a CGF with an IP address of 192.168.1.14:

```
show gtpp statistics cgf-address 192.168.1.14
```
show gtpp statistics

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show gtpp storage-server

Displays information pertaining to the configured GTPP storage server (GSS).

Product
GGSN
P-GW
SAEGW
SGSN

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show gtpp storage-server { counters { all | group name group_name } | group name group_name | local file { counters { all | group name group_name } | statistics [ group name group_name ] } | status { group name group_name | verbose } | streaming file { counters { all | group name group_name } | statistics [ group name group_name ] } } [ | { grep grep_options | more } ]

counters
Displays counters for the external GTPP storage server.

group name group_name
Displays GTPP backup server information for the group name specified as an alphanumeric string of 1 through 64 characters.

local file
Displays statistics and counters for the local storage-server. This is the hard disk if hard disk support has been enabled with the gtpp storage-server mode command in the GTPP Group Configuration Mode.

statistics
Displays statistics for the GTPP storage server.

status [ verbose ]
Displays status of the GTPP storage server. verbose enables the detailed view.

streaming
Displays the status of Charging Data Record (CDR) backup on HDD while streaming mode is enabled.
Usage

Executing this command with no keywords displays status information for the GTPP backup server configured in the context from which this command is issued.

Example

The following command displays the GTPP CDR file statistics stored on the local SMC hard disk.

```
show gtpp storage-server local file counters all
```

The following command displays the status of the GTPP backup server configured in a context called ggsn1:

```
show gtpp storage-server
```

The following command displays statistics for the GTPP backup server configured in a context called ggsn1:

```
show gtpp storage-server statistics
```

The following command displays GCDR storage server counters:

```
show gtpp storage-server counters
```

The following command displays GCDR storage server status:

```
show gtpp storage-server status
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*. 

| ( grep grep_options | more )

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent. 

For details on the usage of `grep` and `more`, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter in the *Command Line Interface Reference*. 

```
show gtpu

Displays GPRS Tunneling Protocol user plane (GTP-U) statistics and counters on this system.

Product

ePDG
P-GW
SAEGW
SGSN
S-GW

Privilege

Inspector

Mode

Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show gtpu { local-addresses | statistics [ [ gtpu-service gtpu_service_name ] | gtpumgr-instance gtpumgr_instance | local-address ipv4/ipv6_address | mseg-service mseg_service_name | peer-address ipv4/ipv6_address ] ] [ | { grep grep_options | more } ] }

local-addresses

Displays the number of sessions on all GTPU local addresses in all GTPU services.

statistics

Displays all GTP-U statistics on all GTP-U services. Refine the display by including one of the filters listed below.

gtpu-service gtpu_service_name

Displays GTP-U statistics for an existing GTP-U service specified as an alphanumeric string of 1 through 63 characters.

gtpumgr-instance instance_number

Displays information for an existing GTP-U manager instance specified as an integer from 1 through 4294967295.

local-address ipv4/ipv6_address

Displays subscriber statistics and counters in the current active session per local GTPU IP address specified in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation in a GTPU service.
show gtpu

```
msg-service mseg_service_name
```

**Important:** This keyword is not supported in this release.

```
peer-address ipv4/ipv6_address
```
Displays GTP-U statistics and counters for an existing peer IP address specified in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

```
| { grep grep_options | more }
```
Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of the `grep` and `more` commands, refer to the Regulating a Command’s Output section of the Command Line Interface Reference Guide.

**Usage**

Use this command to view statistics and counters for GTP-U traffic on this system. Refine the statistics display by including a filter with the command.

**Important:** The `show gtpu statistics` command should be given from the local context only; issuing the command from any other context will result in an error message.

**Example**

The following command displays statistics for the GTP-U service named *gtp1*:

```
show gtpu statistics gtpu-service gtp1
```

The following command displays active sessions on all local-addresses categorised by GTPU service:

```
show gtpu local-addresses
```

The following command displays statistics for local GTPU address *168.123.123.1*:

```
show gtpu statistics local-address 168.123.123.1
```
show gtpu-service

Displays configuration information for GPRS Tunneling Protocol user plane (GTP-U) services on this system.

**Product**
ePDG
P-GW
SAEGW
S-GW

**Privilege**
Inspector

**Mode**
Exec
The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
show gtpu-service { all | name service_name } [ | { grep grep_options | more } ]
```

- **all**
  Displays configuration information for all GTP-U services configured on this system.

- **name service_name**
  Displays configuration information for an existing GTP-U service specified an alphanumeric string of 1 through 63 characters.

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of the `grep` and `more` commands, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Reference Guide*.

**Usage**

Use this command to view configuration information for GTP-U services on this system.

**Example**

The following command displays service statistics for the GTP-U service named `gtpu1`:

```
show gtpu-service name gtpu1
```
Chapter 129
Exec Mode show Commands (H-L)

This section includes the commands `show ha-service` through `show lte-policy`.
The Exec Mode is the initial entry point into the command line interface system. Exec mode `show` commands are useful in troubleshooting and basic system monitoring.

Mode

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Important**: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
show ha-service

Displays information on configured Home Agent (HA) services.

**Product**
HA

**Privilege**
Security Administrator Operator, Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

**Syntax**

```
show ha-service { all | name ha_name } [ | { grep grep_options | more } ]
```

- **all**
  - Displays information on all Home Agent services.
- **name ha_name**
  - Displays information for an existing HA service specified as an alphanumeric string of 1 through 63 characters.

```
| { grep grep_options | more }
```

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the Regulating a Command's Output section of the Command Line Interface Overview chapter.

**Usage**
Display home agent service configuration information.

**Example**
The following commands displays information on the HA service `sampleService` and all services, respectively.

```
show ha-service name sampleService
show ha-service all
```
show ha-spi-list

Displays all or a specific Home Agent-Security Parameters Index (HA-SPI) remote address list(s).

Product
HA

Privilege
Security Administrator Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show ha-spi-list { all | name ha_name } [ | { grep grep_options | more } ]

all | name ha_name

all: Displays information on all HA-SPI lists.
name ha_name: Displays information for an existing HA-SPI list specified as an alphanumeric string of 1 through 63 characters.

| { grep grep_options | more }

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage
Display a single or all HA-SPI lists.

Example
The following commands displays information on the HA-SPI list named spi012 and all lists, respectively.

    show ha-spi-list name spi012
    show ha-spi-list all
show hardware

Displays information on the system hardware.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show hardware { card [ card_num ] | inventory | version [ board | diags | fans ] } [ | { grep grep_options | more } ]

card [ card_num ]
Provides the hardware information for all ASR 5x00 cards or the card specified by card_num. card_num must be a value in the range 1 through 48 for the ASR 5000 or 1 through 20 for the ASR 5500 and must refer to an installed card.

inventory
Displays the ASR 5x00 hardware information for all slots in tabular format.

version [ board | diags | fans ]
Displays the CPU information for all ASR 5x00 application cards and fan controller version for the upper and lower fan trays.

board: Only include the CPLD and FPGA version information.
diags: Only include the CFE diagnostics version information.
fans: Show the fan controller versions for the upper and lower fan trays.

| { grep grep_options | more }

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage
Show the hardware information and hardware component versions.

Example
The following displays the hardware information for a card installed in slot 1.

show hardware card 1
The following command displays the hardware inventory for the entire chassis.

```
show hardware inventory
```

The following command results in the display of the CPU version for all application cards displaying only the CPLD and FPGA information.

```
show hardware version board
```

The following command displays VPC virtual card information:

```
show hardware
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show hd raid

Shows the output of the Redundant Array of Independent Disks (RAID) established on the SMCs or FSCs.

**Product**
All

**Privilege**
Security Administrator, Administrator, Administrator, Operator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
show hd raid [ verbose ]
```

**Example**

```
show hd raid verbose
```

⚠️ **Important:** Output descriptions for commands are available in the *Statistics and Counters Reference.*
show hd-storage-policy

Displays Array Configuration Replicator (ACR) counter and statistic information.

Product
HSGW
P-GW
SAEGW
S-GW

Privilege
Inspector

Mode
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show hd-storage-policy { all | counters [ all ] [ name name ] [ verbose ] | name name |
statistics [ all ] [ name name ] [ verbose ] }

all
Displays ACR information for all HD storage policies configured on the system.

counters [ all ] [ name name ] [ verbose ]
all: Displays ACR counter information for all HD storage policies configured on the system.
name name: Displays ACR counter information for an existing HD storage policy specified as an
alphanumeric string of 0 through 63 characters.

statistics [ all ] [ name name ] [ verbose ]
all: Displays ACR statistical information for all HD storage policies configured on the system.
name name: Displays ACR statistical information for an existing HD storage policy specified as an
alphanumeric string of 0 through 63 characters.

verbose
Displays HD storage statistics based on instance.

Usage
Use this command to display ACR counter and statistic information.

Example
The following command displays ACR statistic information for an HD storage policy named pgwsgw:

    show hd-storage-policy statistics name pgwsgw
show henbgw

This command displays HENBGW service related information.

**Product**
HeNB-GW

**Privilege**
Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name# 
```

**Syntax**

```
show henbgw { henb-association [ all | full | henbgw-access-service henbgw_acc_svc_name |
peer-address peer_ip_address | peer-id peer_id_value | summary ] | session [ all |
callid call_id | full [ all | callid call_id | qci qci_value | sl-peer sl_peer_address |
| qci qci_value | sl-peer sl_peer_address | summary [ all | callid call_id | qci qci_value |
sl-peer sl_peer_address ] ] | ue [ all | summary ] [ | { grep grep_options | 
more } ] }
```

- **henb-association**: Displays information about HENB associations.
  - **all**: Displays information for all HENB associations.
  - **full**: Displays all available information for associated display or filter keyword (previous keyword).
- **henbgw-access-service**: Displays information about HENB associations with the specified henbgw access service.
  - **henbgw_acc_svc_name** is a string of size 1 to 63.
- **peer-address**: Displays information about HENB associations with the specified peer.
  - **peer_ip_address** is an IPv4 address, using dotted-decimal notation or an IPv6 address, using xx:yy::zz format.
- **peer-id**: Displays information about HENB associations for the specified peer.
  - **peer_id_value** is an integer value ranging from 0 to 4294967295.
- **summary**: This is the summary of available information for associated display or filter keyword (previous keyword).

**session**

Displays HENBGW sessions.

```
all
```

Displays information for all HENB sessions.
show henbgw

call-id call_id

call-id : This is specific Call Identification Number. This must be followed by call_id, an eight digit HEX number.

full

This command displays information on session state for matching sessions

qci qci_value

qci : This is specific qci value. Displays henbgw sessions for QCI value. This must be followed by qci_value, an integer between 1 and 9.

s1-peer s1_peer_address

s1-peer : This is specific S1 peer. Must be followed by the IPv4 or IPv6 address of a peer eNodeB. 
s1_peer_address is an IPv4 address, using dotted-decimal notation or an IPv6 address, using xx:yy:zz format.

summary

This command displays summary information covering matching sessions.

ue

Displays UE information.

| { grep grep_options | more }

Pipes (sends) the output of this command to the specified command. You must specify a command to which
the output of this command will be sent.

For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the
Command Line Interface Overview chapter.

Usage

Use this command to displays HENBGW service related information.

Example

The following command displays information for all HENB associations:

    show henbgw henb-association all
show henbgw-access-service

This command displays HENBGW ACCESS service related information.

**Product**
HeNB-GW

**Privilege**
Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local] host_name#
```

**Syntax**

```
show henbgw-access-service { all | henb-association { all | csg-id csg_id_value| full | henbgw-access-service henbgw_acc_svc_name | peer-address peer_ip_address | peer-id peer_id_value | summary | tai mcc mcc_val mnc mnc_val tac } | name name | statistics [ henbgw-access-service henbgw_acc_svc_name | miscellaneous [ verbose ] | peer-id peer_id_value | s1ap [ cause | [ verbose ] ] | sctp [ buffer [ sessmgr sessmgr_value ] ] [ verbose ] ] [ | { grep grep_options | more } ]}
```

**henb-association** : Displays information about HENB associations.
- `all` : Displays all HENBGW ACCESS services.
- `csg-id` : Displays information about HENB associations for the specified CSG ID.
  - `csg_id_value` is an integer value between 0 and 4294967295.
- `full` : Displays all available information for associated display or filter keyword (previous keyword).
- `henbgw-access-service` : Displays information about HENB associations with the specified henbgw access service.
  - `henbgw_acc_svc_name` is a string of size 1 to 63.
- `peer-address` : Displays information about HENB associations with the specified peer.
  - `peer_ip_address` is an IPv4 address, using dotted-decimal notation 0 or an IPv6 address, using xx:yy::zz format.
- `peer-id` : Displays information about HENB associations for the specified peer.
  - `peer_id_value` is an integer value ranging from 0 to 4294967295.
- `summary` : This is the summary of available information for associated display or filter keyword (previous keyword).
- `tai` : Displays Mobile Country Code. MCC is a three digit number between 100 to 999.
- `mcc` : Specifies Mobile Country Code. MCC values of 000-099 are Reserved codes.
- `mcc_val` is MCC value. MCC values of 000-099 are Reserved codes.
- `mnc` : Specifies Mobile National Code. MNC
  - `mnc_val` is MCC value. This is two/three digit number between 00 to 999.
- `tac` : Displays information about HENB associations for the specified TAC.
- `miscellaneous` : Displays all available information for associated display or filter keyword (previous keyword).
show henbgw-access-service

name name statistics [ henbgw-access-service henbgw_acc_svc_name | miscellaneous [ verbose ] | peer-id peer_id价值观 slap [ cause | [ verbose ] ] | sctp [ buffer [ sessmgr sessmgr_value

name: Displays information for specific HENBGW ACCESS service name.

name: is a string of size 1 to 63.

statistics: Displays HENBGW ACCESS service statistics

miscellaneous: Displays Miscellaneous statistics.

slap: Displays S1AP statistics.

case: Displays S1AP cause statistics.

sctp: Displays SCTP statistics.

buffer: Displays SCTP TX/RX buffer statistics.

sessmgr: Displays SCTP TX/RX buffer statistics on a specific sessmgr.

verbose: Specifies the verbosity.

| { grep grep_options | more }

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage

Use this command to display HENBGW ACCESS service related information.

Example

The following command displays S1AP statistics:

    show henbgw-access-service statistics slap
show henbgw-network-service

This command displays configuration for HENBGW NETWORK service.

Product
HeNB-GW

Privilege
Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local] host_name#

Syntax

show henbgw-network-service { all | mme-association { all | full | henbgw-network-service henbgw_net_svc_name | peer-address peer_ip_address | peer-id peer_id_value | summary | name name | statistics { henbgw-network-service henbgw_net_svc_name | peer-id peer_id_value | slap cause | [ verbose ] } | sctp buffer { henbgwmgr henbgwmgr_value } | [ verbose ] } [ | { grep grep_options | more } ]

henb-association [ all | csg-id csg_id_value | full | henbgw-access-service henbgw_acc_svc_name | peer-address peer_ip_address | peer-id peer_id_value | summary ] | name name

mme-association : Displays information about MME associations.
all : Displays all HENBGW NETWORK services.
full : Displays all available information for associated display or filter keyword (previous keyword).
henbgw-network-service : Displays information about HENB associations with the specified henbgw access service.
henbgw_net_svc_name is a string of size 1 to 63.
peer-address : Displays information about HENB associations with the specified peer.
peer_ip_address is an IPv4 address, using dotted-decimalnotation or an IPv6 address, using xx:yy::zz format.
peer-id : Displays information about HENB associations for the specified peer.
peer_id_value is an integer value ranging from 0 to 4294967295.
summary : This is the summary of available information for associated display or filter keyword.

name name statistics [ henbgw-network-service henbgw_net_svc_name | peer-id peer_id_value | slap cause | [ verbose ] ] | sctp buffer { henbgwmgr sessmgr_value }

name : Displays information for specific HENBGW NETWORK service name.
name is a string of size 1 to 63.
statistics : Displays statistics for specified object.
slap : Displays S1AP statistics.
cause : Displays S1AP cause statistics.
sctp : Displays SCTP statistics.
buffer : Displays SCTP TX/RX buffer statistics.
henbgwmgr : Displays SCTP TX/RX buffer statistics on a specific henbgwmgr.
verbose : Specifies the verbosity.

| { grep grep_options | more }
Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage
Use this command to display HENBGW NETWORK service related information.

Example
The following command displays S1AP Cause statistics :

    show henbgw-network-service statistics s1ap Cause
show hnbgw access-control-db

Displays the white list of IMSI records in the Access Control database residing on Home-NodeB Gateway (HNB-GW) service instances that control HNB and UE access to HNB-GW sessions.

Product
HNB-GW

Privilege
Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

`show hnbgw access-control-db { hnbgw-service hnbgw_svc_name | imsi imsi_value}`

**hnbgw-service hnbgw_svc_name**

Displays Access Control database records for an existing HNB-GW service specified as an alphanumeric string of 1 through 63 characters.

**imsi imsi_value**

Specifies the International Mobile Subscriber Identification (IMSI) number which is found on the Access Control database for he HNB-GW service. `imsi_value` is an integer consisting of the 3-digit MCC (Mobile Country Code), the 2- or 3-digit MNC (Mobile Network Code) followed by the MSIN (Mobile Subscriber Identification Number). The total IMSI value must not exceed 15 digits.

Usage

This command displays the white list IMSI records in an Access Control database residing on a system support all Home-NodeB Gateway (HNB-GW) service instances. The white list controls HNB and UE access to HNB-GW sessions. Access Control database records can be filtered by IMSI value.

Example

The following command displays the information for registered IMSIs and their status in the HNB-GW database:

```
show hnbgw access-control-db imsi
```

**Important:** Output descriptions for commands are available in the Statistics and Counters Reference.
show hnbgw counters

Displays the session counter information for Home-NodeB Gateway (HNB-GW) services connected on this system.

Product
HNB-GW

Privilege
Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show hnbgw counters [ hnbgw-service hnbgw_svc_name | hnbid hnb_identifier ] [ | { grep grep_options | more }]

hnbgw-service hnbgw_svc_name

Filters the counter display based on an existing HNB-GW service name specified as an alphanumeric string of 1 through 63 characters.

hnbid hnb_identifier

Filters the counter display based on a Home-NodeB identifier specified as an alphanumeric string of 1 through 255 characters.

| { grep grep_options | more }

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of the grep and more commands, refer to the Regulating a Command’s Output section in Command Line Interface Overview chapter.

Usage

Use this command to view the session counter information for HNB-GW services configured and HNBs connected on this system.

Example

The following command displays the counters for the HNB-GW service named hnbgw1:

    show hnbgw counter hnbgw-service hnbgw1

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show hnbgw-global

Displays the global configuration parameters for configured HNB-GW service(s) on this system.

Product
HNB-GW

Privilege
Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show hnbgw-global

Usage
Use this command to view the global configuration parameters set for all HNB-GW service(s) on this system.

Example

The following command displays the global configuration parameters applicable for all HNB-GW services configured on this system:

    show hnbgw-global

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show hnbgw sessions

Displays the active/dormant session information about registered HNB(s) on Home-NodeB Gateway (HNB-GW) service instances configured and running on this system based on different filter criteria.

Product
HNB-GW

Privilege
Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show hnbgw sessions [full | summary] [all] [address hnb_ip_address | cell-id cell_id | hnb-access-mode {closed | hybrid | open} | hnb-local-id hnb_id | hnbgw-service hnbgw_svc_name [ hnb-access-mode { closed | hybrid | open }] | hnbid hnb_glbl_id | mcc mcc | mnc mnc [lac lac | rac rac | rnc rnc]] [ | {grep grep_options | more }]

**full**
Displays the full information for a specific registered HNB session(s) on an HNB-GW service instance running on the system. The display can be filtered based on given filtering criteria.

**summary**
Displays summarized information for a specific registered HNB session(s) on an HNB-GW service instance running on the system. The display can be filtered based on given filtering criteria.

**all**
Displays summarized information for all registered HNB sessions on an HNB-GW service instance running on the system. The display can be filtered based on given filtering criteria.

**address hnb_ip_address**
Filters the display of full or summarized session statistics to show only HNB session(s) based on the registered HNB IP address expressed in IPv4 dotted-decimal notation.

**cell-id cell_id**
Filters the display of full or summarized session statistics to show only HNB session(s) based on the registered Femto cell ID where the user/subscriber is geographically located. and must be an integer from 0 through 268435455. cell_id is an integer from 0 through 268435455.

**hnb-access-mode {closed | open | hybrid}**
Filters the display of full or summarized session statistics to show only HNB session(s) based on the HNB access mode in an HNB-GW service instance.
**show hnbgw sessions**

- **closed** filters the session statistics for closed HNBs connected with HNB-GW service instance in Closed Access mode.
- **hybrid** filters the session statistics for hybrid HNBs connected with HNB-GW service instance in Hybrid Access mode.
- **open** filters the session statistics for open HNBs connected with HNB-GW service instance in Open Access mode.

<table>
<thead>
<tr>
<th><strong>hnb-local-id hnb_id</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Filters the display of full or summarized session statistics to show only HNB session(s) based on the registered local ID of HNB specified as an integer from 1 through 25.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>hnbgw-service hnbgw_svc_name</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Filters the display of session statistics to show only registered HNB session(s) based on an existing HNB-GW service name specified as an alphanumeric string of 1 through 63 characters. This can be further filtered by using access-mode criteria: Closed, Hybrid, or Open.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>hnbid hnb_glbl_id</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Displays summarized or full information of HNB session(s) based on the registered global ID of HNB specified as an integer between 1 through 255.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>mcc mcc</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Displays summary information of HNB session(s) based on the registered Mobile Country Code (MCC) identification number of the UE specified as an integer between 101 through 999.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>mnc mnc</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Displays summarized or full information of HNB session(s) based on the registered Mobile Network Code (MCC) identification number of the UE specified as a 2- or 3-digit integer between 00 through 999.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>lac lac</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Displays summarized or full information for HNB session(s) based on the registered Location Area Code (LAC) identification number of the UE specified as an integer between 1 through 65535.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>rac rac</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Displays summarized or full information for HNB session(s) based on the registered Radio Access Code (RAC) identification number of the UE specified as an integer between 1 through 255.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>rnc rnc</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Displays summarized or full information for HNB session(s) based on the registered Radio Network Code (RAC) identification number of the HNB specified as an integer between 1 through 65535.</td>
</tr>
</tbody>
</table>

| { grep grep_options | more } |
|---------------------|
| Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent. For details on the usage of the **grep** and **more** commands, refer to the Regulating a Command’s Output section in Command Line Interface Overview chapter. |
show hnbgw sessions

Usage
Use this command to view the session statistics of all or specific registered HNB session(s) or in selected part of user session for HNB-GW services configured and running on this system.

Example
The following command displays summarized session statistics for all registered HNBs on the HNB-GW service named hnbgw1:

    show hnbgw sessions summary hnbgw-service hnbgw1

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show hnbgw statistics hnbgw-service

Displays the session statistics for Home-NodeB Gateway (HNB-GW) services configured and running on this system.

**Product**

HNB-GW

**Privilege**

Inspector

**Mode**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
show hnbgw statistics [ gtpu-only ] [ hnb-access-mode { closed | hybrid | open } ] [ hnbgw-service hnbgw_svc_name [ gtpu-only | hnb-access-mode { closed | hybrid | open } ] | hnbap-only | ipne-only | paging-only | ranap-only | rtp-only | rua-only | sabp-only | sctp-only ] ] [ hnbid hnb_identifier ] [ hnbap-only | ranap-only | rua-only | sccp-only | sctp-only ] ] [ verbose] [ | { grep grep_options | more }]
```

- **gtpu-only**
  Displays Forwarded GTPU Pkt statistics for selected HNB/HNBGW Service.

- **hnb-access-mode { closed | hybrid | open }**
  Displays the session statistics of an existing HNB-GW service based on access mode filters. Other supported filters are:
  - **closed**: shows the statistics of only those UEs which are connected through Closed HNBs to the HNB-GW services on a chassis. This command applies to all Closed HNB sessions on a chassis. If any other criteria specified it will filter the statistics based on given criteria.
  - **hybrid**: shows the statistics of only those UEs which are connected through Hybrid HNBs to the HNB-GW services on a chassis. This command applies to all Closed HNB sessions on a chassis. If any other criteria specified it will filter the statistics based on given criteria.
  - **open**: shows the statistics of only those UEs which are connected through Open HNBs to the HNB-GW services on a chassis. This command applies to all Closed HNB sessions on a chassis. If any other criteria specified it will filter the statistics based on given criteria.

- **hnbgw-service hnbgw_svc_name**
  Filters the display of session statistics for an existing HNB-GW service name specified as an alphanumeric string of 1 through 63 characters.

- **hnbap-only**
  Filters the display of session statistics to show only Home NodeB Application Part (HNBAP) traffic for the selected HNB-GW service which is configured and running on this system.
**ranap-only**
Flitters the display of session statistics to show only Radio Access Network Application Protocol (RANAP) traffic for the selected HNB-GW service which is configured and running on this system.

**rua-only**
Filters the display of session statistics to show only RANAP User Adaptation (RUA) traffic for the selected HNB-GW service which is configured and running on this system.

**sccp-only**
Filters the display of session statistics to show only Signaling Connection Control Part (SCCP) traffic for the selected HNB-GW service which is configured and running on this system.

**sctp-only**
Filters the display of session statistics to show only Stream Control Transmission Protocol (SCTP) traffic for selected HNB-GW service which is configured and running on this system.

**verbose**
Displays detailed statistics for all sessions on HNB-GW services or for a selected filtered and named HNB-GW service which is configured and running on this system.

```
| { grep grep_options | more }
```
Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command’s Output* section in *Command Line Interface Overview* chapter.

**Usage**
Use this command to view the session statistics for overall session or in selected part of user session for HNB-GW services configured and running on this system.

**Example**
The following command displays session statistics for the HNAP part of session details for the HNB-GW service named **hnbgw1**:

```
show hnbgw statistics hnbgw-service hnbgw1 hnbap-only
```

The following command displays session statistics for the RANAP part of session with maximum details for the HNB-GW service named **hnbgw1**:

```
show hnbgw statistics hnbgw-service hnbgw1 ranap-only verbose
```
show hnbgw statistics hnbid

Displays the session statistics for Home-NodeB (HNB) connected to an HNB-GW service on this system.

Product
HNB-GW

Privilege
Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show hnbgw statistics hnbid hnb_identifier [ hnbap-only | ranap-only | rua-only] [ verbose] [ | { grep grep_options | more } ]

hnbid hnb_identifier
Filters the display of session statistics based on an existing Home-NodeB identifier specified as an alphanumeric string of 1 through 255 characters.

hnbap-only
Filters the display of session statistics display to show only Home NodeB Application Part (HNBAP) traffic for the selected HNB which is connected to this system through HNB-GW service.

ranap-only
Filters the display of session statistics display to show only Radio Access Network Application Protocol (RANAP) traffic for the selected HNB which is connected to this system through HNB-GW service.

rua-only
Filters the display of session statistics display to show only RANAP User Adaptation (RUA) traffic for the selected HNB which is connected to this system through HNB-GW service.

verbose
Displays detailed statistics for all HNB sessions or for the selected filter and HNB which is connected to this system through HNB-GW service.

| { grep grep_options | more }

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of the grep and more commands, refer to the Regulating a Command’s Output section in the Command Line Interface Overview chapter.
### Usage

Use this command to view the session statistics for overall session or in selected part of user session for selected HNB which is connected to this system through HNB-GW service.

### Example

The following command displays session statistics for the HNBAP part of session details for the HNB identified as `hnb112234` on this system:

```
show hnbgw statistics hnbid hnb112234 hnbap-only
```

The following command displays detailed session statistics for the RANAP part of session details for the HNB identified as `hnb112234` on this system:

```
show hnbgw statistics hnbid hnb112234 ranap-only verbose
```
show hnbgw-service

Displays the configuration details for configured HNB-GW service(s) on this system.

Product
HNB-GW

Privilege
Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show hnbgw-service { all | hnbgw-service hnbgw_svc_name }

all
Displays configuration and other default parameters for all HNB-GW service configured on this system.

hnbgw-service hnbgw_svc_name
Displays configuration and default parameters for an existing HNB-GW service name specified as an alphanumeric string of 1 through 63 characters.

Usage

Use this command to view the configuration and service parameters set for all or any specific HNB-GW service(s) on this system.

Example

The following command displays configuration parameters for all HNB-GW services configured on this system:

show hnbgw-service all

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show hsgw-service

Displays information for HRPD Serving Gateway (HSGW) services on this system.

**Product**
HSGW

**Privilege**
Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

**Syntax**

```
show hsgw-service { all | name service_name | statistics { all | name service_name } } [ dns-stats | pcf-status { address IPv4_address | filter { all | icmp-monitored | no-calls | summary | up } ] ] [ | { grep grep_options | more } ]
```

- **all**
  Displays configuration information for all HSGW services configured on this system.

- **name service_name**
  Displays configuration information for an existing HSGW service specified as an alphanumeric string of 1 through 63 characters.

- **statistics**
  Displays node-level statistics for the HSGW.

- **dns-stats**
  Displays information related to DNS P-GW selection for load balancing using DNS SRV lookup.

- **pcf-status**
  Displays information about the status of Packet Control Functions (PCFs) being monitored.

- **address IPv4_address**
  Displays status information for the specified PCF.
  *IPv4_address* must be specified using IPv4 dotted-decimal notation.

- **filter { all | icmp-monitored | no-calls | summary | up }**
  Filters the PCF status information. Must be followed by the filter to be applied.
  - **all**: Shows all the PCFs.
  - **icmp-monitored**: Shows only PCFs which are ICMP monitored.
  - **no-calls**: Shows only PCFs which has no active sessions.
  - **summary**: Shows only a summary of the status of the PCFs.
**show hsgw-service**

**Usage**

Use this command to view configuration information for HSGW services on this system.

**Example**

The following command displays service statistics for the HSGW service named `hsgw1`:

```
show hsgw-service name hsgw1
```
show hss-peer-service

Displays service, session, and statistics information for Home Subscriber Server (HSS) peer services configured on this system.

**Product**
MME

**Privilege**
Inspector

**Syntax**

```
show hss-peer-service { service { all | name name } | session { all | callid id | full | mdn mdn | nai nai | summary } | statistics { all | service name | summary } } [ | { grep grep_options | more } ]
```

**service { all | name name }**
Displays HSS peer service statistics for HSS peer services configured on this system.
- **all**: Displays HSS peer service statistics for all configured HSS peer services on this system.
- **name name**: Displays HSS peer service statistics for an existing HSS peer service specified as an alphanumeric string of 1 through 63 characters.

**session { all | callid id | full | mdn mdn | nai nai | summary }**
Displays HSS peer service statistics for sessions on this system.
- **all**: Displays HSS peer service statistics for all sessions on this system.
This keyword is also used to further filter the **full** and **summary** options.
- **callid id**: Displays summarized or detailed statistics of HSS peer service sessions running and filtered on the basis of the call identifier specified as an 8-digit hexadecimal number.
This keyword is also used to further filter the **full** and **summary** options.
- **mdn mdn**: Displays summarized or detailed statistics of MME sessions running and filtered on the basis of an existing Mobile Directory Number (MDN) expressed as an alphanumeric string of 1 through 100 characters.
This keyword is also used to further filter the **full** and **summary** options.
- **nai nai**: Displays summarized or detailed statistics of MME-HSS sessions running and filtered on the basis of an existing Network Access Identifier (NAI) expressed as an alphanumeric string of 1 through 128 characters.
This keyword is also used to further filter the **full** and **summary** options.
- **summary**: Displays a summarized output of session information. This keyword can be further filtered by adding the following options:
  - **full**
  - **callid id**
  - **mdn mdn**
  - **nai nai**

**statistics { all | service name | summary }**
Displays statistics for HSS peer services configured on this system.
- **all**: Displays statistics for all HSS peer services configured on this system.
service name: Displays statistics for an existing HSS peer service expressed as an alphanumeric string of 1 through 63 characters.

summary: Displays summarized statistics for all HSS peer services configured on this system.

| { grep grep_options | more }

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of the `grep` and `more` commands, refer to the *Regulating a Command’s Output* section in *CLI Overview* chapter of the *Command Line Interface Reference*.

**Usage**

Use this command to display service, session, and statistics information for HSS peer services configured on this system.

**Example**

The following command displays HSS peer service information and statistics for a session with a call ID of `08f11fa4`:

```
show hss-peer-service sessions full callid 08f11fa4
```
show imei-profile

Displays information for configured International Mobile Equipment Identity (IMEI) profiles.

**Product**
SGSN

**Privilege**
Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

**Syntax**

```
show imei-profile { all | full { all | name imei_name } | name imei_name } [ | { grep grep_options | more } ]
```

- **all**
  Lists all IMEI profiles configured on the system.

- **full { all | name apn_name }**
  - **full**: Instructs the system to display all information in the IMEI profile(s).
  - **all**: Displays a full set of information for all IMEI profiles configured on the system.
  - **name imei_name**: Displays a full set of information for a specific IMEI profile.
  - **apn_name**: Must be an existing IMEI profile expressed as an alphanumeric string of 1 through 64 characters.

- **name imei_name**
  Displays information for a specific IMEI profile expressed as an alphanumeric string of 1 through 64 characters.

  | { grep grep_options | more } |

  Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
  
  For details on the usage of **grep** and **more**, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter.

**Usage**

Use this command to display information for IMEI profiles configured on the system. APN profiles are configured through the global configuration mode and in the IMEI profile configuration mode. For more information regarding IMEI profile commands, refer to the *IMEI Profile Configuration Mode Commands* chapter.

**Example**

The following command displays all available information for an IMEI profile named *imeiprof1*:

```
show imei-profile full name imeiprof1
```
show ims-authorization policy-control

Displays information and statistics specific to the policy control in IP Multimedia Subsystem (IMS) authorization service.

Product

SCM
GGSN
IMS
P-GW
SAEGW

Privilege

Security Administrator, Administrator, Operator, Inspector

Mode

Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show ims-authorization policy-control statistics [ service ims_auth_svc_name | server { ip-address ip_address [ port port_value ] | name server_name } ] [ | { grep grep_options | more } ]

| statistics
Displays the total collected statistics of all policy control parameters of IMS authorization service sessions since the last system restart or clear command.

| service ims_auth_svc_name
Displays the total collected statistics of all IMS authorization sessions processed by a specific IMS authorization service since the last system restart or clear command. ims_auth_svc_name must be an existing IMS authorization service name, expressed as an alphanumeric string of 1 through 64 characters.

| server { ip-address ip_address [ port port_value ] | name server_name }
Displays the server-level message statistics and the server IP address. Specify the PCRF server name (1 through 64 alphanumeric characters), or server IP address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

| | { grep grep_options | more }

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.
**Usage**

Use this command to display information and statistics about policy control configuration in existing IMS authorization services.

**Example**

The following command displays the existing IMS authorization service name `ims_auth_gx1` on the system:

```
show ims-authorization policy-control statistics service ims_auth_gx1
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show ims-authorization policy-gate

Displays information of installed Policy Gates for specific subscriber in an IP Multimedia Subsystem (IMS) authorization (IMSA) service.

Product
SCM
GGSN
IMS
P-GW
SAEGW

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show ims-authorization policy-gate { { status [ summary | full ] [ { imsi imsi_value [ nsapi nsapi_value ] } | callid call_id | { ims-auth-service ims_auth_svc } [ rulename rule_name ] } | { counters [ all | { imsi imsi_value [ nsapi nsapi_value ] } | { rulename rule_name} | { callid call_id } ] } | { grep grep_options | more } ] ],

status [ summary | full ]
Displays the status of the installed policy gates and their flow definitions along with the run-time status in an IMS authorization service based on the specified criteria.
summary: Limits the display to a summary on the status of the installed policy gates and their flow definitions along with their run-time status in an IMS authorization service based on the specified criteria.
full: Displays the full information on status of the installed policy gates and their flow definitions along with their run-time status in an IMS authorization service based on the specified criteria.

counters all
Displays the counters/statistics of the installed policy gates and their flow definitions along with their run-time status in an IMS authorization service based on the specified criteria.
aall displays all counters of the installed gates and their flow definitions along with their run-time status in an IMS authorization service based on the specified criteria.

imsi imsi_value [ nsapi nsapi_value ]
Displays all of the counters/status of the installed policy gates and their flow definitions along with the run-time status in an IMS authorization service based on the International Mobile Subscriber Identity (IMSI).
nsapi nsapi_value specifies the Network Service Access Point Identifier (NSAPI) and limits the display to a single PDP context of the subscriber.
**callid** `call_id`

Displays all of the counters/status of the installed policy gates and their flow definitions along with their run-time status in an IMS authorization service based on the call identifier.

**ims-auth-service** `ims_auth_svc`

Displays the status of the installed policy gates and their flow definitions along with their run-time status in the named IMS authorization service.

**rulename** `rule_name`

Displays all of the counters/status of the installed policy gates and their flow definitions along with their run-time status in an IMS authorization service based on the named dynamic charging rule.

```
| { grep grep_options | more }
```

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent. Please refer to the *Regulating a Command’s Output* section of the *Command Line Interface Reference* for details on the usage of `grep` and `more`.

**Usage**

Use this command to display information/statistics/counter about all of the installed policy gates and their flow definitions along with the run-time status with specified criteria and filters in existing IMS authorization services.

**Example**

The following command displays the full status of the installed policy gates in an existing IMS authorization service on the system:

```
show ims-authorization policy-gate status full
```

The following command displays the all counters of the installed policy gates in an existing IMS authorization service on the system:

```
show ims-authorization policy-gate counters all
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show ims-authorization servers

Displays information and statistics specific to the authorization servers used for IP Multimedia Subsystem (IMS) authorization (IMSA) service.

Product
SCM
GGSN
IMS
P-GW
SAEGW

Privilege
Security Administrator, Administrator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show ims-authorization servers [ ims-auth-service ims_auth_svc_name [ | { grep grep_options | more } ] ]

server [ ims-auth-service ims_auth_svc_name ]
Displays the information and statistics for all authorization servers configured within an IMS authorization service in a system.
ims-auth-service ims_auth_svc_name: Displays the configured authorization servers for IMS authorization within the named IMS authorization service.

| { grep grep_options | more }
Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
Please refer to the Regulating a Command’s Output section of the Command Line Interface Reference for details on the usage of grep and more.

Usage

Use this command to display information and statistics about IMS authorization servers configured on a system or IMS authorization service.

Example

The following command displays the information and statistics of the authorization servers in the IMS authorization service named in ims_auth_gx1:

show ims-authorization servers ims-auth-service ims_auth_gx1

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show ims-authorization service

Displays information, configuration, and statistics of all/specific IP Multimedia Subsystem (IMS) authorization (IMSA) service.

Product
GGSN
P-GW
SAEGW
SCM

Privilege
Security Administrator, Administrator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show ims-authorization service { { all [ verbose ] | name ims_auth_svc_name [ p-cscf { all | ip_address ipv4/ipv6_address | summary } } | { statistics [ all | name ims_auth_svc_name ] [ verbose ] } [ | { grep grep_options | more } ] }

- **all [ verbose ]**
  
  Displays information and configuration for all configured IMS authorization services with a single line of information for each IMS authorization service.
  
  **verbose**: Displays all information and configuration data for all IMS authorization services configured on system.

- **name ims_auth_svc_name [ p-cscf { all | ip_address ipv4/ipv6_address }**
  
  Displays the information, statistics, and configuration data for the named IMS authorization service. If the optional keyword is configured, this command displays the statistics information of all P-CSCF servers or specific server.

- **summary**
  
  Displays summarized information and configuration data for all IMS authorization services configured in a system.

- **statistics [ all | name ims_auth_svc_name ] [ verbose ]**
  
  Displays the IMS Authorization service statistics including following information:
  
  - Initial authorization procedures
  - Re-authorization procedures initiated by us
  - Re-authorization procedures initiated by servers
  - Various failure statistics
If no criteria are specified, only summarized statistics for all IMS Authorization services are displayed:

- **all**: displays individual statistics for every IMS authorization service configured on system.
- **name ims_auth_svc_name**: Displays the statistics for the IMS authorization service named in
  `ims_auth_svc_name`
- **verbose**: displays detailed statistics for a configured IMS authorization service.

```
| { grep grep_options | more }
```

Pipes (sends) the output of this command to the specified command. You must specify a command to which
the output of this command will be sent. Please refer to the *Regulating a Command’s Output* section of the *Command Line Interface Reference* for
details on the usage of *grep* and *more*.

### Usage

Use this command to display the status, counters and configuration for an IMS Authorization service. The
status includes the state of a server table switchover. The Statistics option displays information about various
processes.

### Example

The following command displays the information and configuration data of the IMS authorization service
named in *ims_auth_gx1*:

```
show ims-authorization service name ims_auth_gx1
```

![Important: Output descriptions for commands are available in the *Statistics and Counters Reference.*]
show ims-authorization sessions

Displays information, configuration, and statistics of sessions active in an IP Multimedia Subsystem (IMS) authorization (IMSA) service.

Product
SCM
GGSN
IMS
P-GW
SAEGW

Privilege
Security Administrator, Administrator

Mode
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax
show ims-authorization sessions [ all | apn apn_name | callid call_id | full | ggsn-only | ims-auth-service ims_auth_svc_name | imsi imsi_value [ nsapi nsapi_value ]| ip-address ip_address | summary ] [ | { grep grep_options | more } ] ]

all
Displays information and configuration for all sessions running in IMS authorization services with a single line of information for each IMS authorization session.

apn apn_name
Displays all of the counters/status for the running services in an IMS authorization service based on the specified Access Point Name (APN).

callid call_id
Displays all of the counters/status for the running services in IMS authorization service based on the named call identifier.

full
Displays complete information and configuration data for all sessions in IMS authorization services configured in a system.

ggsn-only
Displays GGSN-specific information in addition to detailed information about the session.
show ims-authorization sessions

ims-auth-service ims_auth_svc_name
Displays the information, statistics, and configuration data for sessions in the named IMS authorization service.

imsi imsi_value [ nsapi nsapi_value ]
Displays all of the counters/status of the running services in an IMS authorization service based on the specified International Mobile Subscriber Identity (IMSI) and Network Service Access Point Identifier (NSAPI). The display is limited to a single PDP context of the subscriber.

ip-address ip_address
Displays all of the counters/status for the running services in IMS authorization service based on the specified host IP address.

summary
Displays summarized information and configuration data for all IMS authorization services configured in a system.

| { grep grep_options | more }
Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent. Please refer to the Regulating a Command’s Output section of the Command Line Interface Reference for details on the usage of grep and more.

Usage
Use this command to display the sessions running under IMS Authorization service on a system with different filter criteria.

Example
The following command displays the information and statistical data for a session in an IMS authorization service:

    show ims-authorization sessions full

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show inventory

Displays Unique Device Identifier (UDI) information for all hardware in the system for which a UDI is available.

**Product**
All

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Mode**
Exec
The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
show inventory [ | { grep grep_options | more } ]
```

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of the `grep` and `more` commands, refer to the *Regulating a Command’s Output* section in the *Command Line Interface Overview* chapter.

**Usage**
Displays UDI information (card/item description, Cisco PID, serial number) for all hardware installed in this system.

**Example**
The following command displays UDI information for all cards in the system:

```
show inventory
```
show ip access-group statistics

Displays statistics for each rule in an access control group.

**Product**

HA

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Mode**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
show ip access-group statistics [ | { grep grep_options | more } ]
```

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of `grep` and `more`, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter.

**Usage**

Use this command to display the configured access control groups in the current context.

**Example**

The following command displays the contents of an access control group named `ACG_4`:

```
show ip access-list ACG_4
```
show ip access-list

Displays the information for all Access Control Lists (ACLs) or the named ACL. With no keyword supplied, a list of all access lists and their entries is displayed.

**Product**
HA

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

**Syntax**

```
show ip access-list list_name [ | { grep grep_options | more } ]
```

<table>
<thead>
<tr>
<th>list_name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the name of an existing ACL configured in the current context as an alphanumeric string of 1 through 47 characters.</td>
</tr>
</tbody>
</table>

| | { grep grep_options | more } |
|-------------------|-------------------|
| Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent. |
| For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter. |

**Usage**

Use this command to display the configured ACLs in the current context.

**Example**

The following command displays the contents of an ACL named ACL_4:

```
show ip access-list ACL_4
```
show ip arp

Displays the ARP table or the ARP information associated with the specified IP address.

**Important:** When it restarts, the VPN Manager removes all interfaces from the kernel; the kernel then removes all ARP entries. When this happens, the NPU still holds all of the ARP entries so that there is no traffic disruption. From a user point of view, `show ip arp` is broken since this command gathers information from the kernel and not the NPU.

**Product**

HA

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Mode**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
show ip arp [ ip_address | vrf vrf_name ] [ | { grep grep_options | more } ]
```

- `ip_address`
  Specifies an IP address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

- `vrf vrf_name`
  Displays information for an existing VPN Routing and Forwarding (VRF) name expressed as an alphanumeric string of 1 through 63 characters.

- `| { grep grep_options | more }`
  Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
  For details on the usage of `grep` and `more`, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

**Usage**

Use this command to display the configured ACLs in the current context.

**Example**

The following command displays the contents of an ACL named `ACL_4`:

```
show ip access-list ACL_4
```
show ip as-path-access-list

Displays the contents of a Border Gateway Protocol (BGP) router Autonomous System (AS) path access list in the current context.

Product
- HA

Privilege
- Security Administrator, Administrator, Operator, Inspector

Mode
- Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

```bash
show ip as-path-access-list list_name [ | { grep grep_options | more } ]
```

- `list_name`
  Specifies the name of an existing AS path access list configured in the current context as an alphanumeric string of 1 through 79 characters.

- `| { grep grep_options | more }`
  Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
  For details on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage

Use this command to display the configured entries for the specified BGP router AS path access list in the current context.

Example

The following command displays the contents of an AS path access list named `ASlist1`:

```bash
show ip as-path-access-list ASlist1
```
show ip bgp

Displays Border Gateway Protocol (BGP) information for the current context.

Product
HA

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show ip bgp [ ip_address/mask | debugging | filter-list list_name | neighbors [ ip_address ] | route-map map_name | vpnv4 [ all [ ip_address/mask | neighbors | summary ] | route-distinguisher { ipv4_address | asn_value } rd_value | vrf vrf_name [ ip_address/mask | neighbors | summary ] | vpnv6 [ all [ ipv4_address | neighbors | summary ] | route-distinguisher { ipv4_address | asn_value } rd_value | vrf vrf-name [ ip_address/mask | neighbors | summary ] ] [ | { grep grep_options | more } ]

ip_address/mask

Specifies the IP address and netmask bits for the network for which information should be displayed. The IP address and mask is the number of subnet bits, representing a subnet mask in CIDR notation. These must be entered in the IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal CIDR notation.

d Debugging

Displays debug flags that are enabled.

filter-list list_name

Displays routes that match the specified filter list.

neighbors [ip_address]

Displays information for all neighbors or a neighbor specified as an IP address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

route-map map_name

Displays routes that match the specified route-map.

summary

Displays summary BGP information.
Exec Mode show Commands (H-L)

show ip bgp

Displays all VPNv4 routing data.

- **all**: Displays all VPNv4 routing information. If this is specified, the information displayed is gathered from all the VRFs known to BGP and displayed. It could contain the list of neighbors, the list of networks, or a particular network.

- **neighbors**: Displays neighbor information for the all the VRFs including the default VRF or for the VRF with a matching RD value.

- **summary**: Displays summary information of neighbors for all the VRFs including the default VRF or for the VRF with a matching RD value.

- **route-distinguisher { ipv4_address | asn_value } rd_value**: Displays information about the route distinguisher. Where
  - **ipv4_address**: Specifies an IP address in IPv4 dotted-decimal notation.
  - **asn_value**: Specifies an autonomous system number as an integer from 0 through 65535.
  - **rd_value**: Specifies a route distinguisher value as an integer from 0 through 4294967295.

- **vrf vrf_name [ ipv4_address/mask | neighbors | summary ]**: Displays information about the VRF. Where
  - **vrf_name**: Specifies the name of the VRF as an alphanumeric string of 1 through 63 characters.
  - **ipv4_address/mask**: Specifies an IP address in IPv4 dotted-decimal CIDR notation.
  - **neighbors**: Displays neighbor information for the all the VRFs including the default VRF or for the VRF with a matching RD value.
  - **summary**: Displays summary information of neighbors for all the VRFs including the default VRF or for the VRF with a matching RD value.

show vpnv6

Displays all VPNv6 routing data.

- **all**: Displays all VPNv6 routing information. If this is specified, the information displayed is gathered from all the VRFs known to BGP and displayed. It could contain the list of neighbors, the list of networks, or a particular network.

- **neighbors**: Displays neighbor information for the all the VRFs including the default VRF or for the VRF with a matching RD value.

- **summary**: Displays summary information of neighbors for all the VRFs including the default VRF or for the VRF with a matching RD value.

- **route-distinguisher { ipv4_address | asn_value } rd_value**: Displays information about the route distinguisher. Where
  - **ipv4_address**: Specifies an IP address in IPv4 dotted-decimal notation.
  - **asn_value**: Specifies an autonomous system number as an integer from 0 through 65535.
  - **rd_value**: Specifies a route distinguisher value as an integer from 0 through 4294967295.
**show ip bgp**

*`vrf vrf_name [ ipv4_address/mask | neighbors | summary ]`*: Displays information about the VRF. Where

  *`vrf_name`*: Specifies the name of the VRF as an alphanumeric string of 1 through 63 characters.

  *`ipv4_address/mask`*: Specifies an IP address in IPv4 dotted-decimal CIDR notation.

  *`neighbors`*: Displays neighbor information for all the VRFs including the default VRF or for the VRF with a matching RD value.

  *`summary`*: Displays summary information of neighbors for all the VRFs including the default VRF or for the VRF with a matching RD value.

```
| { grep grep_options | more }
```

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of `grep` and `more`, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter.

---

**Usage**

Use this command display to BGP information for the current context.

**Example**

The following command displays information for all BGP neighbors:

```
show ip bgp neighbors
```
show ip igmp group

Displays Internet Group Management Protocol (IGMP) information for all groups in a context or a specific IP address.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show ip igmp group [ ip_address | all ] [ | { grep grep_options | more } ]

- **ip_address**
  Displays IGMP information for the IP address specified in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

- **all**
  Displays information for all IGMP groups associated with this context.

| { grep grep_options | more } |

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter.

Usage

Use this command to display IGMP group information.

Example

To display general IGMP information for all groups in this context, enter the following command;

```
show ip igmp all
```
show ip interface

Displays statistical and configuration information for the IPv4-based interfaces, including a Virtual Routing and Forwarding (VRF) table for a specific context.

**Product**
All

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name# show ip interface
```

**Syntax**

```
show ip interface [ vrf vrf-name ] [ name intfc_name [ tunnel [ gre-keepalive ] ] [ summary ] [ vrf vrf-name ] [ | { grep grep_options | more } ]
```

- `name intfc_name`
  Displays information for an existing interface specified as an alphanumeric string of 1 through 79 characters. If no interface name is specified, the information for all IP interfaces is displayed.

- `summary`
  Displays summarized information about requested IP interfaces.

- `tunnel [ gre-keepalive ]`
  Filters the IP interface information for GRE/IP-in-IP tunnel type interfaces.
  `gre-keepalive`: Displays the keepalive information for a generic routing encapsulation (GRE) tunnel configured with this IP interface.

- `vrf vrf_name`
  Displays Virtual Routing and Forwarding (VRF) routing information for an existing VRF specified as an alphanumeric string of 1 through 63 characters.

- `| { grep grep_options | more }`
  Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
  For details on the usage of `grep` and `more`, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter.

**Usage**

Use this command to display the summarized of detailed configuration and statistical information for a configured IP interface. This information can be used to verify and/or troubleshoot communication difficulties between to a remote host/node.
Example

The following command displays the interface information, including statistics, for the IP interface Interface_1.

```
show ip interface Interface_1 statistics
```

The following command displays the GRE keepalive information for an IP interface named in IP_gre1.

```
show ip interface IP_gre1 tunnel gre-keepalive
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*. 

---

Cisco ASR 5x00 Command Line Interface Reference
show ip ipsp

Displays the names of IP pools that are enabled for the IP pool sharing protocol (IPSP) and lists the disposition of addresses in the pools.

Product

PDSN
HA
ASN-GW

Privilege

Security Administrator, Administrator, Operator, Inspector

Mode

Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show ip ipsp [ summary ] [ | { grep grep_options | more } ]

summary

Displays only the disposition of the addresses in the participating IP pools. Does not show the names of the participating IP pools.

| { grep grep_options | more }

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage

Use this command to list the names of IP pools that are participating in the IPSP and list the disposition of IP addresses in those pools.

Important: For information on configuring and using IPSP refer to the System Administration Guide.

Example

To list information on all IPSP participating pools and address disposition, enter the following command:

    show ip ipsp

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show ip localhosts

Displays host name to IP address mapping for current context. Must be followed by a specific IP host name.

Product
PDSL
HA
GGSN

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show ip localhosts hostname [ | { grep grep_options | more }

hostname
Specifies a configured hostname as an alphanumeric string of 1 through 127 characters.

| { grep grep_options | more }
Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent. For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage
Use this command to display mappings of a host name to IP addresses.

Example
To display IP address mapping for host name local_2345, enter the following command;

    show ip localhosts local_2345
**show ip ospf**

Displays Open Shortest Path First (OSPF) routing information.

**Product**
- PDSN
- HA
- GGSN

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
show ip ospf [ border-routers | database [ verbose ] [ ls-id ip_addr ] [ adv-router ip_addr ] [ ls-type { router | network | summary | asbr-summary | external | nssa | integer } ] | debugging | interface | neighbor [ details ] | route | virtual-links ] [ | { grep grep_options | more } ]
```

<table>
<thead>
<tr>
<th><strong>border-routers</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Displays all known area border routers (ABRs) and autonomous system border routers (ASBRs) for OSPF.</td>
</tr>
</tbody>
</table>

| **database [ verbose ] [ ls-id ip_addr ] [ adv-router ip_addr ] [ ls-type { router | network | summary | asbr-summary | external | nssa | integer } ]** |
|---------------------------------------------------------------|
| Displays a summary of the database information for OSPF.       |
| **verbose:** Displays detailed OSPF database information.      |
| **ls-id ip_addr:** Displays OSPF database information for the link state advertisements (LSAs) with the specified link state identifier (LSID). ip_addr is entered using IPv4 dotted-decimal notation. |
| **adv-router ip_addr:** Displays OSPF database information for the advertising router with the specified LSID. ip_addr is entered using IPv4 dotted-decimal notation. |
| **ls-type { router | network | summary | asbr-summary | external | nssa | LSA_Numerical_Type }** : Displays OSPF database information for the specified LSA type. |

<table>
<thead>
<tr>
<th><strong>debugging</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Lists which debugging parameters are enabled.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>interface</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Displays interface information for OSPF.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>neighbor [ details ]</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Displays summarized information about all known OSPF neighbors.</td>
</tr>
<tr>
<td><strong>details:</strong> Displays detailed information about all known OSPF neighbors.</td>
</tr>
</tbody>
</table>
**route [ summary ]**

Displays the OSPF routing table.

**summary**: Displays the number of intra-area, inter-area, external-1 and external-2 routes.

**virtual-links**

Displays the OSPF virtual links.

```
| { grep grep_options | more }
```

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

**Usage**

Use this command to display OSPF information.

**Example**

To display general OSPF information, enter the following command;

```
show ip ospf
```
show ip policy-forward

Displays information for IP packet redirecting policy for Home Agent (HA).

**Product**  
All

**Privilege**  
Security Administrator, Administrator, Operator, Inspector

**Mode**  
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
show ip policy-forward [ | { grep grep_options | more } ]
```

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of `grep` and `more`, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter.

**Usage**

Use this command to see all the settings for IP packet redirection configuration from existing HA to new HA during upgrade.

**Important:** This is a customer specific command.

**Example**

The following command displays forward policy configuration for an HA:

```
show ip policy-forward
```
show ip pool

Displays statistics specific to IP pools.

Product
- PDSN
- GGSN
- HA
- ASN-GW
- A-BG

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show ip pool [ address { pool-name pool_name | group-name group_name } { used | free | hold | release } [ limit limit ] | group-name group_name | groups | hold-timer { imsi imsi | msid msid | username username [ imsi imsi | msid msid ] } | many-to-one | nat-realm | one-to-one | overlap | pool-name pool_name | private | public | resource | static | summary | verbose | wide ] [ | { grep grep_options | more }]

address { pool-name pool_name | group-name group_name } { used | free | hold | release} [ limit limit ]

Displays IP pool addresses for the specified IP pool or pool group that are currently in the specified state.

pool-name pool_name: Displays IP addresses from an existing IP pool name specified as an alphanumeric string of 1 through 31 characters.

group-name group_name: Displays IP addresses from an existing IP pool group name specified as an alphanumeric string of 1 through 31 characters.

used: Displays the IP addresses that are in a used state.
free: Displays the IP addresses that are in a free state.
hold: Displays the IP addresses that are in a hold state.
release: Displays the IP addresses that are in a release state.

limit limit: Specifies the maximum number of address to display as an integer from 1 through 524287.

group-name group_name

Displays information about an existing IP pool group name specified as an alphanumeric string of 1 through 31 characters.

groups

Lists information about all IP pool groups.
**hold-timer** {imsi imsi | msid msid | username username [imsi imsi | msid msid]}

Displays hold timer address information for the specified IMSI, MSID, or username.

- **imsi imsi**: Displays hold-timer information for a valid IMSI (International Mobile Subscriber Identity), specified as a 15-character field that identifies the subscriber’s home country and carrier.
- **msid msid**: Displays hold-timer information for the MSID specified as a number from 7 through 16 digits.
- **username username**: Displays hold-timer information for an existing username specified as an alphanumeric string of 1 through 127 characters.

**Important**: Active users cannot be displayed. If an active ID or username is entered, the following error message appears: Failure: No address matching the specified information was found! Please confirm that the options used match the network architecture/deployment, i.e. IMSI/MSID only, Username only, or IMSI/MSID plus Username. Please note that this command does not apply for addresses in the used state.

<table>
<thead>
<tr>
<th>many-to-one</th>
<th>Lists information on Many-to-One NAT Realm IP address pools.</th>
</tr>
</thead>
<tbody>
<tr>
<td>nat-realm</td>
<td>Lists information on NAT Realm IP address pools.</td>
</tr>
<tr>
<td>one-to-one</td>
<td>Lists information One-to-One NAT Realm IP address pools.</td>
</tr>
<tr>
<td>overlap</td>
<td>Lists information on overlapping IP pools.</td>
</tr>
<tr>
<td>pool-name pool_name</td>
<td>Displays information about an existing IP pool.</td>
</tr>
<tr>
<td>private</td>
<td>Displays information about IP pools marked Private.</td>
</tr>
<tr>
<td>public</td>
<td>Displays information about IP pools marked Public.</td>
</tr>
<tr>
<td>resource</td>
<td>Displays information about resource IP pools.</td>
</tr>
<tr>
<td>static</td>
<td>Displays information about static IP pools.</td>
</tr>
<tr>
<td>summary</td>
<td>Displays a summary of all IP pool information.</td>
</tr>
<tr>
<td>verbose</td>
<td>Displays detailed information about all IP pools.</td>
</tr>
</tbody>
</table>
show ip pool

Usage
Use this command to display statistics pertaining to IP Pools in the current context.

Example
The following command displays IP address information for an IP Pool named pool1:

    show ip pool address pool-name pool

To display a summary list for all IP pools in the current context, enter the following command:

    show ip pool summary

The following command displays IP pool information for all IP pools configured in the current context:

    show ip pool verbose

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show ip prefix-list

Displays IP prefix lists used to filter routes. With no keyword supplied, a list of all prefix lists and their entries is displayed.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

```
show ip prefix-list [ detail | name | summary ] list_name [ | { grep grep_options | more }
```

<table>
<thead>
<tr>
<th>detail</th>
<th>Displays detailed information for the named prefix list.</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Displays information for the named prefix list.</td>
</tr>
<tr>
<td>summary</td>
<td>Displays summary information for the named prefix list.</td>
</tr>
<tr>
<td>list_name</td>
<td>Specifies the name of an existing prefix list as an alphanumeric string of 1 through 79 characters.</td>
</tr>
</tbody>
</table>

| | { grep grep_options | more }
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Pipe (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent. For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.</td>
<td></td>
</tr>
</tbody>
</table>

Usage

Use this command to display information about IP prefix lists.

Example

To display detailed information about a prefix list named route_101, enter the following command:

```
show ip prefix-list detail route_101
```
**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*.
show ip route

Displays information related to currently configured static or VRF routes for the current context.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show ip route [ ip_address/mask | vrf vrf_name ] [ | { grep grep_options | more }]

ip_address/mask
Specifies an IP address/mask (CIDR) for a static route in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

| vrf vrf_name
Displays information for an existing Virtual Routing and Forwarding (VRF) name expressed as an alphanumeric string of 1 through 63 characters.

| { grep grep_options | more }
Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage
Use this command to display information about IP prefix lists.

Example
To display detailed information about a prefix list named route_101, enter the following command:

    show ip prefix-list detail route_101

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show ip route-access-list

Displays information related to currently configured route-access-list used to filter routes.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show ip route-access-list [ name] [ | { grep grep_options | more ]

name
Specifies the name of an existing route access list as an alphanumeric string of 1 through 79 characters.

| { grep grep_options | more }

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage
Use this command to display information about IP route access lists.

Example
To display detailed information about an access list named access_route_3, enter the following command:

show ip route-access-list accesss_route_3

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show ip static-route

Displays information related to currently configured static routes.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

```plaintext
show ip static route [ip_address/mask] | { grep grep_options | more }
```

<table>
<thead>
<tr>
<th>ip_address/mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies an IP address/mask (CIDR) for a static route in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.</td>
</tr>
</tbody>
</table>

| | { grep grep_options | more } |
|---|---|
| Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent. |
| For details on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter. |

Usage

Use this command to display information about IP static routes.

Example

To display detailed information about route 192.155.33.2/24, enter the following command:

```plaintext
show ip static route 192.155.33.2/24
```

**Important:** Output descriptions for commands are available in the Statistics and Counters Reference.
show ip vrf

Displays configuration information for VPN Routing and Forwarding instances.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

```
show ip vrf [ vrf_name [mpls-map-dscp-exp] ]] | { grep grep_options | more }
```

**vrf_name**
Specifies an existing VRF name as an alphanumeric string of 1 through 63 characters.

**mpls-map-dscp-exp**
Displays the MPLS mapping for the VRF.

Usage

Use this command to display information about VFR names.

Example

To display information for a VRF named corporate_range2 with MPLS mapping:

```
show ip vfr corporate_range2 mpls-map-dscp-exp
```

**Important:**  Output descriptions for commands are available in the Statistics and Counters Reference.
show ip vrf-list

Displays configuration information for VRF lists currently on the system.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show ip vrf-list [ list_name ]

  list_name

  Specifies the name of an existing VRF list as an alphanumerical string of 1 through 63 characters.

Usage

Use this command to display information about all VRF lists or a specified VRF list.

Example

The following command displays information about all VRF lists in the system:

    show ip vrf-list
show ipms status

Displays the status of Intelligent Packet Monitoring System (IPMS) client service with information related to system and call events. It also displays the status of configured IPMS servers.

Product
IPMS

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show ipms status [ summary | all | server address ip_address ]

summary
Displays the summary of all configured IPMS client and IPMS servers.

all
Displays information for all configured IPMS client and IPMS servers.

server address ip_address
Displays status for the IPMS server specified as an IP address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

Usage
This command is used to show/verify the status or configuration of one or all IPMS server along with system and call event information.

Example
The following command displays status of an IPMS server with IP address 10.2.3.4:

show ipms status server address 10.2.3.4
show ipsg service

Displays IP Service Gateway (IPSG) service information.

**Product**
eWAG
IPSG

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Mode**
Exec
The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
show ipsg service { all [ [ verbose ] counters ] | name ipsg_service_name [ counters ] } [ | { grep grep_options | more } ]
```

- **all [ [ verbose ] counters ]**
  - Displays information for all IPSG service(s) configured on the system.
  - `verbose`: Specifies to display detailed information.
  - `counters`: Specifies to display counters associated with IPSG services.

- **name ipsg_service_name [ counters ]**
  - Displays information for the specified IPSG service.
  - `name ipsg_service_name`: Specifies name of the IPSG service. `ipsg_service_name` must be an alphanumeric string of 1 through 63 characters.
  - `counters`: Specifies to display counters associated with IPSG services.

- **| { grep grep_options | more }**
  - Specifies to pipe (send) the output of this command to the specified command. You must specify a command to which the output of this command should be sent.
  - For details on the usage of `grep` and `more`, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter.

**Usage**

Use this command to view information for all or a specific IPSG service.

**Example**

The following command displays information for all IPSG services configured on the system:

```
show ipsg service all
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show ipsg sessions

Displays IP Service Gateway (IPSG) session information.

**Product**
- eWAG
- IPSG

**Privilege**
- Security Administrator, Administrator, Operator, Inspector

**Mode**
- Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
show ipsg sessions [ counters | full | summary ] [ all | callid call_id | ip-address ipv4_address | msid msid_number | peer-address ipv4_address | username user_name ] [ | { grep grep_options | more } ]
```

- **counters**
  Displays session counters for matching sessions.

- **full**
  Displays all available information for matching sessions.

- **summary**
  Displays a summary of available information for matching sessions.

- **all**
  Displays session information including call ID, NAI, and home address for all current IPSG sessions. This is the default behavior for the `show ipsg sessions` command.

- **callid call_id**
  Displays session information for a current IPSG session based on the specified call ID. `call_id` must be an 8-digit hexadecimal number.

- **ip-address ipv4_address**
  Displays session information for a specific IPSG session based on the subscriber IP address. `ipv4_address` must be specified in IPv4 dotted-decimal notation.

- **msid msid_number**
  Displays session information for a current IPSG session based on the specified MSID. `msid_number` must be an 8-digit hexadecimal number.
peer-address ipv4_address
Displays session information for a current IPSG session based on the IP address of the device sending the RADIUS accounting messages.
ipv4_address must be specified in IPv4 dotted-decimal notation.

username user_name
Displays session information for an IPSG session based on subscriber’s user name.
user_name must be an alphanumeric string of 1 through 127 characters.

| { grep grep_options | more }
Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage
Use this command to view IPSG session information.

Example
The following command displays all the existing IPSG service sessions on the system:

```
show ipsg session all
```

**Important:** Output descriptions for commands are available in the Statistics and Counters Reference.
show ipsg statistics

Displays IP Services Gateway (IPSG) service statistics.

**Product**
eWAG
IPSG

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Mode**
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

**Syntax**

```
show ipsg statistics [ name ipsg_service_name | peer-address ipv4_address ] [ | { grep grep_options | more } ]
```

- **name ipsg_service_name**
  Displays cumulative statistics of all IPSG sessions processed by the specified service since the last system restart or clear command.
  `ipsg_service_name` must be the name of an IPSG service, and must be an alphanumeric string of 1 through 63 characters.

- **peer-address ipv4_address**
  Displays cumulative statistics of all IPSG sessions associated with the specified IP address of the device sending the RADIUS accounting messages. The statistics displayed are from the last system restart or clear command.
  `ipv4_address` must be specified in IPv4 dotted-decimal notation.

|  | { grep grep_options | more } |
|---|---|
| Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent. For details on the usage of `grep` and `more`, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter.

**Usage**

Use this command to view IPSG service statistics.

**Example**

The following command displays cumulative IPSG session statistics on the system:

```
show ipsg statistics
```

The following command displays the cumulative IPSG session statistics for an IPSG service named `ipsg1`:
show ipsg statistics name ipsg1

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show ipv6 access-group statistics

Displays statistics for each rule in all IPv6 access groups or a specified IPv6 access control group.

Product
HA

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show ipv6 access-group statistics [ | { grep grep_options | more } ]

| { grep grep_options | more }
Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent. For details on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage

Use this command to display the configured IPv6 access control groups in the current context.

Example

The following command displays the contents of an IPv6 access control group named ACGv6_4:

```
show ipv6 access-group ACGv6_4
```
show ipv6 access-list

Displays the information for all IPv6 Access Control Lists (ACLs) or the named ACL. With no keyword supplied, a list of all access lists and their entries is displayed.

**Product**
HA

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
show ipv6 access-list list_name [ | { grep grep_options | more } ]
```

- `list_name`
  Specifies the name of an existing ACL configured in the current context as an alphanumeric string of 1 through 47 characters.

- `| { grep grep_options | more }`
  Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
  For details on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

**Usage**

Use this command to display the configured IPv6 ACLs in the current context.

**Example**

The following command displays the contents of an IPv6 ACL named `ACLv6_4`:

```
show ipv6 access-list ACLv6_4
```
show ipv6 interface

Displays statistical and configuration information for the IPv6-based interfaces, including a Virtual Routing and Forwarding (VRF) table for a specific context.

**Product**
All

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
show ipv6 interface [ name intfc_name ] [ statistics ] [ summary ] [ vrf vrf-name ] [ | { grep grep_options | more } ]
```

- **name intfc_name**
  Displays information for an existing interface specified as an alphanumeric string of 1 through 79 characters. If no interface name is specified, the information for all IPv6 interfaces is displayed.

- **statistics**
  Displays the session statistics of all ingress and egress packets processed through this IPv6 interface.

- **summary**
  Displays summarized information about requested IPv6 interfaces.

- **vrf vrf-name**
  Displays Virtual Routing and Forwarding (VRF) routing information for an existing VRF specified as an alphanumeric string of 1 through 63 characters.

  ```
  | { grep grep_options | more }
  ```

  Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
  For details on the usage of `grep` and `more`, refer to the *Regulating a Command’s Output* section of the Command Line Interface Overview chapter.

**Usage**

Use this command to display the summarized of detailed configuration and statistical information for a configured IPv6 interface. This information can be used to verify and/or troubleshoot communication difficulties between to a remote host/node.

**Example**


The following command displays the interface information, including statistics, for the IPv6 interface IPv6Interface_2.

```
show ipv6 interface IPv6Interface_2 statistics
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show ipv6 neighbors

Displays the neighbor table for all IPv6 addresses or a specified IPv6 address in the current context.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

```
show ipv6 neighbors [ ipv6_address ] [ vrf vrf-name ] [ | { grep grep_options | more } ]
```

- **ipv6_address**
  Displays information for an existing IPv6 address specified in IPv6 colon-separated-hexadecimal notation. If no IPv6 address is specified, the information for all IPv6 addresses is displayed.

- **vrf vrf_name**
  Displays Virtual Routing and Forwarding (VRF) routing information for an existing VRF specified as an alphanumeric string of 1 through 63 characters.

```
| { grep grep_options | more }
```

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage

Use this command to display neighbor information for IPv6 address(es) in the current context. This information can be used to verify and/or troubleshoot communication difficulties between to a remote host/node.

Example

The following command displays the neighbor information for the IPv6 address `ffe:ffff:101::230:6eff:fe04:d9aa`.

```
show ipv6 neighbor ffe:ffff:101::230:6eff:fe04:d9aa
```

**Important:** Output descriptions for commands are available in the Statistics and Counters Reference.
show ipv6 ospf

Displays information regarding the configuration of the OSPFv3 Protocol on this system.

Product

PDSN
HA
GGSN

Privilege

Security Administrator, Administrator, Operator, Inspector

Mode

Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show ipv6 ospf [ database | debugging | interface | neighbor | route | virtual-links ] [ verbose [ verbose ] [ | { grep grep_options | more } ]

show ipv6 ospf database [ adv-router ipv4-address ] [ ls-type { external | inter-prefix | inter-router | intra-prefix | link | network | router }

show ipv6 ospf debugging

show ipv6 ospf interface

show ipv6 ospf neighbor [ details]

show ipv6 ospf route [ summary ]

show ipv6 ospf virtual-links

show ipv6 ospf database

Displays the OSPFv3 database including the following components.

• **adv-router ipv4-address**: Displays OSPF database information from the advertising router specified as an IP address in IPv4 dotted-decimal notation.

• **ls-type**: Displays the specified Link-State Advertisement (LSA) type, which can be one of the following:
  
  • **external**: Display External LSA information
  
  • **inter-prefix**: Displays Inter Area Prefix LSA information
  
  • **inter-router**: Displays Inter Area Router LSA information
  
  • **intra-prefix**: Displays Intra Area Prefix LSA information
  
  • **link**: Displays Link LSA information
  
  • **network**: Displays Network LSA information
show ipv6 ospf

Displays OSPFv3 Debugging Flags.

show ipv6 ospf interface
Displays OSPFv3 Interfaces.

show ipv6 ospf neighbor [ details ]
Displays OSPFv3 neighbors with the option for full details.

show ipv6 ospf route [ summary ]
Displays OSPFv3 route information with the option for summarized information.

show ipv6 ospf virtual-links
Displays OSPFv3 virtual links.

verbose
Displays detailed information.

| { grep grep_options | more }
Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage
Use this command to see all OSPFv3 information.

Example
The following command displays ipv6 ospf information:

    show ipv6 ospf
show ipv6 pool

Displays information related IPv6 Pool configuration/state.

Product
PDSN
GGSN
ASN-GW

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

\texttt{show ipv6 pool\{ \ texttt{group-name} \ group-name \} \ [ \ texttt{pool-name} \ pool-name \] \ [ \ texttt{summary} \] \ [ \ texttt{verbose} \] \ [ \ texttt{\pipe} \{ \ texttt{grep} \ texttt{grep\_options} \ | \ texttt{more} \} \] } \\

\underline{group-name group-name}
Displays IP address pool information for an existing group-name specified as an alphanumeric string of 1 through 31 characters.

\underline{pool-name pool-name}
Displays IPv6 address pool information for an existing pool name specified as an alphanumeric string of 1 through 31 characters.

\underline{summary}
Displays summary information about all IP address pools; this is the default.

\underline{verbose}
Displays detailed information about all IP address pools.

\texttt{\pipe} \{ \ texttt{grep} \ texttt{grep\_options} \ | \ texttt{more} \} \\
Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of \texttt{grep} and \texttt{more}, refer to the \textit{Regulating a Command’s Output} section of the \textit{Command Line Interface Overview} chapter.

Usage
Use this command to see all the ipv6 pool information.

Example
The following command displays ipv6 pool information:
show ipv6 pool
**show ipv6 prefix-list**

Displays information related to an IPv6 prefix list.

**Product**
- PDSN
- GGSN
- ASN-GW

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
show ipv6 prefix-list [ detail prefix-list-name ] [ name prefix-list-name [ ip-address/mask [ longer ] [ match-first ] ] [ seq seq_value ] ] [ summary prefix-list-name ] [ grep grep_options | more ]
```

- **detail prefix-list-name**
  Displays detailed IP address information for an existing prefix-list specified as an alphanumeric string of 1 through 79 characters.

- **name prefix-list-name**
  Displays IP address information for an existing prefix-list specified as an alphanumeric string of 1 through 79 characters.

- **ip-address/mask**
  Specifies an IPv6 Network Address/Mask Bits combination in CIDR notation.

- **longer**
  Displays IP address prefix-list details in longer format.

- **match-first**
  Displays first matched IP address prefix-list details.

- **seq seq_value**
  Specifies the sequence number as an integer from 1 through 4294967295.
  `seq_value` is the integer value between 1 through 4294967295.

- **summary prefix-list-name**
  Displays prefix-list summary for an existing prefix-list specified as an alphanumeric string of 1 through 79 characters.
| { grep grep_options | more }

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of `grep` and `more`, refer to the `Regulating a Command’s Output` section of the `Command Line Interface Overview` chapter.

**Usage**

Use this command to see all the ipv6 prefix-list information.

**Example**

The following command displays ipv6 prefix-list information:

```
show ipv6 prefix-list
```
show ipv6 route

Displays information related to specific route for current context.

Product
- PDSN
- GGSN
- ASN-GW

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

```
show ipv6 route [ ip-address/mask ] [ vrf vrf-name ] [ | { grep grep_options | more } ]
```

**ip-address/mask**
Specifies an IP address entered using IPv6 colon-separated-hexadecimal and CIDR notation.

**vrf vrf-name**
Displays Virtual Routing and Forwarding (VRF) routing information for an existing VRF specified as an alphanumeric string of 1 through 63 characters.

| { grep grep_options | more }

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command’s Output* section of the Command Line Interface Overview chapter.

Usage
Use this command to see all the ipv6 route information.

Example
The following command displays ipv6 route information:

```
show ipv6 route 2001:0db8:85a3:0000:0000:8a2e:0370:7334/5
```
show ipv6 route-access-list

Displays the route access list.

Product
- PDSN
- GGSN
- ASN-GW

Privilege
- Security Administrator, Administrator, Operator, Inspector

Mode
- Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

```
show ipv6 route-access-list [route-access-list] [ | { grep grep_options | more }]
```

**route-access-list**
- route-access-list is an alphanumeric string of 1 through 79 characters.

| { grep grep_options | more } |
- Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
- For details on the usage of **grep** and **more**, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter.

Usage
- Use this command to see all the IPv6 route access list information.

Example
- The following command displays ipv6 route access list information:

  ```
  show ipv6 route-access-list
  ```
show iups-service

Displays information for Iu-PS services in the current context. The Iu-PS interface links the radio network controller (RNC) with the packet switched core network.

Product
SGSN

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show iups-service { all | name srvc_name} [ gtpu-table | rnc { all | id rnc_id } ] [ | { grep grep_options | more } ]

- **all**
  Shows information for all configured IuPS services.

- **name srvc_name**
  Specifies an existing IuPS service as an alphanumeric string of 1 through 63 characters.

- **gtpu-table**
  Displays the configured GTPU database.

- **rnc all**
  Displays information for all configured RNCs.

- **rnc rnc_id**
  Specifies the identification number of an existing RNC configuration instance as an integer from 0 through 4095.

  | { grep grep_options | more }

  Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of **grep** and **more**, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage

Iu-PS services control the interface between the SGSN and the RNCs in the UMTS radio access network (UTRAN). Iu-PS services include the control plane and the data plane between these nodes.
Use this command to display information for a specific Iu-PS service or for all Iu-PS services configured within the context. A filtering keyword can limit the display to only information for a specific RNC or for a GTPU table in the Iu-PS service configuration.

**Example**

The next command displays information for all Iu-PS services configured in the current context:

```
show iups-service all
```

This command displays information for a specific RNC for a specific Iu-PS services:

```
show iups-service name iups-svc-1 rnc 123name
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show l2tp sessions

Displays information for Layer 2 Tunneling Protocol (L2TP) tunnels.

Product

LNS  
PDSN  
GGSN  
HA

Privilege

Security Administrator, Administrator, Operator, Inspector

Mode

Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show l2tp sessions [ full | summary | counters ] [ all | callid id | username name | msid ms_id | lac-service service_name | lns-service service_name peer-address [ operator ] peer_address ]

full
Displays all available information for the specified sessions.

summary
Displays a summary of available information for the specified sessions.

counters
Displays counters for the specified L2TP sessions.

all
Displays all current sessions.

callid id
Displays session information for the call ID. specified an 8-byte hexadecimal number. The output of the command show l2tp tunnels contains a field labeled Callid Hint which lists the call ID information to use with this command.

username name
Displays session information for an existing subscriber specified as an alphanumerical string of 1 through 127 characters. Wildcard characters $ and * are allowed.
**msid ms_id**
Displays session information for the MSID specified as 7 to 16 digits for an IMSI, MIN, or RMI. Wildcard characters $ and * are allowed.

**lac-service service_name**
Displays all L2TP sessions in the specified LAC service.

**lns-service service_name**
Displays all L2TP sessions in the specified LNS service.

**peer-address [ operator ] peer_address**
Displays all L2TP sessions to the destination (peer LNS) specified as an IP address in IPv4 dotted-decimal notation.
In conjunction with **sessions** keyword, indicates a range of peers is to be displayed.
**peer-address [ operator ] peer_address** is specified using IPv4 dotted-decimal notation.
*operator* implies how to logically specify a range of peer-address and it must be one of the following:
• <: IP address less than the specified **peer_address**
• >: IP address less than the specified **peer_address**
• greater-than: IP address less than the specified **peer_address**
• less-than: IP address less than the specified **peer_address**

**Usage**
Use this command to show information for sessions in the current context.

**Important:** If this command is executed from within the local context, cumulative session information is displayed for all contexts.

**Example**
The following command displays cumulative statistics for all sessions processed within the current context:
```
show l2tp sessions
```
The following command displays all information pertaining to the L2TP session of a subscriber named **isp1vpnuser1**:
```
show l2tp session full username isp1vpnuser1
```

**Important:** Output descriptions for commands are available in the Statistics and Counters Reference.
show l2tp statistics

Displays statistics for all Layer 2 Tunneling Protocol (L2TP) tunnels and sessions.

**Product**
- LNS
- PDSN
- GGSN
- HA

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Mode**
Exec
The following prompt is displayed in the Exec mode:

```
[local] host_name>
```

**Syntax**

```
show l2tp statistics [ lac-service service_name | ins-service service_name | peer-address peer_ip_address ]
```

- **lac-service service_name**
  Displays L2TP statistics for all tunnels and sessions in an existing L2TP Access Concentrator (LAC) service specified as an alphanumeric string of 1 through 63 characters.

- **ins-service service_name**
  Displays L2TP statistics for all tunnels and sessions in an existing L2TP Network Server (LNS) service specified as an alphanumeric string of 1 through 63 characters.

- **peer-address peer_ip_address**
  Displays L2TP statistics for all tunnels and sessions to the destination (peer LNS) at the IP address specified in IPv4 dotted-decimal notation.

**Usage**
Use this command to display statistics for L2TP services.

**Example**
The following command displays statistics for a specific LAC service named `vpn1`:

```
show l2tp statistics lac-service vpn1
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show l2tp tunnels

Displays information for Layer 2 Tunneling Protocol (L2TP) tunnels.

Product
LNS
PDSN
GGSN
HA

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show l2tp tunnels [ full | summary | counters ] [ all | callid id | username name | msid ms_id | lac-service service_name | lns-service service_name | peer-address [ operator ] peer_address ]

full
Displays all available information for the specified tunnels.

summary
Displays a summary of available information for the specified tunnels.

counters
Displays counters for the specified L2TP tunnels.

all
Displays all current tunnels.

callid id
Displays tunnel information for the call id specified as an 8-digit hexadecimal number. The output of the command show l2tp tunnels contains a field labeled Callid Hint which lists the call id information to use with this command.

username name
Displays tunnel information for an existing subscriber specified as an alphanumeric string of 1 through 127 characters. Wildcard characters $ and * are allowed.
**show l2tp tunnels**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>msid ms_id</strong></td>
<td>Displays tunnel information for the MSID specified as 7 to 16 digits for an IMSI, MIN, or RMI. Wildcard characters $ and * are allowed.</td>
</tr>
<tr>
<td><strong>lac-service service_name</strong></td>
<td>Displays all L2TP tunnels in the specified LAC service.</td>
</tr>
<tr>
<td><strong>lns-service service_name</strong></td>
<td>Displays all L2TP tunnels in the specified LNS service.</td>
</tr>
</tbody>
</table>
| **peer-address [ operator ] peer_address** | Displays all L2TP tunnels to the destination (peer LNS) at the IP address specified in IPv4 dotted-decimal notation. In conjunction with `tunnels` keyword, indicates a range of peers is to be displayed. \n
**Usage**

Use this command to show information for tunnels in the current context.

**Example**

The following command displays all of the tunnels currently being facilitated by LAC services within the current context:

```
show l2tp tunnels all
```

The following command displays information pertaining to the L2TP tunnel(s) established for a LAC-service named vpn1:

```
show l2tp tunnels full lac-service vpn1
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show lac-service

Displays the information for all L2TP Access Concentrator (LAC) services or for a particular LAC service.

Product
   PDSN
   HA
   GGSN

Privilege
   Security Administrator, Administrator, Operator, Inspector

Mode
   Exec
   The following prompt is displayed in the Exec mode:

   [local]host_name#

Syntax

show lac-service { all | name service_name } [ | { grep grep_options | more } ]

  all
  Display information for all LAC services.

  name service_name
  Display information only for an existing LAC service specified as an alphanumeric string of 1 through 63 characters.

  | { grep grep_options | more }
  Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
  For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage

Use this command to list information for LAC services configured on this system.

Example

The following commands display information for all LAC services and the LAC service named lac1, respectively.

    show lac-service all
    show lac-service name lac1
show lawful-intercept

Refer to the Lawful Intercept Configuration Guide for a full description of this command.
show lawful-intercept ssdf statistics

Refer to the *Lawful Intercept Configuration Guide* for a description of these statistics.
show ldap connection all

Displays all details about the Lightweight Directory Access Protocol (LDAP) subsystem.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec
The following prompt is displayed in the Exec mode:

[local] host_name#

Syntax

show ldap connection all [ | { grep grep_options | more } ]

| { grep grep_options | more }

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage

Display all details about the LDAP subsystem.

Example

The following command displays full information about the LDAP subsystem.

show ldap connection all
**show leds**

Displays the current status of the light emitting diodes (LEDs) for a specific card or all cards.

**Product**
All

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
``` 

**Syntax**

```
show leds { all | card_num } [ | { grep grep_options | more } ]
```

- **all | card_num**
  - *all*: Displays the LED status for all cards.
  - *card_num*: Displays the LED status for the card specified by its slot number.

- **| { grep grep_options | more }**
  - Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
  - For details on the usage of *grep* and *more*, refer to the *Regulating a Command’s Output* section of the Command Line Interface Overview chapter.

**Usage**

Display the status of the LEDs as a part of an automated periodic script which checks the LEDs of the chassis.

**Important**: This command is not supported on all platforms.

**Example**

The following commands display the LED status for all cards and only card 8, respectively.

```
show leds all
show leds 8
```

**Important**: Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show license information

Displays information about the licenses installed on this system, as well as the maximum number of sessions.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show license information { key_name | full } | { key } [ | { grep grep_options | more } ]

key_name | full

key_name: Displays the information for an existing license key specified as an alphanumeric string of 1 of 1 through 500 characters.
full: Displays the full features and quantities without any hardware limits in place.

key:

Displays the installed keys in encrypted format.

| { grep grep_options | more }

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage

Displays the license information to verify the proper keys have been installed. This command is also helpful in troubleshooting user system access due to the maximum number of sessions being reached.

Example

The following displays the encrypted installed key and the information for sampleKey respectively.

show license information sampleKey

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show linecard

Displays information on the interface cards installed in the rear of the system chassis.

**Product**
All

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name# 
```

**Syntax**

```
show linecard { dlci-utilization card# | table } [ | { grep grep_options | more } ]
```

**dlci-utilization card#**

SGSN only
In tabular format, displays current data link utilization (in 5 minute and 15 minute breakdowns) information for all Frame Relay ports on the specified CLC-type line card. Data links are referred to by data link connection identifiers (DLCI).

*card#* - Identifies the chassis slot number where the line card resides. Enter an integer from 1 to 48.

---

**table**
Displays information on all line card slots in tabular format.

| { grep grep_options | more } |

---

**Usage**

Use this command to show the line card information

- to verify hardware inventories and installed components.
- to review DLCI utilization for a specific Frame Relay channelized line card.

---

**Important:** This command is not supported on all platforms.

**Example**

Use the following command to display a table with information identifying all line cards installed in the chassis:

```
show linecard table
```
Use the following command to display DLCI utilization information for all ports on CLC card in slot 27:

```
show linecard dlci-utilization 27
```

*Important:* Output descriptions for `show` commands are available in the *Statistics and Counters Reference.*
show linkmgr

Displays statistics for the link manager (linkmgr).

Product
SGSN

Privilege
Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show linkmgr { all | instance instance } [ parser | | ]

| all
| Display statistics for all link managers.

| instance instance
| Display statistics for a single instance of a link manager specified as an integer from 1 to 4.

| { grep grep_options | more }
| Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent. For details on the usage of *grep* and *more*, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter.

Usage

This command displays statistical information for the SGSN’s link manager which handles the layer between the session manager and the SS7 functionality downwards from layer 3.

Example

Use the following command to display the statistics for link manager 4:

```
show linkmgr 4
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*.
show llc statistics

Displays traffic statistics for the GPRS logical link-control (LLC) layer.

**Product**
SGSN

**Privilege**
Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
show llc statistics [ gprs-service srvc_name ] [ verbose ] [ | { grep grep_options | more } ]
```

**gprs-service srvc_name**
Displays the statistics for an existing GPRS service specified as an alphanumeric string of 1 through 63 characters.

**verbose**
Displays all possible statistics for specified command or keyword.

```
| { grep grep_options | more }
```

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For more information on the usage of `grep` and `more`, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Reference*.

**Usage**

This command can display either a summarized or full (verbose) view of statistics collected for the traffic that has gone through the LLC layer for either all GPRS services or for a specified GPRS service.

**Example**

The following command displays the frame Tx/Rx LLC statistics for GPRS service gprsl:

```
show llc statistics gprs-service gprsl
```
show llc status

Displays status information for the GPRS logical link-control (LLC) layer.

Product
SGSN

Privilege
Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local] host_name#

Syntax

show llc status gprs-service srvc_name sessmgr instance instance { dlci ms-id ms_id sapi sapid | lsap sapid | ms ms_id | usap sapid | [ | { grep grep_options | more } ]

gprs-service srvc_name
Displays the LLC layer status for an existing GPRS service specified as an alphanumeric string of 1 through 63 characters.

sessmgr instance instance
Displays the LLC status for a session manager instance specified as an integer. The range varies depending upon the release:

• for releases prior to 14.0, the range is from 1 to 4294967295.
• for releases 14.0 and later, the range is from 1 to 384.

dlci ms-id ms_id [ sapi sapid ]
Displays the LLC status for a specific data link connection identifier (DLCI) between the LLC and the mobile station (MS). ms_id must be an integer from 0 to 65536 that identifies the DLCI interface connecting to a specific MS.
sapi: Filters the display of the LLC status information to focus on a specific service access point interface (SAPI) within the specified DLCI specified as an integer from 1 to 11.

lsap sapid
Refines the display of the LLC status to focus on a specific lower service access point interface (LSAP) specified as an integer from 0 to 65536.

ms-id ms_id
Displays the LLC status for a connected MS specified as an integer from 0 to 65536.

usap sapid
Refines the display of the LLC statistics to focus on a specific upper service access point interface (USAP) specified as an integer from 0 to 65536.
| { grep grep_options | more }

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For more information on the usage of `grep` and `more`, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Reference*.

**Usage**

This command can display either a summarized or full (verbose) view of statistics collected for the traffic that has gone through the LLC layer for either all GPRS services or for a specified GPRS service.

**Example**

The following command displays the frame Tx/Rx LLC statistics for GPRS service *gprs1*:

```
show llc statistics gprs-service gprs1
```
show lma-service

Displays statistic and counter information for Local Mobility Anchor (LMA) services on this system.

Product
P-GW
SAEGW

Privilege
Inspector

Mode
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show lma-service all

show lma-service name service_name

show lma-service session [ all | callid id | counters | full | ipv6-address { < address | > address | address | greater-than address [ less-than address ] | less-than address [ greater-than address ] } | summary | username name ]

show lma-service statistics [ lma-service name ] [ | { grep grep_options | more } ]

all
Displays information about all configured LMA services on this system.

name service_name
Displays configuration information for an existing LMA service specified as an alphanumeric string of 1 through 63 characters.

session [ all | callid id | counters | full | ipv6-address { < address | > address | address | greater-than address [ less-than address ] | less-than address [ greater-than address ] } | summary | username name ]

Displays session information filtered by the following parameters:
all: Displays all active LMA sessions using LMA services on the system.
callid id: Displays available session information for the call identification number specified as an eight-byte hexadecimal number.
counters: Displays session counters for active LMA sessions using LMA services on the system. This keyword can also be filtered by the following:
  • all
  • callid
  • ipv6-address
  • username
Refer to the keyword descriptions in this command for information regarding these filters.

**full**: Displays additional session information for active LMA sessions using LMA services on the system. This keyword includes the information in the output of the **all** keyword plus additional information. This keyword can also be filtered by the following:

- **all**
- **callid**
- **ipv6-address**
- **username**

Refer to the keyword descriptions in this command for information regarding these filters.

**ipv6-address**:

- **<< address and less-than address**: Displays summarized information for a group of IPv6 addresses that are less than the specified IPv6 address using one of these keywords. A range can be specified by including an address with the **greater-than** option. **address** must be specified in IPv6 colon-separated-hexadecimal notation.

- **>> address and greater-than address**: Displays summarized information for a group of IPv6 addresses that are greater than the specified IPv6 address using one of these keywords. A range can be specified by including an address with the **less-than** option. **address** must be specified in IPv6 colon-separated-hexadecimal notation.

- **address**: Displays summarized information for a specific IPv6 address using an LMA service on this system. **address** must be specified in IPv6 colon-separated-hexadecimal notation.

**summary**: Displays the number of LMA sessions currently active for LMA services configured on the system.

**username name**: Displays available session information for an existing user specified as an alphanumeric string of 1 through 127 characters.

```
statistics [ lma-service name ]
```

**lma-service name**: Displays LMA service statistics for an existing LMA service specified as an alphanumeric string of 1 through 63 characters.

```
 | { grep grep_options | more }
```

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter.

---

**Usage**

Use this command to view configuration information for LMA services on this system.

**Example**

The following command displays service statistics for the LMA service named `lma1`:

```
show lma-service name lma1
```
show lns-service

Displays the information for all L2TP Network Server (LNS) services or for a particular LNS service.

Product
PDSN
HA
GGSN
LNS

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec
The following prompt is displayed in the Exec mode:
[local]host_name#

Syntax

show lns-service { all | name service_name } [ | { grep grep_options | more } ]

- all
  Display information for all LNS services.

- name service_name
  Displays information only for an existing LNS service specified as an alphanumeric string of 1 through 63 characters.

  | { grep grep_options | more }

  Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
  For details on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage
Use this command to list information for LNS services configured on this system.

Example
The following commands display information for all LNS services and the LNS service named `lns1`, respectively.

  show lns-service all

  show lns-service name lns1
show local-policy

Displays information pertaining to local QoS policy services.

Product
- P-GW
- SAEGW

Privilege
- Security Administrator

Mode
- Exec
The following prompt is displayed in the Exec mode:

[local] host_name#

Syntax

show local-policy statistics { all | service service_name | summary } | { grep grep_options | more }

Usage
- Use this command to display statistics for local QoS policies on this system.

Example
- The following command displays statistics for the local QoS policy named sample1.

show local-policy statistics service sample1

statistics { all | service service_name | summary }
- Display statistics pertaining to local QoS services.
- all: Displays information for all local QoS services.
- service service_name: Displays statistics only for an existing local QoS service specified as an alphanumeric string of 1 through 64 characters.
- summary: Displays summarized statistics all local QoS services.

| { grep grep_options | more }
- Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
- For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.
**show local-user**

Displays information pertaining to local-user accounts.

**Product**

All

**Privilege**

Security Administrator

**Mode**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
show local-user [ [ username name ] [ inactive filter ] [ verbose | wide ] | statistics [ verbose ] ]
```

### username name

Displays information for an existing local-user administrative account specified as an alphanumeric string of 3 through 16 characters that is case sensitive. If a username is not specified, information is displayed for all local users.

### inactive filter

Specifies a filter for displaying inactive local-user accounts:

- `<= days`: Displays accounts that have been inactive less than the specified number of days.
- `>= days`: Displays accounts that have been inactive more than the specified number of days.
- `greater-than days`: Displays accounts that have been inactive more than the specified number of days.
- `less-than days`: Displays accounts that have been inactive less than the specified number of days.

*days* can be configured to an integer from 1 through 365.

### [ verbose | wide ]

Specifies how the information is to be displayed as one of the following options:

- `verbose`: The data is displayed in list format. Additional information is provided beyond what is displayed when the `wide` option is used.
- `wide`: The data is displayed in tabular format. This is the default setting.

### statistics [ verbose ]

Displays local-user statistics.

Using the `verbose` keyword displays additional statistics.
show local-user

Usage
Use this command to display information and statistics on local-user administrative accounts.

Example
The following command displays detailed information on local-user administrative accounts that have been inactive for more than 10 days:

`show local-user inactive greater-than 10 verbose`

The following command displays detailed information for a local-user account named `Test`:

`show local-user username Test verbose`

The following command displays detailed local-user account statistics:

`show local-user statistics verbose`

**Important**: Output descriptions for commands are available in the *Statistics and Counters Reference*. 

---

Cisco ASR 5x00 Command Line Interface Reference
show location-service

Displays information and statistics for all location services or for a specific location service.

Product
MME
SGSN

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show location-service { service { all | name service_name } | statistics { all | service service_name } [ | { grep grep_options | more } ]

service { all | name service_name }
Display configuration information pertaining to location services.
all: Displays information for all location services.
name service_name: Displays information only for an existing location service specified as an alphanumeric string of 1 through 63 characters.

statistics { all | service service_name }
Display statistics pertaining to location services.
all: Displays statistics for all location services.
name service_name: Displays statistics only for an existing location service specified as an alphanumeric string of 1 through 64 characters.

| { grep grep_options | more }
Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage
Use this command to list configuration information and statistics for location services configured on this system.

Example
The following commands display information for all location services and the location service named location_service1, respectively.

show location-service service all
show location-service service name location_service1

The following command displays statistics for the location service named location_service1.

show location-service statistics service location_service1
show logging

Displays the defined logging filters for the current context.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

```
show logging [ active | verbose ] [ | { grep grep_options | more } ]
```

- **active | verbose**
  - **active**: Displays only active CLI logging filter information in concise format.
  - **verbose**: Displays as much information as possible.

- **| { grep grep_options | more }**
  - Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
  - For details on the usage of `grep` and `more`, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter.

Usage
View log filters to troubleshoot disk utilization issues.

Example

```
show logging

show logging active

show logging verbose

show logging active verbose
```
show logical-port utilization table

Displays logical port (VLAN and NPU) utilization for a specified interface port.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec
The following prompt is displayed in the Exec mode:
[local]host_name#

Syntax

show logical port utilization table slot/port [vlan { 5-minute | hourly }] [ | { grep grep_options | more } ]

slot/port
Specifies the port for which logical-port statistics will be displayed. The slot and port must refer to an installed card and port.

vlan { 5-minute | hourly }
Displays only active VLAN information for the specified collection interval.
- 5-minute: Displays 5-minute utilization intervals for the past 24 hours.
- hourly: Displays hourly utilization intervals for the past 24 hours.

| { grep grep_options | more }
Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage
View logical port (VLAN) statistics for 5-minute intervals on port 17/1.

Example

show logical-port utilization table 17/1 vlan 5-minute
show logs

Displays active and inactive logs filtered by the options specified.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec
The following prompt is displayed in the Exec mode:

[local] host_name#

Syntax

show logs [ active ] [ inactive ] [ callid call_id ] [ event-verbosity evt_verboseness ] [ facility facility ] [ level severity_level ] [ pdu-data pdu_format ] [ pdu-verbosity pdu_verboseness ] [ proclet facility ] [ since from_date_time [ until to_date_time ] ] [ | { grep grep_options | more } ]

---

active
Displays data from active logs.

inactive
Displays data from inactive logs.

callid call_id
Displays log information only for a call ID specified as a 4-digit hexadecimal number.

event-verbosity evt_verboseness
Specifies the level of verboseness to use in displaying of event data as one of:

• min - displays minimal information about the event. Information includes event name, facility, event ID, severity level, date, and time.
• concise - displays detailed information about the event, but does not provide the event source within the system.
• full - displays detailed information about event, including source information, identifying where within the system the event was generated.

facility facility
Specifies the facility to modify the filtering of logged information for as one of:

• a10: A10 interface facility
• a11: A11 interface facility
• a11mgr: A11 Manager facility
• aaa-client: Authentication, Authorization and Accounting (AAA) client facility
• **aaamgr**: AAA manager logging facility
• **aaaprox**: AAA Proxy facility
• **aal2**: ATM Adaptation Layer 2 (AAL2) protocol logging facility
• **acl-log**: Access Control List (ACL) logging facility
• **acsctrl**: Active Charging Service (ACS) Controller facility
• **acsmgr**: ACS Manager facility
• **afctrl**: Fabric Controller facility [ASR 5500 only]
• **afmgr**: Fabric Manager logging facility [ASR 5500 only]
• **alarmctrl**: Alarm Controller facility
• **alcap**: Access Link Control Application Part (ALCAP) protocol logging facility
• **alcapmgr**: ALCAP manager logging facility
• **all**: All facilities
• **asngwmgr**: Access Service Network (ASN) Gateway Manager facility
• **asnpmg**: RN Paging Controller Manager facility
• **bfd**: Bidirectional Forwarding Detection (BFD) protocol logging facility
• **bgp**: Border Gateway Protocol (BGP) facility
• **bindmux**: IPCF BindMux-Demux Manager logging facility
• **bngmgr**: Broadband Network Gateway (BNG) Demux Manager logging facility
• **bssap+**: Base Station Sub-system Application Part+ protocol facility for the login interface between the SGSN and the MSC/VLR (2.5G and 3G)
• **bssgp**: Base Station Sub-system GPRS Protocol logging facility handles exchange information between the SGSN and the BSS (2.5G only)
• **callhome**: Call Home application logging facility
• **cap**: CAMEL Application Part (CAP) logging facility for protocol used in prepaid applications (2.5G and 3G)
• **cbsmgr**: Cell Broadcasting Service (CBS) logging facility [HNBGW]
• **cdf**: Charging Data Function (CDF) logging facility
• **cgw**: Converged Access Gateway (CGW) logging facility
• **cli**: Command Line Interface (CLI) logging facility
• **cmp**: Certificate Management Protocol (IPSec) logging facility
• **connectedapps**: SecGW ASR 9000 oneP communication protocol
• **connproxy**: Controller Proxy logging facility
• **credit-control**: Credit Control (CC) facility
• **cscf**: IMS/MMD Call Session Control Function (CSCF)
• **cscfcpmgr**: CSCFCPMGR logging facility
• **csfmgr**: SIP CSCF Manager facility
• **cscfnpdb**: CSCF Number Portability Database (NPDB) logging facility
• **cscfrtcp**: IMS/MMD CSCF RTCP log facility
- **cscfrtp**: IMS/MMD CSCF RTP log facility
- **cscfttmgr**: SIP CSCF Tunnel and Transport Manager facility
- **csp**: Card/Slot/Port controller facility
- **css**: Content Service Selection (CSS) facility
- **css-sig**: CSS RADIUS Signaling facility
- **cx-diameter**: Cx Diameter Messages facility [CSCF <--> HSS]
- **dcardctrl**: IPSec Daughter Card Controller logging facility
- **dcardmgr**: IPSec Daughter Card Manager logging facility
- **demuxmgr**: Demux Manager API facility
- **dgmmbmgr**: Diameter Gmb Application Manager logging facility
- **dhcp**: Dynamic Host Configuration Protocol (DHCP) logging facility
- **dhcpv6**: DHCPv6
- **dhost**: Distributed Host logging facility
- **diabase**: Diabase messages facility
- **diameter**: Diameter endpoint logging facility
- **diameter-acct**: Diameter Accounting
- **diameter-auth**: Diameter Authentication
- **diameter-dns**: Diameter DNS subsystem
- **diameter-ecs**: ACS Diameter signaling facility
- **diameter-hdd**: Diameter Horizontal Directional Drilling (HDD) Interface facility
- **diameter-svc**: Diameter Service
- **diamproxy**: DiamProxy logging facility
- **dpath**: IPSec Data Path facility
- **drvctrl**: Driver Controller facility
- **doulosuemgr**: Doulos (IMS-IPSec-Tool) user equipment manager
- **eap-diameter**: Extensible Authentication Protocol (EAP) IP Security facility
- **eap-ipsec**: Extensible Authentication Protocol (EAP) IPSec facility
- **eap-sta-s6a-s13-s6b-diameter**: EAP/STA/S6A/S13/S6B Diameter messages facility
- **ecs-css**: ACSMG <--> Session Manager Signalling Interface facility
- **egtpc**: eGTP-C logging facility
- **egtpmgr**: enhanced GPRS Tunneling Protocol (eGTP) manager logging facility
- **egtpu**: eGTP-U logging facility
- **epdg**: evolved Packet Data (ePDG) gateway logging facility
- **event-notif**: Event Notification Interface logging facility
- **evlog**: Event log facility
- **famgr**: Foreign Agent manager logging facility
- **firewall**: Firewall logging facility
• **fng**: Femto Network Gateway (FNG) logging facility
• **gbmgr**: SGSN Gb Interface Manager facility
• **gmm**:
  • For 2.5G: Logs the GPRS Mobility Management (GMM) layer (above LLC layer)
  • For 3G: Logs the access application layer (above the RANAP layer)
• **gprs-app**: GPRS Application logging facility
• **gprs-ns**: GPRS Network Service Protocol (layer between SGSN and the BSS) logging facility
• **gq-rx-tx-diameter**: Gq/Rx/Tx Diameter messages facility
• **gss-gcdr**: GTPP Storage Server GCDR facility
• **gtp**: GTP-C protocol logging facility
• **gtpcmgr**: GTP-C protocol manager logging facility
• **gtp**: GTP-prime protocol logging facility
• **gtpu**: GTP-U protocol logging facility
• **gtpumgr**: GTP-U Demux manager
• **gx-ty-diameter**: Gx/Ty Diameter messages facility
• **gy-diameter**: Gy Diameter messages facility
• **h248prt**: H.248 port manager facility
• **hamgr**: Home Agent manager logging facility
• **hat**: High Availability Task (HAT) process facility
• **hdctrl**: HD Controller logging facility
• **henbapp**: Home Evolved NodeB (HENB) App facility
• **henbgw**: HENB-GW facility
• **henbgw-pws**: HENB-GW Public Warning System logging facility
• **henbgw-sctp-acs**: HENB-GW access Stream Control Transmission Protocol (SCTP) facility
• **henbgw-sctp-nw**: HENBGW network SCTP facility
• **henbgwdemux**: HENB-GW Demux facility
• **henbgwmgm**: HENB-GW Manager facility
• **hnb-gw**: HNB-GW (3G Femto GW) logging facility
• **hnbmgm**: HNB-GW Demux Manager logging facility
• **hss-peer-service**: Home Subscriber Server (HSS) Peer Service facility
• **igmp**: Internet Group Management Protocol (IGMP)
• **ikev2**: Internet Key Exchange version 2 (IKEv2)
• **ims-authorizatn**: IP Multimedia Subsystem (IMS) Authorization Service facility
• **ims-sh**: HSS Diameter Sh Interface Service facility
• **imsimgr**: SGSN IMSI Manager facility
• **imsue**: IMS User Equipment (IMSUE) facility
• **ip-arp**: IP Address Resolution Protocol facility
• ip-interface: IP interface facility
• ip-route: IP route facility
• ipms: Intelligent Packet Monitoring System (IPMS) logging facility
• ipne: IP Network Enabler (IPNE) facility
• ipsec: IP Security logging facility
• ipsg: IP Service Gateway interface logging facility
• ipsgmgr: IP Services Gateway facility
• ipsp: IP Pool Sharing Protocol logging facility
• kvstore: Key/Value Store (KVSTORE) Store facility
• l2tp-control: Layer 2 Tunneling Precool (L2TP) control logging facility
• l2tp-data: L2TP data logging facility
• l2tpdemux: L2TP Demux Manager logging facility
• l2tpmgr: L2TP Manager logging facility
• lagmgr: Link Aggregation Group (LAG) manager logging facility
• lcs: Location Services (LCS) logging facility
• ldap: Lightweight Directory Access Protocol (LDAP) messages logging facility
• li: Refer to the Lawful Intercept Interface Reference for a description of this command.
• linkmgr: SGSN/BSS SS7 Link Manager logging facility (2.5G only)
• lcc: Logical Link Control (LLC) Protocol logging facility; for SGSN: logs the LLC layer between the GMM and the BSSGP layers for logical links between the MS and the SGSN
• local-policy: Local Policy Service facility
• location-service: Location Services facility
• m3ua: M3UA Protocol logging facility
• magmgr: Mobile Access Gateway manager logging facility
• map: Mobile Application Part (MAP) protocol logging facility
• megadiammgr: MegaDiameter Manager (SLF Service) logging facility
• mme-app: Mobility Management Entity (MME) Application logging facility
• mme-misc: MME miscellaneous logging facility
• mmedemux: MME Demux Manager logging facility
• mmemgr: MME Manager facility
• mmgr: Master Manager logging facility
• mobile-ip: Mobile IP processes
• mobile-ip-data: Mobile IP data facility
• mobile-ipv6: Mobile IPv6 logging facility
• mpls: Multiprotocol Label Switching (MPLS) protocol logging facility
• mrme: Multi Radio Mobility Entity (MRME) logging facility
• **mseg-app**: Mobile Services Edge Gateway (MSEG) application logging facility (This option is not supported in this release.)
• **mseg-gtpe**: MSEG GTP-C application logging facility (This option is not supported in this release.)
• **mseg-gtpu**: MSEG GTP-U application logging facility (This option is not supported in this release.)
• **msegmgr**: MSEG Demux Manager logging facility (This option is not supported in this release.)
• **mtp2**: Message Transfer Part 2 (MTP2) Service logging facility
• **mtp3**: Message Transfer Part 3 (MTP3) Protocol logging facility
• **multicast-proxy**: Multicast Proxy logging facility
• **nas**: Non-Access Stratum (NAS) protocol logging facility [MME 4G]
• **netwstrg**: Network Storage facility
• **npuctrl**: Network Processor Unit Control facility
• **npudrv**: Network Processor Unit Driver facility [ASR 5500 only]
• **npumgr**: Network Processor Unit Manager facility
• **npumgr-acl**: NPUMGR ACL logging facility
• **npumgr-drv**: NPUMGR DRV logging facility
• **npumgr-flow**: NPUMGR FLOW logging facility
• **npumgr-fwd**: NPUMGR FWD logging facility
• **npumgr-init**: NPUMGR INIT logging facility
• **npumgr-lc**: NPUMGR LC logging facility
• **npumgr-port**: NPUMGR PORT logging facility
• **npumgr-recovery**: NPUMGR RECOVERY logging facility
• **npumgr-rrri**: NPUMGR RRI (Reverse Route Injection) logging facility
• **npumgr-vpn**: NPUMGR VPN logging facility
• **npusim**: NPUSIM logging facility [ASR 5500 only]
• **ntfy-intf**: Notification Interface logging facility [Release 12.0 and earlier versions only]
• **ocsp**: Online Certificate Status Protocol logging facility
• **orbs**: Object Request Broker System logging facility
• **ospf**: OSPF protocol logging facility
• **ospfv3**: OSPFv3 protocol logging facility
• **p2p**: Peer-to-Peer Detection logging facility
• **pagingmgr**: PAGINGMGR logging facility
• **ppcmgr**: Intelligent Policy Control Function (IPCF) Policy Charging and Control (PCC) Manager library
• **pdg**: Packet Data Gateway (PGD) logging facility
• **pdgdmgr**: PDG Demux Manager logging facility
• **pdif**: Packet Data Interworking Function (PDIF) logging facility
• **pgw**: Packet Data Network Gateway (PGW) logging facility
- **pmm-app**: Packet Mobility Management (PMM) application logging facility
- **ppp**: Point-To-Point Protocol (PPP) link and packet facilities
- **pppoe**: PPP over Ethernet logging facility
- **push**: VPNMGR CDR push logging facility
- **radius-act**: RADIUS accounting logging facility
- **radius-auth**: RADIUS authentication logging facility
- **radius-coa**: RADIUS change of authorization and radius disconnect
- **ranap**: Radio Access Network Application Part (RANAP) Protocol facility logging info flow between SGSN and RNS (3G)
- **rct**: Recovery Control Task logging facility
- **rdt**: Redirect Task logging facility
- **resmgr**: Resource Manager logging facility
- **rf-diameter**: Diameter RF interface messages facility
- **rip**: Routing Information Protocol (RIP) logging facility [RIP is not supported at this time.]
- **rlf**: Rate Limiting Function (RLF) logging facility
- **rohc**: Robust Header Compression (RoHC) facility
- **rsvp**: Reservation Protocol logging facility
- **rua**: RANAP User Adaptation (RUA) [3G Femto GW - RUA messages] logging facility
- **s1ap**: S1 Application Protocol (S1AP) Protocol logging facility
- **sabp**: Service Area Broadcast Protocol (SABP) logging facility
- **saegw**: System Architecture Evolution (SAE) Gateway facility
- **scfp**: Signalling Connection Control Part (SCCP) Protocol logging (connection-oriented messages between RANAP and TCAP layers).
- **set**: Shared Configuration Task logging facility
- **sctp**: Stream Control Transmission Protocol (SCTP) Protocol logging facility
- **sef_ecs**: Severely Errored Frames (SEF) APIs printing facility
- **sess-gr**: SM GR facility
- **sessctrl**: Session Controller logging facility
- **sessmgr**: Session Manager logging facility
- **sesstrc**: session trace logging facility
- **sft**: Switch Fabric Task logging facility
- **sgs**: SGs interface protocol logging facility
- **sgsn-app**: SGSN-APP logging various SGSN “glue” interfaces (for example, between PMM, MAP, GPRS-FSM, SMS).
- **sgsn-failures**: SGSN call failures (attach/activate rejects) logging facility (2.5G)
- **sgsn-gtpc**: SGSN GTP-C Protocol logging control messages between the SGSN and the GGSN
- **sgsn-gtpu**: SGSN GTP-U Protocol logging user data messages between the SGSN and GGSN
• **sgsn-mbms-bearer**: SGSN Multimedia Broadcast/Multicast Service (MBMS) Bearer app (SMGR) logging facility
• **sgsn-misc**: Used by stack manager to log binding and removing between layers
• **sgsn-system**: SGSN System Components logging facility (used infrequently)
• **sgsn-test**: SGSN Tests logging facility; used infrequently
• **sgtpcmgr**: SGSN GTP-C Manager logging information exchange through SGTPC and the GGSN
• **sgw**: Serving Gateway facility
• **sh-diameter**: Sh Diameter messages facility
• **sitmain**: System Initialization Task main logging facility
• **sm-app**: SM Protocol logging facility
• **sms**: Short Message Service (SMS) logging messages between the MS and the SMSC
• **sndcp**: Sub Network Dependent Convergence Protocol (SNDCP) logging facility
• **snmp**: SNMP logging facility
• **sprmgr**: IPCF Subscriber Policy Register (SPR) manager logging facility
• **srdb**: Static Rating Database
• **srp**: Service Redundancy Protocol (SRP) logging facility
• **sscfnni**: Service-Specific Coordination Function for Signaling at the Network Node Interface (SSCF-NNI) logging facility
• **sscop**: Service-Specific Connection-Oriented Protocol (SSCOP) logging facility
• **ssh-ipsec**: Secure Shell (SSH) IP Security logging facility
• **ssl**: Secure Socket Layer (SSL) message logging facility
• **stat**: Statistics logging facility
• **supserv**: Supplementary Services logging facility [H.323]
• **system**: System logging facility
• **tacacsplus**: TACACS+ Protocol logging facility
• **tcap**: TCAP Protocol logging facility
• **testctrl**: Test Controller logging facility
• **testmgr**: Test Manager logging facility
• **threshold**: threshold logging facility
• **ttg**: Tunnel Termination Gateway (TTG) logging facility
• **tucl**: TCP/UDP Convergence Layer (TUCL) logging facility
• **udr**: User Data Record (UDR) facility (used with the Charging Service)
• **user-data**: User data logging facility
• **user-l3tunnel**: User Layer 3 tunnel logging facility
• **usertcp-stack**: User TCP Stack
• **vim**: Voice Instant Messaging (VIM) logging facility
• **vinfo**: VINFO logging facility
• `vmgctrl`: Virtual Media Gateway (VMG) controller facility
• `vmgctrl`: VMG Content Manager facility
• `vpn`: Virtual Private Network logging facility
• `wimax-data`: WiMAX DATA
• `wimax-r6`: WiMAX R6
• `wsg`: Wireless Security Gateway (ASR 9000 Security Gateway)

**level severity_level**

`level severity_level`: Specifies the level of information to be logged from the following list which is ordered from highest to lowest:
- `critical`: display critical events
- `error`: display error events and all events with a higher severity level
- `warning`: display warning events and all events with a higher severity level
- `unusual`: display unusual events and all events with a higher severity level
- `info`: display info events and all events with a higher severity level
- `trace`: display trace events and all events with a higher severity level
- `debug`: display all events

**pdu-data pdu_format**

Specifies output format for the display of packet data units as one of:
- `none`: output is in raw format (unformatted).
- `hex`: output being displayed in hexadecimal format.
- `hex-ascii`: output being displayed in hexadecimal and ASCII similar to a main-frame dump.

**pdu-verbosity pdu_verboseness**

Specifies the level of verboseness to use in displaying of packet data units as an integer from 1 through 5, where 5 is the most detailed.

**proclet facility**

Shows the logs from a specific proclet facility. The available facilities are the same as those listed earlier.

**since from_date_time [ until to_date_time ]**

Default: no limit.
`since from_date_time`: indicates only the log information which has been collected more recently than `from_date_time` is to be displayed.
`until to_date_time`: indicates no log information more recent than `to_date_time` is to be displayed.
`until` defaults to current time when omitted.
`from_date_time` and `to_date_time` must be formatted as YYYY:MM:DD:HH:mm or YYYY:MM:DD:HH:mm:ss. Where:
- `YYYY` = 4-digit year
- `MM` = 2-digit month in the range 01 through 12
- `DD` = 2-digit day in the range 01 through 31
- HH = 2-digit hour in the range 00 through 23
- mm = 2-digit minute in the range 00 through 59
- ss = 2-digit second in the range 00 through 59

to_date_time must be a time which is more recent than from_date_time.
The use of the until keyword allows for a time range of log information while only using the since keyword will display all information up to the current time.

```
| { grep grep_options | more }
```
Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

**Usage**

View log files for general maintenance or troubleshooting system issues.

**Example**

The following command displays log information for the allmgr facility starting with July 1th, 2011 at midnight.

```
show logs facility allmgr since 2011:07:11:00:00
```

The following command displays the log information for call ID FE881D32 only in active logs.

```
show logs active callid FE881D32
```
show lte-policy

Displays information for Long term Evolution (LTE) policy configurations on this system including congestion action profiles, handover restriction lists, paging maps, paging profiles, subscriber maps, and tracking area identifiers (TAIs).

**Product**
- MME
- SAEGW
- S-GW

**Privilege**
- Inspector

**Mode**
- Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
show lte-policy { cause-code-group { name group_name | summary } | congestion-action-profile { name congest_profile_name | summary } | foreign-plmn-guti-mgmt-db { name db_name | summary } | henbgw { mme-pool { name mme_pool_name | summary } | overload-control | sl-reset | session-recovery } | ho-restriction-list { name ho_list_name | summary } | lte-emergency-profile { name emer_profile_name | summary } | mme { henbgw_mgmt-db { name henbgw_mgmtdb_name | summary } | paging cache parameters | paging-map { name page_map_name | summary } | paging-profile { name page_profile_name | summary } | peer-map { name sub_map_name | summary } | subscriber-map { name sub_map_name | summary } | tai-list-db { name tai_list_name summary } | tai-mgmt-db { name tai_name | summary } } | { grep grep_options | more } ]
```

---

**cause-code-group { name group_name | summary }**

This MME-specific keyword displays information about the Cause Code Groups configured on this system.

*name group_name*: Displays information about a specific cause code group configured on this system.

*group_name* must be an existing cause code group, expressed as an alphanumeric string of 1 to 16 characters.

*summary*: Displays summarized information about all cause code groups configured on this system.

---

**congestion-action-profile { name congest_profile_name | summary }**

Displays information about MME congesting action profiles configured on this system.

*name profile_name*: Displays information about a specific congestion action profile configured on this system.

*profile_name* must be an existing HO restriction list, expressed as an alphanumeric string of 1 to 64 characters.

*summary*: Displays summarized information about all congestion action profiles configured on this system.

---

**foreign-plmn-guti-mgmt-db { name db_name | summary }**

This MME-specific keyword displays information about LTE Foreign PLMN GUTI management databases configured on this system.
show lte-policy

name db_name: Displays information about a specific management database configured on this system. db_name must be an existing management database, expressed as an alphanumeric string of 1 to 64 characters.

summary: Displays summarized information about all Foreign PLMN GUTI management databases configured on this system.

ho-restriction-list { name list_name | summary }
Displays information about handover restriction lists configured on this system.
name ho_list_name: Displays information about a specific handover restriction list configured on this system. name must be an existing HO restriction list, expressed as an alphanumeric string of 1 to 64 characters.
summary: Displays summarized information about all handover restriction lists configured on this system.

lte-emergency-profile { name emer_profile_name | summary }
Displays information about LTE emergency profiles configured on this system.
name emer_profile_name: Displays information about a specific LTE emergency profile configured on this system. emer_profile_name must be an existing LTE emergency profile, expressed as an alphanumeric string of 1 to 64 characters.
summary: Displays summarized information about all LTE emergency profiles configured on this system.

mme paging cache parameters
Displays the configured MME paging cache timeout and MME paging cache size configured with the mme paging cache command in the LTE Policy configuration mode.

paging-map { name page_map_name | summary }
Displays information about LTE paging maps configured on this system.
name page_map_name: Displays information about an existing LTE paging map specified as an alphanumeric string of 1 through 64 characters.
summary: Displays summarized information about all LTE paging maps configured on this system.

paging-profile { name page_profile_name | summary }
Displays information about LTE paging profiles configured on this system.
name page_profile_name: Displays information about an existing LTE paging profile specified as an alphanumeric string of 1 through 64 characters.
summary: Displays summarized information about all LTE paging profiles configured on this system.

peer-map { name name | summary }
Displays information about peer maps configured on this system.
name map_name: Displays information about an existing peer map specified as an alphanumeric string of 1 through 64 characters.
summary: Displays summarized information about all peer maps configured on this system.

subscriber-map { name name | summary }
Displays information about subscriber maps configured on this system.
name sub_map_name: Displays information about an existing subscriber map specified as an alphanumeric string of 1 through 64 characters.
summary: Displays summarized information about all subscriber maps configured on this system.
tai-list-db { name tai_list_name | summary }
Displays information about TAI list databases configured on this system.
  name: tai_list_name: Displays information about specified TAI list database as an alphanumeric string of 1 through 64 characters.
  summary: Displays summarized information about specified TAI list databases configured on this system.

tai-mgmt-db { name tai_name | summary }
Displays information about TAI management databases configured on this system.
  name: tai_name: Displays information about an existing TAI management database specified as an alphanumeric string of 1 through 64 characters.
  summary: Displays summarized information about all TAI management databases configured on this system.

| { grep grep_options | more }
Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of the grep and more commands, refer to the Regulating a Command’s Output section in CLI Overview chapter.

Usage
Use this command to display information for LTE policy configurations on this system including congestion action profiles, handover restriction lists, paging maps, paging profiles, subscriber maps, and tracking area identifiers (TAIs).

Example
The following command displays information about a subscriber map named map3:

```
show lte-policy subscriber-map name map3
```

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
Chapter 130
Exec Mode show Commands (M-P)

This section includes the commands `show mag-service` through `show ps-network statistics`.
The Exec Mode is the initial entry point into the command line interface system. Exec mode `show` commands are useful in troubleshooting and basic system monitoring.

Mode

Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
show mag-service

Displays statistic and counter information for Mobile Access Gateway (MAG) services on this system.

Product
HSGW
S-GW

Privilege
Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show mag-service { all | name service_name | session [ all | callid id | counters | full | ip-address home_ip_address | msid id | summary | username name ] | statistics [ name service_name ] } [ | { grep grep_options | more } ]

all
Displays information for all configured MAG services on this system.

name service_name
Displays configuration information for a specific MAG service configured on this system.

session [ all | callid id | counters | full | ip-address home_ip_address | msid id | summary | username name ]

- all: Displays all active MAG sessions using MAG services on the system.
- callid id: Displays available session information for the specific call identification number.
  id must be an 8-digit hexadecimal number.
- counters: Displays counters for all MAG services on the system. This keyword can also be filtered by the following:
  - all
  - callid
  - ip-address
  - msid
  - summary
  - username

Refer to the keyword descriptions in this command for information regarding these filters.

full: Displays additional session information for all active MAG sessions using MAG services on the system. This keyword includes the information in the output of the all keyword plus additional information. This keyword can also be filtered by the following:
• all
• callid
• ip-address
• msid
• summary
• username

Refer to the keyword descriptions in this command for information regarding these filters.

**ip-address home_ip_address**: Displays available session information for a specific home IPv4 or IPv6 address of a subscriber in a service session.

**msid id**: Displays available information for a specific mobile station identification number or group of numbers based on wildcard entry.

`id` must be a valid MSID number and can be a sequence of characters and/or wildcard characters (‘$’ and/or ‘*’). The ‘*’ wildcard matches multiple characters and the ‘$’ wildcard matches a single character. If you do not want the wildcard characters interpreted as wildcard enclose them in single quotes (‘’). For example: ‘$’.

**summary**: Displays the number of MAG sessions currently active for MAG services configured on the system.

**username name**: Displays available session information for a specific user in a service session.

`name` must be followed by an existing user name expressed as an alphanumeric string of 1 through 127 characters.

```
statistics [ name service_name ]
```

`name service_name`: Displays MAG service statistics for an existing MAG service specified as an alphanumeric string of 1 through 63 characters.

```
| { grep grep_options | more }
```

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the `grep` and `more` commands, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter.

### Usage

Use this command to view configuration information for MAG services on this system.

### Example

The following command displays service statistics for the MAG service named `mag1`:

```
show mag-service name mag1
```
show map-service

Displays information configured for the Mobile Application Part (MAP) services, including MAP service features and operational configuration. Also includes some related configuration information for the HLR and EIR configuration parameters.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
show map-service [ all | name srvc_name ] [ | { grep grep_options | more } ]
```

- `name srvc_name`
  Specifies an existing MAP service as an alphanumeric string of 1 through 63 characters.

- `| { grep grep_options | more }
  Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

**Usage**

Use this command to display all MAP service or the statistics for a particular MAP service.

**Example**

The following command displays configuration information for the MAP service named `map-svc-1`:

```
show map-service name map-srv-1
```

**Important:** Output descriptions for commands are available in the Statistics and Counters Reference.
show map statistics

Displays Mobile Application Part (MAP) statistics.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

**Syntax**

```show map statistics [ name srvc_name ][ | { grep grep_options | more } ]```

- **name srvc_name**
  Specifies an existing MAP service as an alphanumeric string of 1 through 63 characters.

- | { grep grep_options | more }
  Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

  For details on the usage of `grep` and `more`, refer to the *Regulating a Command’s Output* section of the Command Line Interface Overview chapter.

**Usage**

Use this command to display all MAP statistics or the statistics for a particular MAP service.

**Example**

The following command displays statistics for the MAP service named `map-svc-1`:

```show map statistics name map-svc-1```

The following command displays combined statistics for all MAP services in the current context:

**Important:** Output descriptions for commands are available in the Statistics and Counters Reference.
show maximum-temperatures

Shows the maximum temperature reached by each card since the last temperature timestamp reset.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

Syntax

```
show maximum-temperatures [ verbose] [ | { grep grep_options | more } ]
```

- **verbose**
  Indicates that the output is to contain detailed information.

- **| { grep grep_options | more }**
  Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

  For details on the usage of `grep` and `more`, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter.

Usage

Verify the maximum temperature reached by components in the chassis since the indicated timestamp.

**Important:** This command is not supported on all platforms.

Example

```
show maximum-temperatures

show maximum-temperatures verbose
```
show mbms bearer-service

Displays configuration information for bearer services configured for the multimedia broadcast multicast service (MBMS) running on this system.

Product
GGSN
SGSN

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec
The following prompt is displayed in the Exec mode:

[local]\host_name#

Syntax

show mbms bearer-service [ all ] [ apn apn_name mcast-addr ip_address ] [ full ] [ instance instance_id ] [ service-type { broadcast | multicast } ] [ sgsn-sessions ] [ summary ] [ | { grep grep_options | more } ]

all
Displays information on all bearer services configured on the system.

apn apn_name mcast-addr ip_address
Displays bearer service information of the MBMS for a specific Access Point Name (APN). apn_name is bound to a given BM-SC (Broadcast Multicast - Service Center) server address ip_address. apn_name is the name of the APN expressed as an alphanumeric string of 1 through 62 characters that is case sensitive. ip_address is the IP address of the BM-SC server in IPv4 dotted-decimal notation bound to the APN.

full
Displays full information for specific or all instances of bearer service in MBMS feature on system.

instance instance_id
Displays session information filtered for an instance of a bearer service running as an MBMS session and specified an integer from 1 through 64.

service-type { broadcast | multicast }
Displays information for a specific type of service for MBMS. broadcast: Specifies the MBMS service type as broadcast only. multicast: Specifies the MBMS service type as multicast only.

sgsn-sessions
Displays summary information for all the SGSN multicast sessions.
show mbms bearer-service

summary
Displays summary information for specific or all instances of a bearer service.

| { grep grep_options | more }
Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of grep and more options, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage
Use this command to verify the configuration of one or all bearer services and active instances of bearer services under MBMS. It is also useful for monitoring or troubleshooting purposes.
If this command is executed from within the local context with the all keyword, information for all bearer service instances running under MBMS will be displayed.

Example
The following command displays configuration information for all bearer service instances running on system:

```
show mbms bearer-service full all
```

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show mipfa

Displays information for specified Mobile IP Foreign Agent (MIP-FA) calls.

Product

PDSN
GGSN
ASN-GW

Privilege

Security Administrator, Administrator, Operator, Inspector

Mode

Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show mipfa { [ [ counters | full | summary ] { all | callid call_id | msid ms_id | peer-address [ operator ] peer_address | reverse-tunnel { on | off } | username user_name } | statistics [ fa-service fa_name | peer-address [ peer_address | greater-than peer_address | less-than peer_address | > peer_address | < peer_address ] ] ] | peers fa-service service_name [ current-sessions { { > | greater-than } sessions | < sessions } | { < | less-than } sessions [ > sessions | sessions ] ] [ peer-address address ] } [ [ grep grep_options | more ] ]

counters | full | summary

counters: Displayed output includes the statistical counters.
full: Displays detailed information.
summary: Displays only summary information. This is the default setting.
These options are not available in conjunction with the statistics keyword.

all | callid call_id | msid ms_id | peer-address peer_ip_address | reverse-tunnel { on | off } | username user_name

all: Displays all available information.
callid call_id: Displays information only for calls with the call ID specified as a 4-byte hexadecimal number.
msid ms_id: Displays information for a mobile subscriber ID expressed as a string from 7 to 16 digits for an IMSI, MIN, or RMI and/or characters $ and * for wildcard filter.
show mipfa msid 01234567$$
Shows any subscriber with an MSID that matches the upper 8 digits of the supplied MSID, such as 01234567, and any two digits at the remaining two places.
peer-address peer_ip_address: Displays information for the MIP call for the peer IP address specified using IPv4 dotted-decimal notation.
reverse-tunnel { on | off }: Enables the display of reverse IP tunnel information.
username user_name: Displays MIP call user information for the username specified as an alphanumeric string of 1 through 127 characters that may include wildcard characters ($ and *).
show mipfa

```
statistics [ fa-service fa_name | peer-address [ peer_address | greater-than peer_address | less-than peer_address ] ]
```

Displays information for the foreign agent service specified by name or peer IP address.

- `fa-service fa_name` must be an alphanumeric string of 1 through 63 characters.
- `peer-address peer_address` must be specified using IPv4 dotted-decimal notation.
- `greater-than peer_address`: Specifies the range of IPv4 addresses greater than `peer_address`.
- `less-than peer_address`: Specifies the range of IPv4 addresses less than `peer_address`.
- `> peer_address`: Specifies the range of IPv4 addresses greater than `peer_address`.
- `< peer_address`: Specifies the range of IPv4 addresses less than `peer_address`.
- `peer-address [ operator ] peer_address`

In conjunction with the `mipfa [ summary ] peer-address` keyword, indicates a range of peers is to be displayed.

- `peer-address [ operator ] peer_address` must be specified using IPv4 dotted-decimal notation.
- `operator` implies how to logically specify a range of peer-address and it must be one of the following:
  - `<`: IP address is less than the specified `peer_address`
  - `>`: IP address is greater than the specified `peer_address`
  - `greater-than`: IP address is greater than the specified `peer_address`
  - `less-than`: IP address is less than the specified `peer_address`

```
peers fa-service service_name [ current-sessions { { > | greater-than } sessions [ < sessions ] | { < | less-than } sessions [ > sessions ] | sessions } ] [ peer-address address ]
```

Displays peer servers for the specified FA service.

- `fa-service service_name`: Specifies the name of an existing FA service for which the associated peer servers are to be displayed as an alphanumeric string of 1 through 63 characters.
- `current-sessions`: Displays only peer servers with current sessions meeting the following criteria:
  - `>` greater-than sessions: Displays only peer servers currently running sessions higher than the value entered in this parameter. `sessions` must be an integer from 1 to 3000000. Note: the keyword “greater-than” and the “>” symbol are interchangeable in this instance of the command.
  - `< sessions`: Displays only peer servers that are currently running sessions lower than the value entered in this parameter. `sessions` must be an integer from 1 to 3000000. Note: the keyword “less-than” and the “<” symbol are interchangeable in this instance of the command.
  - `>` sessions: Displays only peer servers that are currently running sessions lower than the `less-than` parameter but more than the value entered in this parameter. `sessions` must be an integer from 1 to 3000000.
  - `sessions`: Displays only peer servers currently running sessions that are equal to the value entered in this parameter. `sessions` must be an integer from 1 to 3000000.
- `peer-address address`: Displays only peer servers matching the IP address entered in this parameter. `address` must be specified using IPv4 dotted-decimal notation and can be followed by the netmask of the address.
Exec Mode show Commands (M-P)

show mipfa

| { grep grep_options | more }

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent. For details on the usage of *grep* and *more*, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter.

Usage

View MIP foreign agent information to support troubleshooting subscriber issues by viewing call information and filtering on the subscriber information using various methods.

Example

The following displays the call information for all mobile IP FA calls and statistics for *fa1*, respectively:

```
show mipfa all
```

The following command displays the statistics for the foreign agent service *fa1*:

```
show mipfa statistics fa-service fa1
```

The following commands displays call information for user *user6@aaa* in full detail and in summary:

```
show mipfa full username user6@aaa
show mipfa summary username user1
```

The following displays MIP FA call information for calls from mobile subscriber *4412345678* and peer address *10.2.3.4*, respectively:

```
show mipfa msid 4412345678 4412345678
show mipfa peer-address 10.2.3.4
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference.*
show mipha

Displays information for specified Mobile IP Home Agent (MIP-HA) calls.

Product
HA

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show mipha { [ [ counters | full | summary ] { all | callid call_id | imsi imsi_num | ip-address ip_addr | msid msid_num | peer-address [ operator ] peer_address | reverse-tunnel { on | off } | username user_name ] | statistics [ ha-service ha_name | peer-address peer_address ] ] } | peers ha-service service_name [ current-sessions { { > | greater-than } sessions [ < sessions ] | { < | less-than } sessions [ > sessions ] | sessions } ] [ peer-address address ] } [ [ grep grep_options | more ] ]

counters | full | summary

Default: concise output.
counters: Displayed output includes the statistical counters.
full: Displays detailed information.
summary: Displays only summary information.
These options are not available in conjunction with the statistics keyword.

msid msid_num

Displays information for the subscriber with the supplied MSID on HA.
msid msid_num specifies a mobile subscriber ID for which information is to be displayed. ms_id must be from 7 to 16 digits for an IMSI, MIN, or RMI and/or characters $ and * for wildcard filtering.
If enforce imsi-min equivalence is enabled on the chassis and MIN or IMSI numbers are supplied, this keyword/filter will show subscribers with a corresponding MSID (MIN or IMSI) whose lower 10 digits matches the lower 10 digits of the supplied MSID.
show mipha msid ABCD0123456789 or
show mipha msid 0123456789
Shows any subscriber with a MSID that matches the lower 10 digits of MSID supplied, such as 0123456789.
show mipha msid 01234567$$
Shows any subscriber with a MSID that matches the upper 8 digits of the supplied MSID, such as 01234567 and any two digits at the remaining two places.

all | callid call_id | imsi imsi_num | ip-address ip_addr | msid msid_num | peer-address [ operator ] peer_address | reverse-tunnel { on | off } | username user_name

all: Displays all available information.
**callid call_id**: Displays information only for calls with the call ID specified as a 4-byte hexadecimal number.

**imsi imsi_num**: Specifies an IMSI (international mobile subscriber ID) for which information is to be displayed. The IMSI is a 15-character field which identifies the subscriber’s home country and carrier.

**ip-address ip_addr**: Displays statistics for a call with the IP address specified in IPv4 dotted-decimal notation.

**msid msid_num**: Specifies a mobile subscriber ID only for which information is to be displayed. ms_id must be from 7 to 16 digits specified as an IMSI, MIN, or RMI.

**peer-address peer_address**: Displays statistical information for the peer IP address specified using IPv4 dotted-decimal notation.

**reverse-tunnel { on | off }**: Enables the display of reverse IP tunnel information.

**username user_name**: Displays user MIP call information for the username specified as an alphanumeric string of 1 through 127 characters including wildcard characters ($ and *).

**peer-address [ operator ] peer_address**

In conjunction with mitha [ summary ] peer-address keyword, indicates a range of peers is to be displayed. peer_address must be specified using IPv4 dotted-decimal notation.

operator implies how to logically specify a range of peer-addresses and it must be one of the following:

- `<`: IP address is less than the specified peer_address
- `>`: IP address is greater than the specified peer_address
- `greater-than`: IP address is greater than the specified peer_address
- `less-than`: IP address is less than the specified peer_address

**statistics [ ha-service ha_name | peer-address peer_address ]**

Displays statistical information for the home agent service specified by its name (an alphanumeric string of 1 through 63 characters) or peer IP address (IPv4 notation).

**peers ha-service service_name [ current-sessions { { > | greater-than } sessions [ { < sessions ] | { < | less-than } sessions [ > sessions ] | sessions } } [ peer-address address ]**

Displays peer servers for the specified HA service.

ha-service service_name: Specifies the name of an existing HA service for which the associated peer servers are to be displayed as an alphanumeric string of 1 through 63 characters.

current-sessions: Displays only peer servers with current sessions meeting the following criteria:

- `>`: greater-than sessions: Displays only peer servers currently running sessions higher than the value entered in this parameter. sessions must be an integer from 1 to 3000000. Note: the keyword “greater-than” and the “>” symbol are interchangeable in this instance of the command.

- `< sessions`: Displays only peer servers that are currently running sessions higher than the greater-than parameter but less than the value entered in this parameter. sessions must be an integer from 1 to 3000000.

- `>`: greater-than sessions: Displays only peer servers currently running sessions lower than the value entered in this parameter. sessions must be an integer from 1 to 3000000. Note: the keyword “less-than” and the “<” symbol are interchangeable in this instance of the command.

- `>`: greater-than sessions: Displays only peer servers that are currently running sessions lower than the less-than parameter but more than the value entered in this parameter. sessions must be an integer from 1 to 3000000.
- **sessions**: Displays only peer servers currently running sessions that are equal to the value entered in this parameter. `sessions` must be an integer from 1 to 3000000.

- **peer-address address**: Displays only peer servers matching the IP address entered in this parameter. `address` must be specified using IPv4 dotted-decimal notation and can be followed by the netmask of the address.

```bash
| { grep grep_options | more }
```

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of `grep` and `more`, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter.

### Usage

View MIP home agent information to support troubleshooting subscriber issues by viewing call information and filtering on the subscriber information using various methods.

### Example

The following displays the call information for all mobile IP HA calls and statistics for `ha1`, respectively:

```bash
show mipha all
show mipha statistics ha-service ha1
```

The following commands displays call information for user `isp1user1` in full detail and in summary:

```bash
show mipha full username isp1user1
show mipha summary username user1
```

The following displays MIP-HA call information for calls from mobile subscribers with reverse tunneling `off` and peer address `10.2.3.4`, respectively:

```bash
show mipha reverse-tunnel off
show mipha peer-address 10.2.3.4
```

**Important**: Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show mipv6ha

Displays information for specified Mobile IPv6 Home Agent (MIPv6-HA) calls.

**Product**
PDSN
HA

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
show mipv6ha [ all | callid call_id | counters filter | full filter | ipv6-address ip_addr| statistics mipv6ha-service mipv6ha-service_name | summary filter | username user_name ]
```

- **all**
  Displays all information for MIPv6-HA calls.

- **callid call_id**
  Specifies the Call Identification number as an 8-digit hexadecimal number.

- **counters [ all | callid | ipv6-address | username ]**
  Displays the counters associated with the MIPv6-HA service. The following filters are available:
  - `all`
  - `callid`
  - `ipv6-address`
  - `username`

- **full [ all | callid | ipv6-address | username ]**
  Displays all available information for the associated display or filter keyword. The following filters are available:
  - `all`
  - `callid`
  - `ipv6-address`
  - `username`

- **ipv6-address ip_addr**
  Displays information for subscribers connected via the packet control function for a specific or range of IPv6 addresses. The address must be specified using the IPv6 colon-separated-hexadecimal notation.
• <: Filters output so that only information less than the specified IPv6 address value is displayed.
• >: Filters output so that only information greater than the specified IPv6 address value is displayed.
• \texttt{less-than}: Filters output so that only information less than the specified IPv6 address value is displayed.
• \texttt{greater-than}: Filters output so that only information greater than the specified IPv6 address value is displayed.

\texttt{statistics [ mipv6ha-service mipv6ha-service_name ]}

Displays all information collected for specific protocol since last the \texttt{restart} or \texttt{clear} command. This can be filtered according to a specified \texttt{mipv6ha-service}.

\texttt{summary [ all | callid | ipv6-address | username ]}

Displays summary information for defined sessions, based on defined parameters. The following filters are available:
• \texttt{all}
• \texttt{callid}:
• \texttt{ipv6-address}
• \texttt{username}

\texttt{username user_name}

Displays session information for a specific username.

\section*{Usage}

View MIPv6 home agent information to support troubleshooting subscriber issues by viewing call information and filtering on the subscriber information using various methods.

\section*{Example}

The following displays the call information for all mobile IPv6 HA calls:

\begin{verbatim}
show mipv6ha all
\end{verbatim}

The following command displays call information for user \texttt{mipv6hauser1} in full detail and in summary:

\begin{verbatim}
show mipv6ha full username mipv6hauser1
\end{verbatim}

\textbf{Important:} Output descriptions for commands are available in the \textit{Statistics and Counters Reference}.  

---

Cisco ASR 5x00 Command Line Interface Reference
show mme-service

Displays configuration information for Mobility Management Entity (MME) services on this system.

**Product**
MME

**Privilege**
Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
show mme-service { all | name svc_name [ offload statistics ] } [ | { grep grep_options | more } ]
```

- **all**
  Displays configuration information for all MME services configured on this system.

- **name service_name**
  Displays configuration information for an existing MME service specified as an alphanumeric string of 1 through 63 characters.

- **offload statistics**
  Displays configuration information for the MME load rebalancing feature (UE offload), as well as current statistics about any active offloading processes.
  This keyword option is only available in Release 14.0 and higher.

- **| { grep grep_options | more }**
  Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
  For details on the usage of the `grep` and `more` commands, refer to the *Regulating a Command’s Output* section in the *Command Line Interface Overview* chapter.

**Usage**

Use this command to view configuration information for MME services on this system.

**Example**

The following command displays service statistics for the MME service named `mme1`:

```
show mme-service name mme1
```

**Important:** Output descriptions for these commands are available in the *Statistics and Counters Reference*. 
show mme-service db record

Displays the Mobile Management Entity (MME) database records for MME sessions grouped in session instances on this system and filtered with IMSI or GUTI as criteria.

**Product**
MME

**Privilege**
Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name# 
```

**Syntax**

`show mme-service db record { all | call-id call_id | guti plmn plmn_id group-id mme_grp_id code mme_code m-tmsi mtmsi_value | imsi imsi_identifier }`

- **all**
  Displays all database records of a session instance used for MME service.

- **call-id call_id**
  Displays database records filtered by the call ID specified as an 8-digit hexadecimal number.

- **guti plmn plmn_id group-id mme_grp_id code mme_code m-tmsi mtmsi_value**
  Displays database records filtered by the Globally Unique Temporary Identifier (GUTI). The GUTI is constructed from the GUMMEI and the M-TMSI.
  The GUMMEI is constructed from the public land mobile network (PLMN) ID [MMC and MNC] and the MME Group ID (MMEGI). Within the MME, the mobile is identified by the M-TMSI.
  A GUTI has: 1) a unique identity for the MME which allocated the GUTI; and 2) the unique identity of the UE within the MME that allocated the GUTI.
  The MME Identifier (MMEI) is constructed from an MME Group ID (MMEGI) and an MME Code (MMEC).

- **imsi imsi_identifier**
  Displays database records filtered by International Mobile Subscriber Identity (IMSI).
  **imsi_identifier** is a 15-character IMSI field which identifies the subscriber’s home country and carrier.
  Wildcard characters $ and * are allowed. The * wildcard matches multiple characters and the $ wildcard matches a single character. If you do not want the wildcard characters interpreted as a wildcard enclose them in single quotes (’’). For example; ‘$’.

**Usage**

Use this command to view database records for all or a particular instance of session manager for MME services on this system with IMSI or GUTI as a filter criteria.

**Example**

Cisco ASR 5x00 Command Line Interface Reference

4520
The following command displays the summary database records of a session instance for a subscriber having IMSI as 123455432112345 in the MME service:

```
show mme-service db record imsi 123455432112345
```

**Important:** Output descriptions for these commands are available in the *Statistics and Counters Reference*. 
**show mme-service db statistics**

This command displays the Mobile Management Entity (MME) database statistics for all or specific MME sessions on this system.

**Product**
MME

**Privilege**
Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
show mme-service db statistics [ instance smgr_instance ]
```

<table>
<thead>
<tr>
<th>instance smgr_instance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Displays MME database statistics for a specific instance of a session manager running the MME service.</td>
</tr>
<tr>
<td>smgr_instance is an instance ID specified as an integer from 0 through 4294967295. If an instance is not specified, summary statistics are displayed.</td>
</tr>
</tbody>
</table>

**Usage**

Use this command to view database statistics for all or a particular instance of session manager for MME services on this system.

**Example**

The following command displays summary database statistics for the MME service running on a system:

```
show mme-service db statistics
```

**Important:** Output descriptions for these commands are available in the Statistics and Counters Reference.
show mme-service enodeb-association

Displays configuration information for an eNodeB association within an MME service.

**Product**
MME

**Privilege**
Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
show mme-service enodeb-association [ summary | full | path-info ] [ all | enodeb-name enodeb_name | ipsec | mme-service-name mme_svc_name | peer-address peer_ip_address | peer-id peer_identifier ] [ | { grep grep_options | more } ]
```

- **summary**
  Displays summarized output for this command.

- **full**
  Displays detailed output for this command.

- **path-info**
  Displays S1 path association information of eNodeBs associated with MME services on this system.

- **all**
  Displays information of all eNodeBs associated with MME services on this system.

- **enodeb-name enodeb_name**
  Displays information for the specified eNodeB associated with MME services on this system.

- **ipsec**
  Displays information of all IPSec enabled eNodeBs associated with MME services on this system.

- **mme-service-name mme_svc_name**
  Displays summarized or detailed configuration information for eNodeBs associated with an existing MME service specified as an alphanumeric string of 1 through 63 characters.

- **peer-address peer_ip_address**
  Displays summarized or detailed configuration information of eNodeBs associated with an existing MME peer IP address configured with an MME service and expressed in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.
peer-id peer_identifier
Displays summarized or detailed configuration information for eNodeBs associated with an existing MME peer ID configured with an MME service and specified as an integer from 1 through 4294967295.

| { grep grep_options | more }
Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of the grep and more commands, refer to the Regulating a Command’s Output section in the Command Line Interface Overview chapter.

Usage
Use this command to view configuration information of eNodeBs associated with an MME service on this system.

Example
The following command displays detailed service statistics for associated eNodeBs within the MME service named ingress:

    show mme-service enodeb-association full mme-service-name ingress

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show mme-service id

This command displays the current number of MME-assigned and eNodeB-assigned S1AP session IDs.

**Product**
MME

**Privilege**
Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
show mme-service id summary [ | { grep grep_options | more } ]
```

<table>
<thead>
<tr>
<th>id summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Displays the current number of MME-assigned and eNodeB-assigned S1AP session IDs.</td>
</tr>
</tbody>
</table>

| | { grep grep_options | more } |
|---|
| Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent. |
| For details on the usage of the `grep` and `more` commands, refer to the *Regulating a Command’s Output* section in the *Command Line Interface Overview* chapter. |

**Usage**

Use this command to display the current number of MME-assigned and eNodeB-assigned S1AP session IDs.
show mme-service session

Displays session information for Mobile Management Entity (MME) service(s) running on a peer or local system.

Product
MME

Privilege
Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

```plaintext
show mme-service session [ summary | full | counters ] [ all | callid call_identifier | imei imei_id | imsi imsi_id | ipsec | mme-service service_name | msisdn number | pdn-address pdn_ip_address | sl-peer sl_peer_ip_address | s1-peer s1_peer_ip_address | vlr-name vlr_name | ue-ecm-state { connected | idle } ] [ | { grep grep_options | more } ]
```

**summary**
Displays summarized output for this command.

**full**
Displays detailed output for this command.

**counters**
Displays all counters for related events and messages for an MME session running on a system.

**all**
Displays information for all MME sessions running on this system.

**callid call_identifier**
Displays summarized or detailed configuration information for an MME session filtered by a call identifier within an MME service configured on this system. call_identifier must be an existing call identity in 8-digit hexadecimal format running in an MME service on this system.

**imei imei_id**
Displays summarized or detailed configuration information about MME sessions running and filtered by an International Mobile Equipment Identification (IMEI) number within an MME service configured on this system. imei_id must be an existing IMEI in an existing MME service on the system. imei_id must contain an 8-digit TAC (Type Allocation Code) and a 6-digit SNR (Serial Number).
Show MME Service Session

```plaintext
imsi  imsi_id
```
Displays summarized or detailed configuration information about MME sessions running and filtered by an International Mobile Subscriber Identity (IMSI) number within an MME service configured on the system. `imsi_id` must be an existing IMSI in an existing MME service on the system. `imsi_id` is a 15-character IMSI field which identifies the subscriber’s home country and carrier. Wildcard characters $ and * are allowed. The * wildcard matches multiple characters and the $ wildcard matches a single character. If you do not want the wildcard characters interpreted as a wildcard enclose them in single quotes (‘’). For example; ‘$’.

```plaintext
ipsec
```
Displays information for all IPSec enabled sessions using MME services on the system.

```plaintext
mme-service  service_name
```
Displays summarized or detailed configuration information about MME sessions running and filtered by an MME service name configured on the system. `service_name` must be a configured MME service on the system, expressed as an alphanumeric string of 1 through 63 characters.

```plaintext
msisdn  number
```
Displays summarized or detailed configuration information about MME sessions running and filtered by a Mobile Station International ISDN Number. `number` must be a combination of the CC (Country Code) and National (significant) mobile number, not exceeding 15 digits.

```plaintext
pdn-address  pdn_ip_address
```
Displays summarized or detailed configuration information about MME sessions running and filtered by the IP address of a connected PDN(s) within an MME service configured on this system. `pdn_ip_address` must be a configured IP address of a PDN expressed in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation within an existing MME service on the system.

```plaintext
s1-peer  s1_peer_ip_address
```
Displays summarized or detailed configuration information of MME sessions running and filtered by the IP address of a peer connected through an S1 interface within an MME service configured on this system. `s1_peer_ip_address` must be a configured IP address of a peer on S1 interface expressed in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation within an existing MME service on the system.

```plaintext
s11-peer  s11_peer_ip_address
```
Displays summarized or detailed configuration information of MME sessions running and filtered by IP address of a peer connected through S11 interface with an MME service configured on this system. `s11_peer_ip_address` must be a configured IP address of a peer on S11 interface expressed in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation within an existing MME service on this system.

```plaintext
vlr-name  vlr_name
```
Displays summarized or detailed configuration information of MME sessions running and filtered by Visitor Location Register (VLR) name. `vlr_name` must be an alphanumeric string of 1 through 63 characters.
**show mme-service session**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
</table>
| Show MME service session | The status of MME sessions on the system can be viewed using the `show mme-service session` command. This command displays information about MME sessions running on the system, including their state, QoS, and other relevant details.

**Usage**

**Example**

The following command displays detailed session statistics for an MME service running on this system:

```bash
show mme-service session full
```

**Important:** Output descriptions for these commands are available in the *Statistics and Counters Reference.*

The following command displays detailed session counters for an MME service running on this system:

```bash
show mme-service session counters
```
show mme-service statistics

This command displays MME service statistics specified by various criteria.

Product
MME

Privilege
Security Administrator, Administrator

Mode
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show mme-service statistics [ emm-only | esm-only | handover | mme-service \ mme_svc_name [ emm-only | esm-only | handover | slap | sctp ] | peer-id \ peer_identifier [ emm-only | esm-only | handover | slap | sctp ] | verbose ] [ | { grep \ grep_options | more } ]

display

emmm-only
Displays only EPS mobility management (EMM) related statistics, or filters EMM statistics for a specific MME service name or a specific eNodeB association peer identifier.

emsm-only
Displays only EPS session management (ESM) related statistics, or filters ESM statistics for a specific MME service name or a specific eNodeB association peer identifier.

handover
Displays only handover related statistics (such as Intra-MME, EUTRAN<>EUTRAN via S10, EUTRAN<>UTRAN via GnGp, EUTRAN<>GERAN via GnGp, and EUTRAN<>UTRAN via S3), or filters handover statistics for a specific MME service name or a specific eNodeB association peer identifier.

mme-service \ mme_svc_name
Displays MME service statistics for only the specified MME service name.

peer-id \ peer_identifier
Displays MME service statistics for only the specified eNodeB association peer identifier.

slap
Displays only S1-AP related statistics, or filters S1-AP statistics for a specific MME service name or a specific eNodeB association peer identifier.
show mme-service statistics

**sctp**
Displays only SCTP related statistics, or filters SCTP statistics for a specific MME service name or a specific eNodeB association peer identifier.

**verbose**
Displays comprehensive information for a specific argument or set of arguments.

```
| { grep grep_options | more }
```
Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of the `grep` and `more` commands, refer to the *Regulating a Command’s Output* section in the *Command Line Interface Overview* chapter.

**Usage**
This command is used to display the statistical information of MME services based on various filter criteria.

**Example**
The following command displays all service statistics for all MME services on a system:

```
show mme-service statistics
```
The following command displays the service statistics of all MME services on a system related to S1-AP:

```
show mme-service statistics s1ap
```
The following command displays only EMM related statistics for the only the MME service named *ingress*:

```
show mme-service statistics mme-service ingress emm-only
```
show module

Displays the current status of the Version Priority List (VPL) for one or all plugin modules installed on the system. This command is associated with the dynamic software upgrade process.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

```
show module [ plugin_name ]
```

`plugin_name`
Filters the output of the VPL by an existing plugin name expressed as an alphanumeric string of 1 through 16 characters.

Usage
Display the priority, load status, location, installation timestamp and download status of one or all plugin modules. A plugin module is a shared object library that can be dynamically updated or rolled back. Refer to the System Administration Guide for additional information on dynamic software updates.

Example
The following command displays the VPL status of all plugin modules currently installed on the system:

```
show module
```
show mpls cross-connect

Displays Multiprotocol Label Switching (MPLS) cross-connect information.

Product
GGSN

Privilege
Security Administrator, Administrator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

```
show mpls cross-connect [ | { grep grep_options | more } ]
```

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the `grep` and `more` commands, refer to the Regulating a Command’s Output section in the Command Line Interface Overview chapter.

Usage

This command displays MPLS cross-connect information. MPLS tunnel cross-connects between interfaces and Label-Switched Paths (LSPs) connect two distant interface circuits of the same type by creating MPLS tunnels that use LSPs as the conduit.

Example

The following command displays MPLS cross-connect information:

```
show mpls cross-connect
```

**Important:** Output descriptions for these commands are available in the Statistics and Counters Reference.
show mpls ftn

Displays MPLS FEC-to-NHLFE (FTN) table information.

Product
GGSN

Privilege
Security Administrator, Administrator

Mode
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

    show mpls ftn [ vrf vrf_name ] [ | { grep grep_options | more } ]

vrf vrf_name
Displays FTN information for the Virtual Routing and Forwarding (VRF) specified as an alphanumeric string of 1 through 63 characters.

| { grep grep_options | more }

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of the grep and more commands, refer to the Regulating a Command’s Output section in the Command Line Interface Overview chapter.

Usage
This command displays MPLS FEC (Forward Error Correction)-to-NHLFE (Next-Hop label Forwarding Entry) table information.

Example
The following command displays MPLS FTN information:

    show mpls ftn

Important: Output descriptions for these commands are available in the Statistics and Counters Reference.
show mpls ilm

Displays MPLS Incoming Label Map (ILM) table information.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
show mpls ilm [ fec | label label_value | verbose ] [ | { grep grep_options | more } ]
```

**fec**
Displays Forwarding Equivalency Class (FEC) information.

**label label_value**
Displays MPLS ILM information for the specified label. label_value is an integer from 16 through 1048575.

**verbose**
Displays detailed information for the MPLS ILM table.

```
| { grep grep_options | more }
```

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent. For details on the usage of the `grep` and `more` commands, refer to the *Regulating a Command’s Output* section in the *Command Line Interface Overview* chapter.

**Usage**
This command displays MPLS Incoming Label Map (ILM) table information.

**Example**

The following command displays information for MPLS ILM information:

```
show mpls ilm
```

**Important:** Output descriptions for these commands are available in the *Statistics and Counters Reference*. 
show mpls ldp

Displays MPLS Label Distribution Protocol (LDP) information.

Product
GGSN

Privilege
Security Administrator, Administrator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show mpls ldp { bindings [ ldp-id IPv4_addr | local [ ldp-id | local | prefix | remote ] | prefix IPv4_addr | remote ] | discovery | neighbor [ detail | ldp-id ] }

bindings
Displays the MPLS LDP label bindings.

ldp-id
Displays label values for a specific peer LDP ID.

local
Displays locally assigned label values.

prefix
Displays label values for a specific prefix.

remote
Displays remotely assigned label values.

discovery
Displays the MPLS LDP discovery information.

neighbor
Displays the MPLS LDP peer information.

detail
Displays the MPLS LDP peer information in details. The displayed information includes, Local LDP ID, Peer LDP ID, Transport address, State (for example, Established), Role (for example, Active), Uptime, Keepalive negotiated hold time, Proposed Local/Peer, Remaining Keepalive hold time, and Address advertised.
Usage
This command displays statistical information for an MPLS Label Distribution Protocol configuration. The information includes Prefix, LDP ID, Label, Nexthop, and Egress_if_index for all MPLS LDP Bindings configurations.

Example
The following command displays information about MPLS LDP protocol related configurations:

```
show mpls ldp discovery neighbor ldp-id 10.2.3.4 detail bindings ldp-id 31.32.33.34 prefix 192.168.102.232 local remote
```

The following command displays the MPLS LDP discovery information, including, LDP Peer IDs, Hold time (in seconds), Proposed Local/Peer, and Remaining (time in seconds):

```
show mpls ldp discovery
```

The following command displays the remotely assigned label values in the MPLS LDP binding configuration:

```
show mpls ldp bindings remote
```

**Important:** Output descriptions for these commands are available in the Statistics and Counters Reference.
show mpls nexthop-label-forwarding-entry

Displays MPLS Next-Hop Label Forwarding Entry (NHLFE) table information.

Product
GGSN

Privilege
Security Administrator, Administrator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show mpls nexthop-label-forwarding-entry [ | { grep grep_options | more } ]

| { grep grep_options | more }

Pipes (sends) the output of the command to the command specified. You must specify a command to which
the output will be sent.
For details on the usage of the grep and more commands, refer to the Regulating a Command’s Output
section in the Command Line Interface Overview chapter.

Usage

This command displays MPLS Next-Hop Label Forwarding Entry (NHLFE) table information.

Example

The following command displays MPLS NHLFE information:

    show mpls nexthop-label-forwarding-entry

Important: Output descriptions for these commands are available in the Statistics and Counters Reference.
show mrme-service

Displays configuration and/or statistical information for MRME services on this system.

Product
SaMOG

Privilege
Security Administrator, Administrator, Operator, Inspector

Syntax

```
show mrme-service { all | name name | statistics { all [ verbose ] | dns-stats | name name [ dns-stats ] } } [ | { grep grep_options | more } ]
```

- **all**
  Displays all MRME services.

- **name name**
  Displays information for specific MRME service name.
  `name` is a string of size 1 to 63.

- **statistics**
  Displays Node level Statistics for MRME.

- **verbose**
  Specifies Detailed statistics.

- **dns-stats**
  Specifies the information related to the DNS selection of P-GW.

  `| { grep grep_options | more }`

  Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
  For details on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage
Use this command to displays configuration and/or statistical information for MRME services on this system.

Example

```
show mrme-service all
```
show mseg-config

This command is not supported in this release.
show mseg-service

This command is not supported in this release.
show multicast-sessions

Displays information for multicast sessions defined by the specified keywords.

Product

PDSN
GGSN

Privilege

Security Administrator, Administrator, Operator, Inspector

Mode

Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show multicast-sessions [ command_keyword ] [ filter_keywords ] [ | { grep grep_options | more }]

command_keyword

The following keywords are base commands that each have a distinct display output. Only one keyword can be entered on the command line.

debug-info { callid id | flowid id }

Displays internal call troubleshooting information for multicast sessions defined by the specified keywords. 

**callid id**: Displays subscriber information for the call specified as an 8-digit hexadecimal number. 

**flowid id**: Displays information for a specific BCMCS flow, defined by the flow ID as a hexadecimal number.

full

Displays all available multicast session information. The following filter keywords are valid for this command: active, all, callid, card-num, dormant, flowid, flowid-type, mcast-address, pcf, pdsn-service, grep, more

summary

Only displays a summary of multicast session information. The following commands are valid for this command: active, all, callid, card-num, dormant, flowid, flowid-type, mcast-address, pcf, pdsn-service, grep, more

filter_keywords

The following keywords are filters that modify or filter the output of the Command Keywords. Not all filters are available for all Command Keywords. Multiple Filter Keywords can be entered on a command line. When multiple Filter Keywords are specified, the output conforms to all of the Filter Keywords specifications.
**active**

Only displays information for multicast sessions that are currently active.

**all**

If no keywords are specified before **all**, information for all multicast sessions is displayed. If keywords are specified before **all**, all information is displayed with no further options being allowed.

**callid id**

Displays multicast session information for the call specified by **id**. The call must be specified as an 8-digit hexadecimal number.

**card-num card_num**

The slot number of the processing card by which the subscriber session is processed. **card_num** is a slot number from 1 through 7 or 10 through 16 on the ASR 5000, or 1 through 4 or 7 through 10 on the ASR 5500.

**dormant**

Shows information for subscriber sessions that are dormant (not transmitting or receiving data).

**flowid id**

Displays information for a specific BCMCS flow, defined by **id**. The flow ID must be a hexadecimal number.

**flowid-type [ flow | program ]**

Displays information for multicast sessions according to the type of flow.

**flow**: Shows all multicast sessions for the flow ID type “flow”.

**program**: Shows all multicast sessions for the flow ID type “program”.

**mcast-address ipv4_address**

Show multicast sessions for a specific multicast address. Must be followed by the IP address of an interface, using IPv4 dotted-decimal notation.

**pcf ipv4_address**

Displays information for multicast sessions connected via the packet control function, defined by **ipv4_address**. The address must be specified using IPv4 dotted-decimal notation.

**pdsn-service svc_name**

Displays information for multicast session connected to the packet data service **svc_name**. The packet data service must have been previously configured and expressed as an alphanumeric string of 1 through 63 characters.

| { grep grep_options | more }

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

Please refer to the *Regulating a Command’s Output* section in the *Command Line Interface Overview* chapter for details on the usage of **grep** and **more**.
show multicast-sessions

Usage
Use this command to view information about multicast sessions.
The output of this command may be considered for part of a periodic system auditing program by verifying active and dormant sessions.

Example
The following command displays the all broadcast-multicast sessions active in a context/system:

```plaintext
show multicast-sessions all
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference.*
show network-requested-pdp-context

Displays information for the specified network-requested packet data protocol (PDP) context.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

**Syntax**

```
show network-requested-pdp-context imsi imsi_value
```

**Usage**

Use this command to display information pertaining to network-requested PDP contexts.

**Example**

The following command displays network-requested PDP context information for a subscriber with an IMSI of 123456789:

```
show network-requested-pdp-context imsi 123456789
```
show network-service-entity

Displays information regarding the network service entities (NSEs) in the network.

Product
SGSN

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show network-service-entity { consolidated-status | fr-config [ peer-nsei nsei ] | ip-config [ nsvl { all | instance value } ] }

---

consolidated-status
Displays Network Service Virtual Connection (NSVC) status information for all network service entities in the network. This keyword is particularly useful for troubleshooting.

---

fr-config [ peer-nsei nsei ]
Displays network service configurations for NSEs using Frame Relay configurations.
peer-nsei nsei limits the display to a specific peer NSE identified as an integer from 0 through 65535.

---

ip-config [ nsvl { all | instance value } ]
Displays network service configurations for NSEs using IP configurations.
Including the nsvl keyword limits the display to all or a single (instance 0 to 3) of a network service virtual link.

Usage
Use this command to display NSE information pertaining to the NSVCs of the NSEs in the networks or NSEs configured for Frame Relay or IP.

Example
The following command displays the status of all the NSVCs for all the NSEs in the network.

show network-service-entity consolidated-status
show npu error-counters

Displays packet error counters.

Product
ASR 5000 only

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec
The following prompt is displayed in the Exec mode:

[local]\ host_name#

Syntax

```
show npu error-counters [ | { grep grep_options | more } ]
```

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage
View network timing protocol information to troubleshooting system clock issues by displaying the associations and status of the local NTP client.

Example
The following displays the NPU information.

```
show npu error-counters
```

```
show npu error-counters | grep qwe
```
show npu utilization

Displays NPU information utilization.

Product
ASR 5000, ASR 5500

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show npu utilization table { | { grep grep_options | more } }

| { grep grep_options | more }

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter.

Usage

View network timing protocol information to troubleshooting system clock issues by displaying the associations and status of the local NTP client.

Example

The following displays the NPU information.

```
show npu utilization table

show npu utilization table | grep qwe
```
show ntp

Displays the network timing protocol (NTP) associations and status.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show ntp { associations | status } [ address ip_address ] [ | { grep grep_options | more } ]

associations
Displays the current NTP server associations and related statistics.

status
Displays the client permeates configured and the synchronization status.

address ip_address
Specifies the IP address of an NTP server/client in the current context in IPv4 dotted-decimal notation.

| { grep grep_options | more }

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage

View network timing protocol information to troubleshooting system clock issues by displaying the associations and status of the local NTP client.

Example

The following displays the NTP associations and status, respectively.

show ntp associations
show ntp status

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show nw-reachability server

Displays the configuration of network reachability servers for the current context.

Product
HA

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec
The following prompt is displayed in the Exec mode:
[local]host_name#

Syntax

```
show nw-reachability server { all | ipv4-only | ipv6-only | name server_name }
```

- **all**
  Displays configuration information for all network reachability servers in the current context.

- **ipv4-only**
  Displays IPv4 Network Reachability Detection servers.

- **ipv6-only**
  Displays IPv6 Network Reachability Detection servers.

- **name server_name**
  Displays configuration information for an existing network reachability server specified as an alphanumeric string of 1 through 15 characters.

Usage
Use this command to display configuration information on network reachability servers configured in the current context.

Example
The following command displays information on all network reachability servers in the current context:

```
show nw-reachability server all
```

**Important:** Output descriptions for commands are available in the Statistics and Counters Reference.
show operator-policy

Displays the information configured for an operator policy.

**Product**

MME
SAEGW
S-GW
SGSN

**Privilege**

Inspector

**Mode**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
show operator-policy { all | full { all | name op_policy_name } | name op_policy_name } [ | { grep grep_options | more } ]
```

- **all**
  Displays a list of all operator policies configured on the system.

- **full { all | name op_policy_name }**
  - **full**: Displays a full set of available information for the specified operator policy (policies).
  - **all**: Displays a full set of available information for all operator policies configured on the system.
  - **name op_policy_name**: Displays a full set of available information for an existing operator policy specified as an alphanumeric string of 1 through 64 characters.

- **name op_policy_name**
  Displays a full set of available information for an existing operator policy specified as an alphanumeric string of 1 through 64 characters.

  | { grep grep_options | more } |

  Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

  For details on the usage of **grep** and **more**, refer to the *Regulating a Command’s Output* section in the *Command Line Interface Overview* chapter.

**Usage**

Use this command to display information for operator policies configured on the system. Operator policies are configured through the Global Configuration Mode and in the Operator Policy Configuration Mode. For
more information regarding operator policy commands, refer to the *Operator Policy Configuration Mode Commands* chapter.

**Example**

The following command displays all available information for an operator policy named *policy-5*:

```bash
show operator-policy full name policy-5
```
show orbem

Displays information and statistics for the Object Request Broker Element Manager (ORBEM) interface in the current context.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show orbem { client { id client_name | table } | event-notif-service filters | session { id session_name | table } | status } [ | { grep grep_options | more } ]

client { id client_name | table }
Indicates the Common Object Request Broker Architecture (CORBA) client information is to be displayed. The keyword table is used to output to the display information on all configured clients. The keyword id is used to specify a specific client for which information is to be displayed specified as client_name. client_name must refer to an existing client which is found using the table keyword option.

event-notif-service filters
Displays information pertaining to filters configured for the ORB Notification Service.

Important: In 18.0 and later releases, this keyword is obsolete.

session { id session_name | table }
Indicates session information is to be displayed. The keyword table is used to output to the display information on all configured clients. The keyword id is used to specify a specific session for which information is to be displayed specified as session_name. session_name must refer to an existing session which is found using the table keyword option.

status
Indicates that the ORBEM server status information is to be displayed.

| { grep grep_options | more }
Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of grep and more, refer to the Regulating a Command’s Output section in the Command Line Interface Overview chapter.
Usage
Display current sessions when ORBEM system response may appear sluggish. This command is also useful in periodic verification of the server status.

Example
The following commands will display the information for all clients.

```bash
show orbem client table
```

The following commands display the information for the `clientName` and `sessionID`, respectively:

```bash
show orbem client id clientName
show orbem session id sessionId
```

The following command displays the ORBEM server status:

```bash
show orbem status
```

The following command displays the information for all sessions:

```bash
show orbem session table
```

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show patch progress

Displays the status of the on-going software patch installation.

**Product**
All

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
show patch progress
```

**Usage**

Use this command to show the status of an on-going software patch installation.

**Important:** Software Patch Upgrades are not supported in this release.
show pcc-af service

Displays the statistical and configuration information of configured Policy and Charging Control- Application Function (PCC-AF) services configured in a context.

Product
IPCF

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show pcc-af service [ statistics ] { all | name pcc_af_svc_name | summary } [ | { grep grep_options | more } ]

- `all`: displays information for all configured PCC-AF services.
- `name pcc_af_svc_name`: Displays information only for an existing PCC-AF service specified as an alphanumeric string of 1 through 79 characters
- `statistics`: Displays the statistical information for a specific service or all PCC-AF services configured in a context.
- `summary`: Displays the summarized output of this command.

Usage

Use this command to display the statistical and configuration information of configured PCC-AF services configured in a context.

Display can further be filtered for specific PCC-AF service name or summarized output of the command.

Example

The following command displays the information for the PCC-AF service named `pccApp1` in summarized output:
show pcc-af service name pccApp1 summary

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference.*
show pcc-af session

Displays the active/dormant session information about Policy and Charging Control- Application Function (PCC-AF) service instances configured and running on this system based on different filter criteria.

Product
IPCF

Privilege
Inspector

Mode
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show pcc-af sessions [ full | summary] [ all ] [ apn | call-id call_id | ip-address pcc_af_ip_address | service pcc_af_svc_name | sipuri sip_uri ] [ | { grep grep_options | more } ]

full
Displays the full information of specific registered IP Connectivity Access Network (IP-CAN) session(s) on a PCC-AF service instance running on system. Display can be filtered based on given filtering criteria.

summary
Displays summarized information for specific registered IP-CAN session(s) on a PCC-AF service instance running on system. Display can be filtered based on given filtering criteria.

all
Displays summarized or full information for all registered IP-CAN session(s) on a PCC-AF service instance running on system. Display can be filtered based on given filtering criteria.

apn apn_name
Displays information for PCC-AF service sessions connected via an existing APN at the Policy and Charging Enforcement Function (PCEF).

ip-address pcc_af_ip_address
Filters the display of full or summarized session statistics for IP-CAN session(s) based on the IP address of a registered PCC-AF server on a PCC-AF service instance. pcc_af_ip_address is an IP address expressed in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

call-id call_id
Filters the display of full or summarized session statistics for IP-CAN session(s) based on the registered call ID on a PCC-AF service instance for the IP-CAN session subscriber in 8-digit hexadecimal format.
**pcc-af-service pcc_af_svc_name**
Filters the display of session statistics for a registered IP-CAN session(s) based on an existing PCC-AF service name specified as an alphanumeric string of 1 through 63 characters.

**sipuri sip_uri**
Displays summarized or full information for IP-CAN session(s) based on the SIP-URI on a PCC-AF service instance.

sip_uri is the Session Initiation Protocol (SIP) addressing schema to call another person. It resembles an e-mail address and is written in the SIP URI format as sip:x@y:Port format, where x = username and y = host (domain or IP)

| { grep grep_options | more }

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of the `grep` and `more` commands, refer to the Regulating a Command’s Output section in the Command Line Interface Overview chapter.

**Usage**

Use this command to view the session statistics of all or specific registered IP-CAN session(s) or in selected part of user session for PCC-AF services configured and running on this system.

**Example**

The following command displays the summarized session statistics for all registered IP-CAN sessions on the PCC-AF service named pccAF1:

```
show pcc-af sessions summary all service pccAF1
```

**Important:** Output descriptions for commands are available in the Statistics and Counters Reference.
show pcc-policy service

Displays the statistical and configuration information of configured PCC-Policy services configured in a context.

Product
IPCF

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show pcc-policy service [ statistics] { all | name pcc_ply_svc_name | summary } [ | { grep grep_options | more } ]

- **all**
  all: displays information for all configured PCC-Policy services.

- **name pcc_ply_svc_name**
  Displays information for an existing PCC-Policy service specified as an alphanumeric string of 1 through 79 characters.

- **statistics**
  Displays statistical information for a specific or all PCC-Policy services configured in a context.

- **summary**
  Displays summarized output for this command.

  | { grep grep_options | more } |
  Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
  For details on the usage of the **grep** and **more** commands, refer to the **Regulating a Command’s Output** section in the **Command Line Interface Overview** chapter.

Usage
Use this command to display the statistical and configuration information of configured PCC-Policy services configured in a context.
Display can further be filtered for specific PCC-Policy service name or summarized output of the command.

Example

The following command displays the information for the PCC-Policy service named **pcc_policy1** in summarized output:
show pcc-policy service

```
show pcc-policy service name pcc_policy1 summary
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference.*
show pcc-policy session

Displays active/dormant session information about PCC-Policy service instances configured and running on this system based on different filter criteria.

Product
IPCF

Privilege
Inspector

Mode
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax
show pcc-policy sessions [ full | summary ] [ all ] [ apn | call-id call_id | imsi imsi_id | ip-address pcc_pcef_ip_address | service pcc_plcy_svc_name ] [ | { grep grep_options | more } ]

full
Displays full information for a specific registered IP Connectivity Access Network (IP-CAN) session(s) on a PCC-Policy service instance running on system. Display can be filtered based on given filtering criteria.

summary
Displays summarized information for a specific registered IP-CAN session(s) on a PCC-Policy service instance running on system. Display can be filtered based on given filtering criteria.

all
Displays summarized or full information for all registered IP-CAN session(s) on a PCC-Policy service instance running on system. Display can be filtered based on given filtering criteria.

apn apn_name
Displays information for PCC-Policy service sessions connected via an existing APN on the PCEF.

imsi imsi_id
Displays summarized or full information for IP-CAN session(s) based on the International Mobile Subscriber Identity (IMSI) of a subscriber in a PCC-Policy service instance.

imsi_id is the IMSI and must be a 15-character field which identifies the subscriber’s home country and carrier.

ip-address pcc_pcef_ip_address
Filters the display of full or summarized session statistics for IP-CAN session(s) based on the IP address of the registered PCEF node specified in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.
**call-id call_id**

Filters the display of full or summarized session statistics display for an IP-CAN session(s) based on the registered call ID in a PCC-Policy service instance.

*call_id* must be an existing call identifier in the IP-CAN session subscriber expressed in 8-digit hexadecimal format.

**pcc-policy-service pcc_plcy_svc_name**

Filters the display of session statistics for registered IP-CAN session(s) based on an existing PCC-Policy service name specified as an alphanumeric string of 1 through 63 characters.

```
| grep grep_options | more |
```

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the `grep` and `more` commands, refer to the *Regulating a Command’s Output* section in the *Command Line Interface Overview* chapter.

**Usage**

Use this command to view the session statistics for all or a specific registered IP-CAN session(s) for PCC-Policy services configured and running on this system.

**Example**

The following command displays summarized session statistics for all registered IP-CAN sessions on the PCC-Policy service named `pccPolicy1`:

```
show pcc-policy sessions summary all service pccPolicy1
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*. 
**show pcc-service**

Displays the configuration information for Policy and Charging Control (PCC) services configured in a context.

**Product**
IPCF

**Privilege**
Security Administrator, Operator, Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
show pcc-service { summary | all | service-name pcc_svc_name } [ | { grep grep_options | more } ]
```

- **all**
  - all: displays information for all configured PCC services.

- **service-name pcc_svc_name**
  - Displays information for an existing PCC service specified as an alphanumeric string of 1 through 79 characters.

- **summary**
  - Displays the summarized output of this command.

- **| { grep grep_options | more }**
  - Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
  - For details on the usage of the `grep` and `more` commands, refer to the Regulating a Command’s Output section in the Command Line Interface Overview chapter.

**Usage**

Use this command to display statistical and configuration information for configured PCC services in a context.

Display can further be filtered for a specific PCC service name.

**Example**

The following command displays the information for the PCC service named `pcc_svc1`:

```
show pcc-service service-name pcc_svc1 summary
```

**Important:** Output descriptions for commands are available in the Statistics and Counters Reference.
show pcc-service session

Displays active/dormant session information about Policy and Charging Control (PCC) service instances configured and running on this system based on different filter criteria.

Product
IPCF

Privilege
Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show pcc-service sessions [ full | summary ] [ all emergency-only ] [ call-id call_id | instance instance_id | service-name pcc_svc_name ] [ | { grep grep_options | more } ]

---

**full**
Displays full information for a specific registered IP Connectivity Access Network (IP-CAN) session(s) in a PCC service instance running on system. Display can be filtered based on given filtering criteria.

**summary**
Displays summarized information for a specific registered IP-CAN session(s) in a PCC service instance running on system. Display can be filtered based on given filtering criteria.

**all**
Displays summarized or full information for all registered IP-CAN sessions on a PCC service instance running on system. Display can be filtered based on given filtering criteria.

**emergency-only**
Displays summarized or full information for all IP-CAN sessions on a PCC service instance running on system which are using emergency APN for emergency services. Display can be filtered based on given filtering criteria.

**instance instance_id**
Displays summarized or full information for an IP-CAN session(s) based on the PCC service instance identifier on an IPCF/PCRF node specified as an integer from 1 through 512.

**service-name pcc_svc_name**
Filters the display of session statistics display of registered IP-CAN session(s) based on an existing PCC service name specified as an alphanumeric string of 1 through 63 characters.
show pcc-service session

| { grep grep_options | more }

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the `grep` and `more` commands, refer to the Regulating a Command’s Output section in the Command Line Interface Overview chapter.

Usage

Use this command to view session statistics for all or a specific registered IP-CAN session(s) in PCC services configured and running on this system.

Example

The following command displays summarized session statistics for all registered IP-CAN sessions in the PCC service named `pccsvc1`:

```
show pcc-service sessions summary service-name pccsvc1
```
show pcc-service statistics

Displays the statistical information for Policy and Charging Control (PCC) services configured in a context.

Product
IPCF

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show pcc-service statistics { all | service-name pcc_svc_name [ profile-name pcc_profile_name ] } [ | { grep grep_options | more } ]

all
Displays statistical information for all configured PCC services on a system.

service-name pcc_svc_name
Displays information for an existing PCC service specified as an alphanumeric string of 1 to 79 characters. It can be further filtered by the PCC profile name used in an IP-CAN session.

profile-name pcc_profile_name
Displays information for an existing PCC profile in an IP-CAN session.

| { grep grep_options | more }

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the grep and more commands, refer to the Regulating a Command’s Output section in the Command Line Interface Overview chapter.

Usage
Use this command to display the statistical information for PCC services configured in a context. Display can further be filtered for a specific Profile name used in a session.

Example
The following command displays the information for the PCC service named pcc_svc1 using PCC profile named pcc_profile_default:

```plaintext
show pcc-service statistics service-name pcc_svc1 profile-name pcc_profile_default
```

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show pcc-sp-endpoint

Displays statistical and configuration information for a configured PCC Sp-Endpoint instance in a context.

Product

IPCF

Privilege

Security Administrator, Administrator, Operator, Inspector

Mode

Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show pcc-sp-endpoint [statistics] [all | name sp_endpt_name] [ | [grep grep_options | more]] [connection [all | name sp_endpt_name]]

- **all**
  Displays statistical information for all configured PCC Sp-Endpoint instances on a system.

- **name sp_endpt_name**
  Displays information for an existing PCC Sp-Endpoint instance specified as an alphanumeric string of 1 through 79 characters.

- **| {grep grep_options | more}**
  Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
  For details on the usage of `grep` and `more` commands, refer to the Regulating a Command’s Output section in the Command Line Interface Overview chapter.

- **connection**
  Displays statistics for the configured connection values along with peer selection success and failures.

Usage

Use this command to display statistical information and peer name for a configured PCC Sp-Endpoint instance in a context.

**Important:** If the secondary peer is not configured, then N/A is printed in the output.

Example

Display can further be filtered for a specific PCC Sp-Endpoint instance used in a session.

The following command displays statistical information for the PCC Sp-Endpoint instance named `Sp_Intf1`:

```
show pcc-sp-endpoint statistics name Sp_Intf1
```
**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference.*
show pcc-sp-endpoint connection

Displays statistical and configuration information for an Sp interface connection in a PCC Sp-Endpoint instance.

Product
IPCF

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show pcc-sp-endpoint connection [ all | name sp_endpt_name [ peer sp_peer_name ] ] [ | { grep grep_options | more } ]

- **all**
  Displays statistical information for all configured PCC Sp-Endpoint instances on a system.

- **name sp_endpt_name**
  Displays information for an existing PCC Sp-Endpoint instance specified as an alphanumeric string of 1 through 79 characters. It can further be filtered with an Sp Endpoint peer (SSC/SPR) name used for the IP Connectivity Access Network (IP-CAN) session.

- **peer ssc_name**
  Displays information only for the PCC Sp-Endpoint instance within an existing Subscriber Service Controller/Subscriber Profile Repository (SSC/SPR) as a peer for an IP-CAN session.

  *ssc_name* is the name of the SSC/SPR node used by the Sp Endpoint interface.

- | { grep grep_options | more }
  Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

  For details on the usage of the **grep** and **more** commands, refer to the Regulating a Command’s Output section in the Command Line Interface Overview chapter.

Usage

Use this command to display statistical information for Sp interface connections in PCC Sp-Endpoint instances.

Display can further be filtered for a specific peer name (SSC/SPR).

Example

The following command displays the Sp interface connection related statistical information for the PCC Sp-Endpoint instance named *Sp_Intf1* using peer name *SSC1*:

```
show pcc-endpoint connection name Sp_Intf1 peer SSC1
```
show pcc-sp-endpoint connection

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference.*
### show pdg-service

Displays configuration information about PDG services configured on the system.

**Product**  
PDG/TTG

**Privilege**  
Security Administrator, Administrator, Operator, Inspector

**Mode**  
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
show pdg-service { all | name service_name } | { grep grep_options | more }
```

- **all**  
  Displays information for all configured Packet Data Gateway/Tunnel Termination Gateway (PDG/TTG) services.

- **name service_name**  
  Displays information only for an existing PDG service specified as an alphanumeric string of 1 through 63 characters.

- **| { grep grep_options | more }**  
  Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

  For details on the usage of `grep` and `more`, refer to the *Regulating a Command’s Output* section in the *Command Line Interface Overview* chapter.

**Usage**

Use this command to display information for PDG services.

**Example**

The following command displays available information for all active PDG services:

```
show pdg-service all
```
show pdg-service statistics

Displays statistics for the Packet Data Gateway/Tunnel Termination Gateway (PDG/TTG) since the last restart or clear command. The output includes the number of each type of Extensible Authentication Protocol (EAP) messages.

Product
PDG/TTG

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show pdg-service statistics [ name service_name | peer-address ipv4_address ]

name service_name
Displays statistics for an existing PDG service specified an alphanumeric string of 1 through 63 characters.

peer-address ipv4_address
Displays statistics for a specific subscriber with the WLAN IP address specified in IPv4 dotted-decimal notation.

| { grep grep_options | more }
Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of grep and more, refer to the Regulating a Command’s Output section in the Command Line Interface Overview chapter.

Usage
Use this command to display PDG service statistics.

Example
The following command displays statistics for all active PDG services:

show pdg-service statistics
show pdif-service

Displays configuration information about Packet Data Interworking Function (PDIF) services configured on the system.

**Product**

PDIF

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Mode**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
show pdif service { all [ counters ] | name name [ counters ] | statistics [ name name | peer-address address ] } [ | { grep grep_options | more } ]
```

- **all [ counters ]**
  Displays configuration information and statistical counters for all PDIF services in the system.

- **name name [ counters ]**
  Displays configuration information and statistical counters for an existing PDIF service specified as an alphanumeric string of 1 through 63 characters.

- **statistics [ name name | peer-address address ]**
  - **name name**: Displays service statistics for a an existing PDIF service specified as an alphanumeric string of 1 through 63 characters.
  - **peer-address address**: Displays service statistics for a peer server IP address specified in IPv4 dotted-decimal notation.

| { grep grep_options | more } |

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of `grep` and `more`, refer to the *Regulating a Command’s Output* section in the Command Line Interface Overview chapter.

**Usage**

Use this command to display configuration information and statistics about PDIF services on the system.

**Example**

The following example displays configuration information about a PDIF service named `pdif23`:

```
show pdif service name pdif23
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference.*
show pdsn-service

Displays information for configured packet data services in the current context.

Product
PDSN

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show pdsn-service { all | name pdsn_name } [ pcf-status [ address ip_address | filter { all | icmp-monitored | no-calls | summary | up } ] ] [ | { grep grep_options | more } ]

- **all**: Displays information for all configured packet data services.
- **name pdsn_name**: Displays information only for an existing PDSN service specified as an alphanumeric string of 1 through 79 characters.

pcf-status [ address ip_address | filter { all | icmp-monitored | no-calls | summary | up } ]

- **pcf-status**: Displays summary information for all Packet Control Functions (PCFs).
- **address ip_address**: Only lists information for the PCF with the IP address specified in IPv4 dotted-decimal notation.
- **filter**: Filters the output so only the specified information is displayed. If a filter is specified with no keywords, summary information for all PCFs is displayed.
  - **all**: Displays information for all the PCFs
  - **icmp-monitored**: Displays information only for PCFs which are ICMP monitored
  - **no-calls**: Displays information only for PCFs which have no active sessions
  - **summary**: Displays only a summary of the status of the PCFs
  - **up**: Displays information only for PCFs which are alive

| { grep grep_options | more }

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of **grep** and **more**, refer to the *Regulating a Command’s Output* section in the *Command Line Interface Overview* chapter.

Usage
Show the PDSN service information for standard system monitoring or troubleshooting.

Example
The following will display the information for all configured services and `sampleService`, respectively:

```plaintext
show pdsn-service all
show pdsn-service name sampleService
```
show peer-profile

Displays configuration of the specified peer profile.

Product

GGSN
P-GW
SAEGW
S-GW

Privilege

Security Administrator, Administrator, Operator, Inspector

Mode

Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show peer-profile { all | full { all | name profile_name } | name profile_name } [ | { grep grep_options | more } ]

all
Displays a list of all peer profiles configured on the system, arranged by service type.

full { all | name profile_name }
Displays detailed peer profile configuration information.
all: Displays detailed configuration information for all peer profiles configured on the system.
name profile_name: Displays detailed configuration information for the specified peer profile.
profile_name is an alphanumeric string of 1 through 64 characters.

name profile_name
Lists the specified peer profile, and the service type to which it belongs.
profile_name is an alphanumeric string of 1 through 64 characters.

| { grep grep_options | more }
Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of grep and more, refer to the Regulating a Command’s Output section in the Command Line Interface Overview chapter.

Usage

Use this command to display configuration information for the peer profiles created on the system.
Refer to the peer-profile command in the Global Configuration Mode Commands chapter and the Peer Profile Configuration Mode Commands chapter for more information.

Example
The following command displays detailed configuration information for the `pp2` peer profile.

```
show peer-profile full name pp2
```
show pgw-service

Displays configuration information for PDN Gateway (P-GW) services on this system.

Product
P-GW
SAEGW

Privilege
Inspector

Mode
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show pgw-service { all | name service_name | statistics { all | name service_name } [ verbose ] } [ | { grep grep_options | more } ]

- **all**
  Displays configuration information for all P-GW services configured on this system.

- **name service_name**
  Displays configuration information for an existing P-GW service specified as an alphanumeric string of 1 through 63 characters.

- **statistics { all | name service_name } [ verbose ]**
  Displays P-GW service statistics.
  - **all**: Displays statistics for all P-GW services on the system.
  - **name service_name**: Displays statistics for an existing P-GW service specified as an alphanumeric string of 1 through 63 characters.
  If **verbose** is also specified, the information is displayed in more detail.

- **| { grep grep_options | more }**
  Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
  For details on the usage of **grep** and **more**, refer to the Regulating a Command’s Output section in the Command Line Interface Overview chapter.

Usage
Use this command to view configuration information for P-GW services on this system.

Example
The following command displays service statistics for the P-GW service named **pgw1**:

```
show pgw-service name pgw1
```
show plugin

Displays the current configuration of one or all plugin modules installed on the system. This command is associated with the dynamic software upgrade process.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

**Syntax**

`show plugin [ plugin_name ]`

*plugin_name*
Filters the output by an existing plugin name expressed as an alphanumeric string of 1 through 16 characters.

**Usage**
Displays the attribute settings, priority and version for one or all plugin modules. A plugin module is a shared object library that can be dynamically updated or rolled back. Refer to the *System Administration Guide* for additional information on dynamic software updates.

**Example**
The following command displays the configuration status of all plugin modules currently installed on the system:

`show plugin`
show port

Displays information on configured parameters and operational statistics for physical and logical ports in the system.

Product

All

Privilege

Security Administrator, Administrator, Operator, Inspector

Mode

Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show port { datalink counters [ slot/port ] | info [ slot/port ] [ vlan vlan_id ] | npu counters [ slot/port [ tagged | untagged | vlan tag_id ] ] | table | transceiver

show port info { slot/port } [ vlan vlan_id ] [ | { grep grep_options | more } ]

datalink counters slot/port

Displays the physical layer information for all data links or only the one specified by the slot/port location of a previously configured port.

info [ slot/port ] [ vlan vlan_id ]

Displays detailed information for all ports within the chassis or only the one specified by slot/port location of a previously configured port.

vlan vlan_id: Displays detailed information about all Virtual Local Area Networks (VLANs) in the port/slot. If the optional vlan_id is not specified, this keyword displays port information for all VLANs in the slot/port location.

npu counters [ slot/port [ tagged | untagged | vlan tag_id ] ] | bound | unbound

Displays the information for Network Processing Unit (NPU) ports. The information for all ports is output or only the one specified by the slot/port location of a previously configured port. For ASR 5500 MIO ports, this command displays the combined statistics for the specified port and its paired port (virtual pair).

tagged: Display statistics for all tagged packets.
untagged: Display statistics for all untagged packets.

vlan tag_id: Display NPU counters for a previously configured VLAN ID.

bound: Displays individual and cumulative NPU port counters for the bound ports within the current context. If the command is invoked in the local context, all of the bound ports for all contexts and cumulative counter values for all contexts are displayed.

unbound: Displays individual and cumulative NPU port counters for all unbound ports within system.
Exec Mode show Commands (M-P)

show port

Displays information for all physical ports on rear-installed cards with physical interfaces.

transceiver slot/port

Displays diagnostic information for all SFP+ transceivers connected to a specified subscriber traffic port on the MIO card.

utilization table [ verbose ]

Shows average port utilization in Mbps. The output is a table that lists the current utilization average, a 5-minute average, and a 15-minute average, for all enabled ports. The verbose option displays port utilization with kilobyte accuracy using decimal points.

| { grep grep_options | more } |

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of grep and more, refer to the Regulating a Command’s Output section in the Command Line Interface Overview chapter.

Usage

Display port information for troubleshooting of network communications by viewing statistics and configuration information for physical ports.

Example

The following displays detailed information for port 1 in slot 17:

```
show port info 17/1
```

The following displays information for the data link port 33/1:

```
show port datalink counters 33/1
show port npu counters 33/1
```

The following displays detailed information for port 11 in slot 5:

```
show port info 5/11
show port table
```

**Important:** Output descriptions for commands are available in the Statistics and Counters Reference.
show power

Displays information about the power on/off status of individual cards and the operating status of installed power filter units.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

```
show power [ all | chassis | card_num ] [ | { grep grep_options | more } ]
```

- **all | chassis | card_num**
  - all: Displays power on/off state for all cards in the chassis.
  - chassis: Displays the operating status of installed power filter units. This is the default setting.
  - card_num: Displays the power on/off state for a single card specified an integer from 1 through 48 for the ASR 5000 or 1 through 20 for the ASR 5500.

- **| { grep grep_options | more }**
  - Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
  - For details on the usage of **grep** and **more**, refer to the Regulating a Command’s Output section in the Command Line Interface Overview chapter.

Usage

View power source information to quickly check the power for all cards within a chassis.

**Important:** On some platforms, only show power is supported with no other keywords or variables.

Example

The following displays power supply status for the chassis:

```
show power
```

The following command displays the power status for all slots:

```
show power all
```
**show ppp**

Displays the point-to-point protocol (PPP) information, detailed or summarized, for one or all connections by the use of filtering options.

**Product**
- PDSN
- GGSN

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Mode**
- Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
show ppp { [ counters | full | summary ] { all | callid call_id | imsi id | msid ms_id | username user_name } | statistics [ pcf-address [ pcf_ip_addr | all ] | pdsn-service pdsn_name ] } [ | { grep grep_options | more } ]
```

- **counters | full | summary**
  - Filters the output for the level and type of information with the options described below.
  - **counters**: Displays PPP statistics.
  - **full**: Displays all available information.
  - **summary**: Displays only a summary of available information.

- **all | callid call_id | imsi imsi_id | msid ms_id | username user_name**
  - **all**: Displays all available information.
  - **callid call_id**: Displays PPP information only for the call ID specified as a 4-digit hexadecimal number.
  - **imsi id**: Displays PPP information only for the subscriber with the specified IMSI (International Mobile Subscriber Identity). *id* is a 15-digit field which identifies the subscriber’s home country and carrier.
  - **msid ms_id**: Displays information for a mobile subscriber ID specified as 7 to 16 digits for an IMSI, MIN, or RMI.
  - **username user_name**: Displays user PPP information for the specified username.

- **statistics [ pcf-address [ pcf_ip_addr | all ] | pdsn-service pdsn_name ]**
  - Displays statistics for all packet data services.
  - **pcf-address [ pcf_ip_addr | all ]**: Displays statistics only for the time the session is connected to the specified PCF (Packet Control Function) or for all PCFs. *pcf_ip_addr* must be specified using IPv4 dotted-decimal notation.
  - **pdsn-service pdsn_name**: Displays statistics only for an existing PDSN service specified as an alphanumeric string of 1 through 63 characters.

  | { grep grep_options | more } |

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter in the Command Line Interface Reference.

**Usage**

View Point-to-Point Protocol information to support troubleshooting subscriber connections by viewing information on PPP connections for a specific subscriber.

**Example**

The following displays the PPP summary for all connections.

```
show ppp summary all
```

The following outputs the point-to-point detailed information for the user `user1`.

```
show ppp full username user1
```

The following command displays the standard information for the call with ID `FF0E11CD`.

```
show ppp callid ff0e11cd
```

The following command displays the PPP statistics for `pdsn1`.

```
show ppp statistics pdsn-service pdsn1
```

The following command provides summarized information for the PPP statistics.

```
show ppp
```

---

**Important:** Output descriptions for commands are available in the Statistics and Counters Reference.
**show prepaid 3gpp2**

Displays prepaid accounting information for all services or only the service specified.

**Product**
- PDSN
- GGSN

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
show prepaid 3gpp2 statistics all [ | { grep grep_options | more } ]
show prepaid 3gpp2 statistics { ggsn-service | ha-service | lns-service | pdsn-service { all | name service_name } [ | { grep grep_options | more } ]
show prepaid 3gpp2 statistics per-service-summary } [ | { grep grep_options | more } ]
```

- **all**
  Displays prepaid statistics for all services.

- **ggsn-service**
  Displays statistics for GGSN service(s).

- **ha-service**
  Displays statistics for HA service(s).

- **lns-service**
  Displays statistics for LNS service(s).

- **pdns-service**
  Displays statistics for PDSN service(s).

- `{ all | name service_name }`

  **all**: Displays statistics for all services of the specified type.
  **name service_name**: Displays statistics for an existing service specified an alphanumeric string of 1 through 63 characters.

- **per-service-summary**
  Displays prepaid statistics per service summary for all services.
show prepaid 3gpp2

\[ \{ \texttt{grep} \ \texttt{grep\_options} \ | \ \texttt{more} \} \]

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of \texttt{grep} and \texttt{more}, refer to the \textit{Regulating a Command’s Output} section of the \textit{Command Line Interface Overview} chapter in the \textit{Command Line Interface Reference}.

**Usage**

Displays Pre-paid statistics for a particular named service or for all services.

**Example**

To display statistics for a PDSN service named \texttt{PDSN1}, enter the following command:

\[ \texttt{show prepaid 3gpp2 statistics pdsn-service name PDSN1} \]

\[ \text{ Important: Output descriptions for commands are available in the Statistics and Counters Reference.} \]
show prepaid wimax

This command displays prepaid WiMAX accounting information for all services or only the service specified.

Syntax

```
show prepaid wimax statistics { all | asngw-service { all | name service_name } | ha-service { all | name service_name } | per-service-summary } [ | { s grep_options | more } ]
```

<table>
<thead>
<tr>
<th>all</th>
</tr>
</thead>
<tbody>
<tr>
<td>This keyword displays prepaid statistics for all services.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>asngw-service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Displays prepaid statistics for Access Service Network-Gateway (ASN-GW) service(s).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ha-service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Displays prepaid accounting statistics for Home Agent (HA) service(s).</td>
</tr>
</tbody>
</table>

| { all | name service_name } |
|---------------------------|
| **all**: Displays statistics for all services of the specified type. |
| **name service_name**: Displays statistics for an existing service specified as an alphanumeric string of 1 through 3 characters. |

<table>
<thead>
<tr>
<th>per-service-summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Displays prepaid statistics per service summary for all services.</td>
</tr>
</tbody>
</table>

| | { grep grep_options | more } |
|-----------------------------|
| Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent. |
| For details on the usage of `grep` and `more`, refer to the `Regulating a Command’s Output` section in the `Command Line Interface Overview` chapter. |

Usage

Use this command to display prepaid WiMAX accounting statistics for named service or for all services.

Example

Use this command to display prepaid WiMAX accounting statistics for named service or for all services.
The following command displays prepaid WiMAX accounting statistics for an ASN-GW service named asnl:

```
show prepaid wimax statistics asngw-service name asnl
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference.*
show profile-id-qci-mapping

Displays QoS Class Identifier-Radio Access Network (QCI-RAN) mapping tables configured on this system.

Product
HSGW

Privilege
Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show profile-id-qci-mapping table { all | name table_name } [ | { grep grep_options | more } ]

| all
| Displays information for all QCI-RAN mapping tables configured on this system.

| name table_name
| Displays information for an existing QCI-RAN table specified as an alphanumeric string of 1 through 63 characters.

| | { grep grep_options | more } |
| Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
| For details on the usage of grep and more, refer to the Regulating a Command’s Output section in the Command Line Interface Overview chapter.

Usage

Use this command to display the contents of a specific QCI-RAN mapping table or all mapping tables configured on this system.

Example

The following command displays the contents of a QCI-RAN mapping table named table1:

show profile-id-qci-mapping table name table1
show ps-network

Displays statistics for the Packet Switched (PS)-network(s) instance configured on a chassis for HNB-GW service sessions.

**Product**
HNB-GW

**Privilege**
Security Administrator, Administrator, Operator

**Mode**
Exec
The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
show ps-network { all | name ps_name } [ status ] [ | { grep grep_options | more }]
```

- **all**
  Displays status counters for all PS (packet switched) networks configured for HNB-GW service sessions on a chassis.

- **name ps_name**
  Displays status counters for a PS network configured for HNB-GW service specified as an alphanumeric string of 1 through 127 characters that is case sensitive

  | { grep grep_options | more }

  Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent. Refer to *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter for details on the usage of *grep* and *more*.

**Usage**
Use this command to display the status of any or all PS-network(s) instance configured on a chassis for HNB-GW service sessions.

**Example**
The following command displays the output for PS network instance status named *ps_1_hnb*:

```
show ps-network name ps_1_hnb status
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show ps-network counters

Displays the session counter information for a PS Network associated with Home-NodeB Gateway (HNB-GW) services configured and running on a system.

Product
HNB-GW

Privilege
Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show ps-network counters [ name ps_svc_name [ sgsn sgsn_point_code ] ] [ | { grep grep_options | more } ]

name ps_svc_name
Filters the counter display based on an existing HNB-PS Network service name associated with an HNB-GW service running on system. ps_svc_name is an alphanumeric string of 1 through 63 characters.

sgsn sgsn_point_code
Filters the counter display filtered on the basis of SGSN address provided in the SS7 point code that is connected to a particular HNB-PS Network service. sgsn_point_code must be the address of an SGSN in SS7 point code notation.

| { grep grep_options | more }

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of the grep and more commands, refer to the Regulating a Command’s Output section in Command Line Interface Overview chapter.

Usage

Use this command to view the session counter information for HNB-PS Network services configured and SGSNs connected on a system.

Example

The following command displays the counters for the HNB-PS Network service named hnb_ps_svc1:

    show ps-network counters name hnb_ps_svc1

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show ps-network statistics

Displays the Packet Switched session statistics for Home-NodeB Gateway (HNB-GW) services configured and running on this system.

Product
HNB-GW

Privilege
Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local] host_name#

Syntax

show ps-network statistics [ name ps_svc_name [ sgsn sgsn_point_code]] [ gtpu-only | ranap-only | sccp-only ] [ | { grep grep_options | more } ]

name ps_svc_name
Filters the session statistics display based on an existing HNB-PS Network service name that is associated with an HNB-GW service running on this system. ps_svc_name is an alphanumeric string of 1 through 63 characters.

sgsn sgsn_point_code
Filters the counter display filtered on the basis of SGSN address provided in the SS7 point code that is connected to a particular HNB-PS Network service. sgsn_point_code must be the address of an SGSN in SS7 point code notation.

gtpu-only
Filters the session statistics to display only GTP-U traffic for the specified HNB-PS Network service which is configured and associated with an HNB-GW service running on this system.

ranap-only
Filters the session statistics to display only Radio Access Network Application Protocol (RANAP) traffic for an HNB-PS Network service which is configured and associated with an HNB-GW service running on this system.

sccp-only
Filters the session statistics to display only Signaling Connection Control Part (SCCP) traffic for the specified HNB-PS Network service which is configured and associated with an HNB-GW service running on this system.
show ps-network statistics

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
For details on the usage of the `grep` and `more` commands, refer to the Regulating a Command’s Output section in Command Line Interface Overview chapter of the Command Line Interface Reference.

**Usage**

Use this command to view the session statistics for overall session or in selected part of user session for HNB-GW services configured and running on this system.

**Example**

The following command displays the session statistics for the HNB-PS Network service named `hnb_psl`:

```
show ps-network statistics name hnb_psl
```

**Important:** Output descriptions for commands are available in the Statistics and Counters Reference.
Chapter 131
Exec Mode show Commands (Q-S)

This chapter includes the commands qci-qos-mapping through show system uptime.
The Exec Mode is the initial entry point into the command line interface system. Exec mode show commands are useful in troubleshooting and basic system monitoring.

Mode
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

⚠ Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
show qos npu inter-subscriber traffic

This command is only supported on PACs running on ST16 platforms. It has been deprecated for use on ASR 5x00 platforms.
**show radius**

Displays and statistic information for RADIUS accounting and/or authentication.

**Product**

- PDSN
- HA
- GGSN
- ASN-GW

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Mode**

Exec

The following prompt is displayed in the Exec mode:

```
[local] host_name#
```

**Syntax**

```
show radius { accounting servers | authentication servers } [ detail ] [ admin-status { enabled | disabled } ] [ | { grep grep_options | more } ] [ radius group group_name [ detail ] [ | { grep grep_options | more } ] ]
```

---

**accounting servers**

Lists information for configured accounting servers and their current state.

---

**authentication servers**

Lists information for configured authentication servers and their current state.

---

[ detail ]

Displays historical state information for configured servers of the specified type.

---

**admin-status { enabled | disabled }**

Displays information for accounting and/or authentication servers with an administrative status of “enabled” or “disabled”.

---

**radius group group_name**

Displays the authentication/authorization RADIUS server group information for an existing server group specified as an alphanumeric string of 1 through 63 characters.

---

| { grep grep_options | more } |

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter.
**Usage**

Display the RADIUS server information as part of periodic monitoring of the health of the system.

**Example**

The following displays the information on configured accounting servers:

```
show radius accounting server
```

The following command displays detailed information for RADIUS accounting servers:

```
show radius accounting servers detail
```

The following command displays detailed information for RADIUS server group `star1` used for authentication:

```
show radius authentication servers radius group star1 detail
```

The following command displays detailed information for RADIUS server group `star1` used for accounting:

```
show radius accounting servers radius group star1 detail
```

**Important:** Output descriptions for commands are available in the Statistics and Counters Reference.
show radius charging servers

This command displays the RADIUS authentication and accounting servers or server group that are configured for use by charging services.

Product
- PDSN
- HA
- GGSN
- ASN-GW

Privilege
- Security Administrator, Administrator, Operator, Inspector

Mode
- Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

```
show radius charging servers [ radius group group_name ] [ | { grep grep_options | more } ]
```

- **radius group group_name all**
  - Displays all RADIUS counter information for an existing server group configured for use by charging services. `group_name` is specified as an alphanumeric string of 1 through 63 characters.

  ```
  | { grep grep_options | more }
  ```

  Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

  For details on the usage of the `grep` and `more` commands, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage

Use this command to display information about RADIUS servers or server group configured for use by Charging Services.

Example

The following command displays RADIUS servers configured for Charging Services:

```
show radius charging servers
```

**Important**: Output descriptions for commands are available in the Statistics and Counters Reference.
show radius client

Displays information about the RADIUS client configured on the system.

**Product**
- PDSN
- HA
- GGSN
- ASN-GW

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
show radius client status [ | { grep grep_options | more } ]
```

**status**
Displays a status summary for the RADIUS client.

```
| { grep grep_options | more }
```

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the `grep` and `more` commands, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter.

**Usage**

Configuring the RADIUS protocol on the system enables RADIUS client functionality. This command displays information pertaining to the status of the client.

**Example**

The following command displays detailed information pertaining to the system’s RADIUS client:

```
show radius client status
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show radius counters

Displays RADIUS server and statistic information for accounting and/or authentication.

Product
PDSN
HA
GGSN
ASN-GW

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

```
show radius counters { all | dynamic-auth | radius group group_name [ all | server ip_address [ port number ] | summary [ all-contexts [ verbose ] ] ] } [ | { grep grep_options | more } ]
```

counters { all | server ip_address [ port number ] }

all: Displays statistics for all servers.
server ip_address: Displays statistics for the server specified by its IPv4 address.
port number: Displays statistics for a port on the server specified as an integer from 0 through 65535.

radius group group_name all
Displays all RADIUS counter information for an existing server group specified as an alphanumeric string of 1 through 63 characters.
all: Displays statistics for all servers.

dynamic-auth
Displays Dynamic Authorization counters for configured RADIUS servers.

summary [ all-contexts [ verbose ] ]
Displays a summary of RADIUS statistics for all the RADIUS servers configured in a specific context.
all-contexts: Displays a summary of RADIUS statistics for all RADIUS servers configured in all context.
If verbose is also specified, the information is displayed in more detail.

| { grep grep_options | more }
Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of the grep and more commands, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.
show radius counters

Usage
Display the RADIUS server information as part of periodic monitoring of the health of the system.

Example
The following command displays detailed information pertaining to the RADIUS server group star1 with in current context:

```
show radius counters radius group star1 all
```

The following displays the statistics for the server with IP address 10.2.3.4, then just port 7777, followed by all services.

```
show radius counters server 10.2.3.4
show radius counters server 10.2.3.4 port 7777
show radius counters all
```

`Important:` Output descriptions for commands are available in the Statistics and Counters Reference.
show resources

Displays the resource information by CPU or session.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

```
show resources { cpu | npu | session } [ | { grep grep_options | more } ]
```

```
  cpu | npu | session

  cpu: Displays resource information by CPU.
  npu: Displays resource information by network processing unit (NPU).
  session: Displays resource information by session.
```

```
| { grep grep_options | more }
```

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the `grep` and `more` commands, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage

View resource utilization as part of troubleshooting systems which appear sluggish or are having excessive connection timeouts or other connection issues.

Example

The following display the resource information by CPU and session, respectively.

```
show resources cpu

show resources session
```

**Important:** Output descriptions for commands are available in the Statistics and Counters Reference.
show rlf-context-statistics

Displays the statistics for all active RLF contexts.

Product
GGSN
P-GW

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show rlf-context-statistics [ diamproxy [ facility_num | [ endpoint endpoint_name [ peer-realm realm_name [ peer-host host_name ] ] ] | summary | verbose ] [ | { grep grep_options | more } ] [ facility_num ]

facility_num
Displays the context information for the specified facility. num must be an integer from 1 through 16.

endpoint endpoint_name
Displays the context information only for the endpoint specified as a string of size ranging from 1 through 63 characters.

realm realm_name
Displays the context information only for the realm specified as a string of size ranging from 1 through 127 characters.

peer-host host_name
Displays the context information only for the host specified as a string of size ranging from 1 through 63 characters.

instance facility_num
Displays the facility information for specific instance.

summary
Displays summary information.

verbose
Specifies to display detailed (all available) information. If not specified, concise information is displayed.
Displays the instance level stats. When multiple diamproxies are active, an RLF context's instance is created on each diamproxy or session manager for each peer.

| { grep grep_options | more }

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the `grep` and `more` commands, refer to the *Regulating a Command's Output* section of the *Command Line Interface Overview* chapter.

### Usage

Use this command to display RLF statistics for all active RLF contexts.

An RLF context is created only when –

- A peer is bound to a RLF template.
- The peer is in "OPEN" state.

Failure of any of these conditions will cause the RLF context to be deleted.

### Example

The following command displays RLF statistics for all active RLF contexts:

```bash
show rlf-context-statistics diamproxy
```
show rlf-memcache-statistics

Displays the memory used by RLF for processing the messages.

**Product**

GGSN
P-GW

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Mode**

Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

**Syntax**

```
show rlf-memcache-statistics { diamproxy facility_num [ | { grep grep_options | more } ]
```

`facility_num`
Displays the information for the specified facility. `num` must be an integer from 1 through 16.

```
| { grep grep_options | more }
```
Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of the `grep` and `more` commands, refer to the *Regulating a Command’s Output* section of the Command Line Interface Overview chapter.

**Usage**

Use this command to display the memory used by RLF for processing the messages. The output will be displayed only if the memcache is used.

**Example**

The following commands displays memory cache statistics for DIAMPROXY facility:

```
show rlf-memcache-statistics diamproxy
```
show rlf-template

Displays the statistics for all active RLF templates.

Product
GGSN
P-GW

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec
The following prompt is displayed in the Exec mode:
[local]host_name#

Syntax

show rlf-template { all | name template_name } [ | { grep grep_options | more } ]

| all
| Displays the statistics information for all the configured RLF templates.

| name template_name
| Displays the statistics information for the specified RLF template. template_name must be an integer from 1 through 127 characters.

| | { grep grep_options | more }
| Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
| For details on the usage of the grep and more commands, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage
Use this command to display statistics for all or specified RLF template(s).

Example
The following command displays statistics for all RLF templates:

    show rlf-template all
show rohc counters

Displays ROBust Header Compression (ROHC) counters for all active calls.

Product
- PDSN
- HSGW
- ASN-GW

Privilege
- Security Administrator, Administrator, Operator, Inspector

Mode
- Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

```
show rohc counters [ all | callid call_id | imsi imsi_num | ip-address ip_addr | msid msid_num | username user_name ] [ | { grep grep_options | more } ]
```

| all |
| Displays all information. |

| callid call_id |
| Displays the information only for the call ID specified as a 4-byte hexadecimal number. |

| imsi imsi_num |
| Displays information for the specified IMSI (International Mobile Subscriber Identity). The IMSI is an up to 15-digit field which identifies the subscriber’s home country and carrier: 3 digits of Mobile Country Code (MCC), 2 or 3 digits of Mobile Network Code (MNC), followed by the Mobile Subscriber Identification Number MSIN. Example: 123-45-678910234. May also be entered as 12345678910234. |

| ip-address ip_addr |
| Displays information only for the mobile subscriber IP address specified in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation. |

| msid msid_num |
| Displays information only for a mobile subscriber ID from 7 to 16 digits for an IMSI, MIN, or RMI. |

| username user_name |
| Displays radio-packet (R-P) interface information only for a specified username. |

| { grep grep_options | more } |
| Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent. |
For details on the usage of the `grep` and `more` commands, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter.

**Usage**

Use this command to display ROHC counters for all active calls.

**Example**

The following command displays ROHC counters for all active calls:

```
show rohc counters all
```
show rohc statistics

Displays statistics and counters for RObust Header Compression (ROHC) IP header compression.

**Product**
- PDSN
- HSGW
- ASN-GW

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Mode**
Exec
The following prompt is displayed in the Exec mode:

```
[local]host_name# 
```

**Syntax**

```
show rohc statistics [ pdsn-service pdsnsvc_name ] [ asngw-service asngwsvc_name ] [ hsgw-service hsgwsvc_name ] [ | { grep grep_options | more } ]
```

**Important:** Keywords available for this command are license-driven. For example, if a PDSN license is loaded, the `pdsn-service` option is visible.

- **pdsn-service pdsnsvc_name**
  Displays ROHC statistics and counters for the existing PDSN service specified as an alphanumeric string of 1 through 63 characters.

- **asngw-service asngwsvc_name**
  Displays ROHC statistics and counters for the existing ASN-GW service specified as an alphanumeric string of 1 through 63 characters.

- **hsgw-service hsgwsvc_name**
  Displays ROHC statistics and counters for the existing HSGW service specified as an alphanumeric string of 1 through 63 characters.

<table>
<thead>
<tr>
<th>grep grep_options</th>
<th>more</th>
</tr>
</thead>
</table>
| Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent. For details on the usage of the `grep` and `more` commands, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter.

**Usage**
Use this command to display ROHC statistics for all services or for a specific ASN-GW, PDSN, or HSGW.
The following command displays ROHC statistics for the PDSN service named pdsn1:

```
show rohc statistics pdsn-service pdsn1
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference.*
show route-map

Displays entries for all route maps or a specific route map.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show route-map [ name route-map name ] [ | { grep grep_options | more } ]

name route-map name
Displays information for a route-map specified as an alphanumeric string of 1 through 79 characters.

| { grep grep_options | more }
Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of the grep and more commands, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage

Use this command to see the rules configured in all route-maps for the current context.

Example

The following command displays the route-map information for prefix list Prefix100:

show route-map Prefix100

Refer to the match and set command descriptions in the Route-map Configuration Mode Commands chapter for descriptions of the various entries listed.
show rp

Displays radio-packet (R-P) interface statistics using the filtering options specified.

Product
PDSN

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show rp [ counters | full | summary ] { all | callid call_id | msid ms_id | peer-address peer_ip_address | username user_name } [ | { grep grep_options | more } ]

| counters | full | summary |
---|---|---|
| Provides an optional modifier to the output for the desired level and type of information. | | |
counters: Displays R-P protocol statistics. | full: Displays all available information. | summary: Displays only a summary of available information. |
| These options are not available in conjunction with the keywords statistics or service-option statistics. | | |

| all | callid call_id | msid ms_id | peer-address peer_ip_address | username user_name |
---|---|---|---|---|
| all: Displays all R-P information. | callid call_id: Displays only the information for the call ID specified as a 4-digit hexadecimal number. | msid ms_id: Displays information only for a mobile subscriber ID specified by 7 to 16 digits for an IMSI, MIN, or RMI. | peer-address peer_ip_address: Displays R-P information for the peer IP address of the PCF specified in IPv4 dotted-decimal notation. | username user_name: Displays R-P information for the specified username. |

| | { grep grep_options | more } |
---|---|
| Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent. | For details on the usage of the grep and more commands, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter. |

Usage

View the R-P interface statistics for the current context.

Example
The following displays the summary for all connections.

`show rp summary all`

The following outputs the R-P interface detailed information for the user `ispluser1`.

`show rp full username ispluser1`

The following command displays the standard information for the call with ID `FF0E11CD`.

`show rp callid ff0e11cd`

The following displays the statistics summary for the R-P facility.

`show rp`

---

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference.*
show rp service-option

Displays the radio-packet (R-P) service option statistics using the filtering options specified.

**Product**

PDSN

**Privilege**

Security Administrator, Administrator, Operator, Inspector

**Mode**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
show rp service-option statistics [ number svc_option_num | pdsn-service pdsn_name ] [ | { grep grep_options | more } ]
```

- `number svc_option_num | pdsn-service pdsn_name`
  - Default: display statistics for all service option numbers and associated packet data services.
  - `number svc_option_num`: Displays statistics for the specified service option number.
  - `pdsn-service pdsn_name`: Displays statistics for the specified packet data service.

- `| { grep grep_options | more }

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the `grep` and `more` commands, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter.

**Usage**

View the R-P service option statistics for the current context.

**Example**

The following displays the statistics for all service options.

```
show rp service-option statistics
```

The following displays the statistics for service option 5.

```
show rp service-option statistics number 5
```

The following command displays the statistics for all service options in collected for the packet data service `sampleService`.

```
show rp service-option statistics pdsn-service sampleService
```
show rp statistics

Displays the radio-packet (R-P) protocol statistics using the filtering options specified.

Product
PDSN

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show rp statistics [ hsgw-service hsgw-name | pcf-summary [ wfl ] | pdsn-service pdsn_name | peer-address { peer_address | all } | include-bcmcs ] [ verbose ] [ | { grep grep_options | more } ]

hsgw-service hsgw_name

Specifies an eHRPD Serving Gate Way service followed by the name of an HSGW service specified as an alphanumeric string of 1 through 63 characters.

pcf-summary [ wfl ]

Displays a session summary of Packet Control Function (PCF) statistics. The wfl option displays PCF statistics in wide-format number 1.

pdsn-service pdsn_name

Displays the statistics information for the pdsn-service specified as an alphanumeric string of 1 through 63 characters.

peer-address { peer_address | all }

- peer_address: Displays statistics only for the peer specified by its IP address in IPv4 dotted-decimal notation.
- all: Displays statistics for all peers.

verbose

Displays more detailed statistics.

| { grep grep_options | more }

 Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the grep and more commands, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.
Usage
View the R-P statistics for the current context.

Example
The following displays all collected R-P statistics.

   show rp statistics

The following displays the R-P statistics associated with the peer address 10.2.3.4.

   show rp statistics peer-address 10.2.3.4

The following command displays the R-P statistics for the packet data service PCFnet.

   show rp statistics pdsn-service PCFnet

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*.
show rsvp counters

Displays Resource Reservation Protocol (RSVP) counters using the filtering options specified.

Product
PDSN

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show rsvp counters [ all | callid call_id | msid ms_id | username user_name ]

- **all**: Displays all RSVP information.
- **callid call_id**: Displays information only for the call ID specified as a 4-digit hexadecimal number.
- **msid ms_id**: Displays information for a mobile subscriber ID specified a string of 7 to 16 digits for an IMSI, MIN, or RMI.
- **username user_name**: Displays RSVP information only for the specified username.

Usage

View the RSVP counters for the current context.

Example

The following displays all collected RSVP counters.

    show rsvp counters all
show rsvp statistics

Displays Resource Reservation Protocol (RSVP) statistics using the filtering options specified.

Product
PDSN

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

> [local]host_name#

Syntax

```
show rsvp counters [ pdsn-service service | sessmgr instance instance ]
```

- `pdsn-service service`: Displays statistics for the service specified as an alphanumeric string of 1 through 63 characters.
- `sessmgr instance instance`: Displays statistics for the specified session manager instance.

Usage
View the RSVP statistics for the current context.

Example
The following displays collected RSVP statistics for a `sampleService`.

```
show rsvp statistics pdsn-service sampleService
```
show saegw-service

Displays configuration information and node-level statistics for System Architecture Evolution Gateway (SAEGW) services on this system.

**Product**

SAEGW

**Privilege**

Inspector

**Mode**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
show saegw-service { all | name service_name | statistics { all | name service_name } [ function { pgw [ interface { GnGp | S2a | S5S8 } ] | sgw } ] [ verbose ] } [ | { grep grep_options | more } ]
```

- **all**
  Displays configuration information for all SAEGW services configured on this system.

- **name service_name**
  Displays configuration information for an existing SAEGW service specified as an alphanumeric string of 1 through 63 characters.

- **statistics { all | name service_name } [ function { pgw [ interface { GnGp | S2a | S5S8 } ] | sgw } ] [ verbose ]
  Displays node-level statistics for SAEGW.

  - **all**: Displays consolidated node-level statistics for all SAEGW services on the system.
  - **name service_name**: Displays node-level statistics for an existing SAEGW service specified as an alphanumeric string of 1 through 63 characters.

- **function**: Displays node-level statistics of one of the following functions:
  - **pgw**: Displays node-level statistics of P-GW function within SAEGW.
  - **sgw**: Displays node-level statistics of S-GW function within SAEGW.

- **interface**: Displays node-level statistics of P-GW function with respect to one of the following interfaces:
  - **GnGp**: Displays node-level statistics of P-GW function with respect to GnGp interface.
  - **S2a**: Displays node-level statistics of P-GW function with respect to S2a interface.
  - **S5S8**: Displays node-level statistics of P-GW function with respect to S5S8 interface.

If **verbose** is also specified, the information is displayed in more detail.

```
| { grep grep_options | more }
```

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of `grep` and `more`, refer to the *Regulating a Command’s Output* section in the *Command Line Interface Overview* chapter.

**Usage**

Use this command to view configuration information and node-level statistics for SAEGW services on this system.

**Example**

The following command displays configuration information for the SAEGW service named `saegw1`:

```
show saegw-service name saegw1
```
show samog-service

Displays configuration and/or statistical information for SaMOG services on this system.

**Product**
SaMOG

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Syntax**

```
show samog-service { all | name name | statistics [ name name ] } [ | { grep grep_options | more } ]
```

- **all**
  Displays all SaMOG services.

- **name name**
  Displays information for specific SaMOG service name.
  *name* is a string of size 1 to 63.

- **statistics**
  Displays Node level Statistics for SaMOG.

- **verbose**
  Specifies Detailed statistics.

  | { grep grep_options | more } |
  Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
  For details on the usage of **grep** and **more**, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter.

**Usage**

Use this command to displays configuration and/or statistical information for SaMOG services on this system.

**Example**

```
show samog-service all
```
show sccp-network

Displays SS7 Signaling Connection Control Part (SCCP) network configuration and status information.

Product
SGSN

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show sccp-network { ntwk_index | all } [ status [ all | dpc ] ]

ntwk_index
Displays configuration and status information for the SCCP network configuration with the network index specified as an integer from 1 through 12.

all
Displays all available configuration and status information for all SCCP networks.

status all
Displays all status information for specified SCCP networks.

status dpc
Displays status information for the device in the SCCP network identified by the destination point-code (DPC).

Usage
Use this command to display global SCCP statistics or to display SCCP statistics for a specified service or network.

Example
The following command displays global SCCP statistics:

    show sccp-network all

The following command displays information for an SCCP network configuration with the network index of 1:

    show sccp-network 1

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show sccp statistics

Displays SS7 Signaling Connection Control Part (SCCP) statistics for services that use the SCCP protocol.

**Product**
SGSN

**Privilege**
Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
show sccp statistics [ iups-service iups_srvc_name | map-service map_srvc_name | sccp-network ntwk_index | dpc dpc | ssn ssn | global-title-translation { address-map instance add_map_inst | association instance assoc_inst } [ sessmgr instance sessmgr_inst ] [ | { grep grep_options | more } ]
```

---

**iups-service iups_srvc_name**

Displays SCCP protocol statistics for an existing IuPS service in the current context specified as an alphanumeric string of 1 through 63 characters.

---

**map-service map_srvc_name**

Displays SCCP protocol statistics for the an existing Mobile Application Part (MAP) service in the current context specified as an alphanumeric string of 1 through 63 characters.

---

**sccp-network ntwk_index**

Displays SCCP protocol statistics for the SSCP network configuration with a network index specified as an integer from 1 through 12.

The following filters can be added to fine tune the display of SCCP network statistics:

- **dpc dpc**: Enter a standard pointcode address to limit the display of SCCP network statistics to those for the identified DPC.
- **ssn ssn**: Enter an integer from 1 to 255 to limit the display of SCCP network statistics to those for the identified subsystem number.
- **global-title-translation address-map instance add_map_inst**: Enter an integer from 1 to 4096 to limit the display of SCCP network statistics to those for the identified GTT address-map.
- **global-title-translation association instance assoc_inst**: Enter an integer from 1 to 16 to limit the display of SCCP network statistics to those for the identified GTT association.
- **sessmgr instance sessmgr_inst**: Enter an integer from 1 to 384 to limit the display of SCCP network statistics to those for the identified session manager.
**Usage**

Use this command to display global SCCP statistics or to display SCCP statistics for a specified service or SCCP network.

**Example**

The following command displays global SCCP statistics:

```plaintext
show sccp statistics
```

The following command displays SCCP statistics for the IuPS service named `iups-serv1`:

```plaintext
show sccp statistics iups-service iups-serv1
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference.*
show sctp-param-template

Displays configuration information for Stream Control Transmission Protocol (SCTP) parameter templates configured on this system.

Product
MME

Privilege
Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show sctp-param-template { all | name template_name } [ | { grep grep_options | more } ]

`all`
Displays configuration information for all SCTP parameter templates configured on this system.

`name template_name`
Displays configuration information for an existing SCTP parameter template specified as an alphanumeric string of 1 through 63 characters.

`[ | { grep grep_options | more } ]`
Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the `grep` and `more` commands, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage
Use this command to view configuration information for SCTP parameter templates on this system.

Example
The following command displays configured parameters for an SCTP parameter template named `sctp_pt3`:

```
show sctp-param-template name sctp_pt3
```
show service all

Displays configuration information for all services currently configured on this system.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show service all

Usage
Use this command to view configuration information for all services configured on this system.

Example
The following command displays information about all services configured on this system:

show service all
**show session counters historical**

Displays historical information for session-related counters based on data collected in bulk statistics.

**Product**
All

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local] host_name# 
```

**Syntax**

```
show session counters historical { all | arrived | callops | connected | disconnected | failed | handoff | rejected | renewal } [ all-intervals | recent-intervals ] [ cumulative | incremental ] [ graph | table ] [ | { grep grep_options | more } ]
```

- **all**
  Displays data for all counters either as a single, wide table or multiple graphs.

- **arrived**
  Displays only data for “total calls arrived” counters. This is based on the “sess-ttlarrived” statistic in the system schema.

- **callops**
  Displays data for all call operations. This is a calculated value based on the following formula: 
  \((\text{arrived} + \text{rejected} + \text{disconnected} + \text{failed} + \text{handoffs} + \text{renewals})\)

- **connected**
  Displays only data for “total calls connected” counters. This is based on the “sess-ttlconnected” statistic in the system schema.

- **disconnected**
  Displays only data for “total calls disconnected” counters. This is based on the “sess-ttldisconnect” statistic in the system schema.

- **failed**
  Displays only data for “total calls failed” counters. This is based on the “sess-ttlfailed” statistic in the system schema.

- **handoff**
  Displays only data for “total handoffs” counters. This is based on the “sess-ttlhandoff” statistic in the system schema.
rejected
Displays only data for “total calls rejected” counters. This is based on the “sess-ttlrejected” statistic in the system schema.

renewal
Displays only data for “total renewal” counters. This is based on the “sess-ttlrenewal” statistic in the system schema.

{ grep grep_options | more }
Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of grep and more, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Output Options
The following output options are available for this command:
- **all-intervals**: Displays all available historical information from all samples. This filter is used by default.
- **cumulative**: Displays total data for all samples up to and including the last one. In this view, values increase over time.
- **graph**: Displays data in graphical form.
- **incremental**: Displays data changes for each specific sample. The data for each sample is the amount of change since the previous sample. This filter is used by default.
- **recent-intervals**: Displays historical information for only recent samples.
- **table**: Displays data in tabular form. This is the default view.

Usage
This command provides the ability to track key session-related statistic information over time. This information can be used as part of system performance monitoring and capacity planning.

**Important**: The information provided in the output of this command requires that bulk statistics functionality be enabled on the system. Refer to the System Administration Guide for more information on configuring and enabling bulk statistics support.

The output of this command displays historical data collected at various sample intervals. The interval length is 15 minutes and is not user-configurable. Up to 192 samples (two days’ worth of data) are maintained.

**Important**: Data collection is “best-effort” over these intervals. Data is preserved on the SMC or MIO card switchovers. As with all counters, certain session failures can cause inaccuracies with counters, including counters which appear to go backwards.

Each sample is identified by a timestamp that displays the approximate time the data was gathered. The timestamp is in the format YYYY:MM:DD:hh:mm:ss.
Data acquired during the sample may be marked with an “S” appended to the end of the timestamp or to the counter value. The “S” indicates that the data is suspect (potentially bad). Occurrences of this result from events like changes to the real time clock, which can cause an interval to be an atypical length. Instances of suspect data should be rare. Additionally, there may be occasions in which a sample may be marked as “invalid”. “invalid” identifies bad data, a situation that could result when the polling has not run long enough, or because of an unexpected error retrieving data. Since baseline values must be obtained prior to collecting interval samples, the first interval of data will not be available until up to twice the interval period.

Example

The following command displays cumulative total calls arrived information for the most recent intervals and displays the output in graphical format:

```
show session counters historical arrived recent-intervals cumulative graph
```

The following command displays historical data for all counters for all intervals and displays the output in tabular format:

```
show session counters historical all
```

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show session counters pcf-summary

Displays the Packet Control Function (PCF) summary which include the number of calls, call types, and Tx/Rx packets/octets statistics.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

**Syntax**

```
show session counters pcf-summary [ call-types | data | wf1 [ pcf pcf_address | [ | { grep grep_options | more } ] ] ]
```

- **call-types**
  Displays the number of calls and the types of calls.

- **data**
  Displays the number of successful calls and Tx/Rx packets/octets statistics.

- **pcf pcf_address**
  Displays the given PCF summary for a particular address.

- **wf1**
  Displays the PCF summary in a single very wide line.

| { grep grep_options | more } |
|-----------------------------|
Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the `grep` and `more` commands, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter.

**Usage**
Use this command to display a summary of all PCFs.

**Example**

```
show session counters pcf-summary
```
**show session disconnect-reasons**

Displays a list of the reasons for call disconnects and the number of calls disconnected for each reason.

**Product**
All

**Privilege**
Security Administrator, Administrator, Inspector, Operator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local] host_name#  
```

**Syntax**

```
show session disconnect-reasons [ gprs-only | sgsn-only | mme-only | verbose ] [ | { grep grep_options | more } ] 
```

- **gprs-only**
  Only supported on the SGSN.
  This keyword limits the display to session disconnect reasons for the SGSN’s 2G MM and PDP context disconnects.

- **sgsn-only**
  Only supported on the SGSN.
  Displays session disconnect reasons for the SGSN’s 3G MM and PDP context disconnects.

- **mme-only**
  Displays session disconnect reasons for MME call disconnects.

- **verbose**
  List all disconnect reasons even if the values are zero (0).

- `| { grep grep_options | more }`
  Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

  For details on the usage of the `grep` and `more` commands, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter.

**Usage**

Use this command to display a list of the reasons why calls were disconnected.

**Example**

To view session disconnect statistics, enter the following command:

```
show session disconnect-reasons
```
To view a list of the disconnect reasons with verbose output, enter the following command:

```
show session disconnect-reasons verbose
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show session duration

Displays session duration information for the current context filtered by the options specified.

Product
All

Privilege
Security Administrator, Administrator, Inspector, Operator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local] host_name#

Syntax

```
show session duration [ session_filter ] [ | { grep grep_options | more } ]
```

`session_filter`

Specifies the name of the entity whose session duration information is to be filtered and displayed. This options are:

- `apn apn_name`: Displays session information for an existing Access Point Name (APN) specified as an alphanumeric string of 1 through 62 characters that is case sensitive.
- `asn-peer-address ip_address`: Displays session information for the ASN GW peer whose IP address is specified in IPv4 dotted-decimal notation.
- `asngw-service service_name`: Displays session information for the specified ASN-GW service.
- `asnpc-peer-address ip_address`: Displays session information for the Access Service Network Paging Controller (ASN PC) peer whose IP address is specified in IPv4 dotted-decimal notation.
- `asnpc-service service_name`: Displays session information for the specified ASN PC service.
- `cscf-service service_name`: Displays session information for an existing Call Session Control Function (CSCF) service specified as an alphanumeric string of 1 through 63 characters.

**Important:** Displays information for in-progress CSCF SIP calls only. Registrations are not considered calls.

- `dhcp-server dhcp_address`: Displays session information for the Dynamic Host Configuration Protocol (DHCP) server specified by its IP address in IPv4 dotted-decimal notation.
- `epdg-service service_name`: Displays session information for ePDG service specified as an alphanumeric string of 1 through 63 characters that is case sensitive.
- `fa fa_address`: Displays session information for the foreign agent (FA) whose IP address is specified in IPv4 dotted-decimal notation.
- `fa-service fa_name`: Displays session information for the named foreign agent service.
- `fng-service fng_name`: Displays session information for the named Femto Network Gateway service.
- `ggsn-service ggsn_name`: Displays session information for an existing GGSN service specified as an alphanumeric string of 1 through 63 characters that is case sensitive.
show session duration

- **gprs-only**: Limits the display to the session information for the SGSN’s 2G MM and PDP contexts.
- **ha ha_address**: Displays session information for the home agent specified by its IP address in IPv4 dotted-decimal notation.
- **ha-service ha_name**: Displays session information for the named home agent (HA) service.
- **hnbgw-only**: Displays session information for the HNB-GW service related sessions instances (such as HNB, IuPS, IuCS).
- **hsgw-service service_name**: Displays session information for an existing HSGW service specified as an alphanumeric string of 1 through 63 characters.
- **lma-service service_name**: Displays session information for an existing Local Mobility Anchor (LMA) service specified as an alphanumeric string of 1 through 63 characters.
- **mag-service service_name**: Displays session information for an existing Mobile Access Gateway (MAG) service specified as an alphanumeric string of 1 through 63 characters.
- **mme-service service_name**: Displays session information for an existing Mobility Management Entity (MME) service specified as an alphanumeric string of 1 through 63 characters.
- **pcc-service service_name**: Displays session information for an existing Policy and Charging Control service specified as an alphanumeric string of 1 through 63 characters.
- **pcf pcf_address**: Displays session information for the packet control function specified by its IP address in IPv4 dotted-decimal notation.
- **pdif-service service_name**: Displays session information for the named Packet Data Interworking Function service.
- **pdsn-service pdsn_name**: Displays session information for the named packet data service.

**Important**: If no PCF address or PDSN service is specified, the session information for all sessions is displayed.

- **sgsn-address sgsn-address**: Displays session information for the SGSN specified by its IP address in IPv4 dotted-decimal notation.
- **sgsn-only**: Limits the display to the session information for the SGSN’s 3G MM and PDP contexts.
- **sgw-service service_name**: Displays session information for an existing S-GW service specified as an alphanumeric string of 1 through 63 characters.

| { grep grep_options | more }

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent. For details on the usage of the *grep* and *more* commands, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter.

**Usage**

View the session information to troubleshoot subscriber problems and for general monitoring for orphaned sessions.

**Example**

The following commands display the duration for the session connected to the packet control function with address 10.2.3.4, packet data service *sampleService*, and for all sessions, respectively.

```
show session duration pcf 10.2.3.4
```
show session duration pdsn-service sampleService

show session duration
show session progress

Displays session progress information for the current context filtered by the options specified.

Product

All

Privilege

Security Administrator, Administrator, Inspector, Operator

Mode

Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show session progress [ asn-peer-address ip_address | asngw-service service_name | asnpc-service service_name | asnpc-peer-address ip_address | apn apn_name | csccf-service service_name | dhcp-server dhcp_address | epdg-service service_name | fa fa_address | fa-service fa_name | ggsn-service ggsn_name | ha ha_address | ha-service ha_name | hsgw-service service_name | lma-service service_name | mag-service service_name | mme-address | mseg-service mseg_service_name | pcf { pcf_address | all } | pdn-service pdn_name | pdsn-service pdnservice | pgw-address ip_address | samog-service service_name | sgsn-address sgsn_address | sgw-service service_name ] [ | { grep grep_options | more } ]

progress: indicates session progress information is to be displayed.
  • asn-peer-address ip_address: Displays session information for the Access Service network-Gateway (ASN-GW) peer specified by its IP address in IPv4 dotted-decimal notation.
  • asngw-service service_name: Displays session information for the named ASN-GW service.
  • asnpc-service service_name: Displays session information for the named Access Service Network Paging Controller (ASN PC) service.
  • asnpc-peer-address ip_address: Displays session information for the ASN PC peer specified by its IP address in IPv4 dotted-decimal notation.
  • apn apn_name: Displays session information for an existing Access Point Name (APN) specified as an alphanumeric string of 1 through 63 characters that is case sensitive.
  • csccf-service service_name: Displays session information for an existing Call Session Control Function (CSCF) service specified as an alphanumeric string of 1 through 63 characters.
**Important:** Displays information for in-progress CSCF SIP calls only. Registrations are not considered calls.

- **show session progress**

**Important:** If no PCF address or PDSN service is specified, the session information for all sessions is displayed.

- **show session progress**

**Important:** Displays information for in-progress CSCF SIP calls only. Registrations are not considered calls.

- **dhcp-server dhcp_address**: Displays session information for the Dynamic Host Configuration Protocol (DHCP) server specified by its IP address in IPv4 dotted-decimal notation.

- **epdg-service service_name**: Displays session information for ePDG service specified as an alphanumeric string of 1 through 63 characters that is case sensitive.

- **fa fa_address**: Displays session information for the foreign agent (FA) whose IP address is specified in IPv4 dotted-decimal notation.

- **fa-service fa_name**: Displays session information for the named foreign agent service.

- **ggsn-service ggsn_name**: Displays session information for an existing GGSN service specified as an alphanumeric string of 1 through 63 characters that is case sensitive.

- **gprs-only**: Limits the display to the session information for the SGSN’s 2G MM and PDP contexts.

- **ha ha_address**: Displays session information for the home agent specified by its IP address in IPv4 dotted-decimal notation.

- **ha-service ha_name**: Displays session information for the named home agent (HA) service.

- **hnbgw-only**: Displays session information for the HNB-GW service related sessions instances (such as HNB, IuPS, IuCS).

- **hsgw-service service_name**: Displays session information for an existing HSGW service specified as an alphanumeric string of 1 through 63 characters.

- **lma-service service_name**: Displays session information for an existing Local Mobility Anchor (LMA) service specified as an alphanumeric string of 1 through 63 characters.

- **mme-service service_name**: Displays session information for an existing Mobility Management Entity (MME) service specified as an alphanumeric string of 1 through 63 characters.

- **mag-service service_name**: Displays session information for an existing Mobile Access Gateway (MAG) service specified as an alphanumeric string of 1 through 63 characters.

- **pcf pcf_address**: Displays session information for the packet control function specified by its IP address in IPv4 dotted-decimal notation.

- **pdsn-service pdsn_name**: Displays session information for the named packet data service.

- **pgw-address ip_address**: Displays session progress information for the P-GW specified by its IP address in IPv4 dotted-decimal notation.

- **samog-service service_name**: Displays session progress information for an existing SaMOG service specified as an alphanumeric string of 1 through 63 characters.

- **sgsn-address sgsn-address**: Displays session information for the SGSN specified by its IP address in IPv4 dotted-decimal notation.

- **sgw-service service_name**: Displays session progress information for an existing S-GW service specified as an alphanumeric string of 1 through 63 characters.
show session progress

| { grep grep_options | more }

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of the `grep` and `more` commands, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter.

### Usage

View the session information to troubleshooting subscriber problems and for general monitoring for orphaned sessions.

### Example

The following commands display the status information for the session connected to the packet control function with address 10.2.3.4, packet data service `sampleService`, and for all sessions, respectively.

```
show session progress pcf 10.2.3.4
show session progress pdsn-service sampleService
show session progress
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show session recovery status

Displays session recovery status information for the current context filtered by the options specified.

**Product**
All

**Privilege**
Security Administrator, Administrator, Inspector, Operator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local] host_name#
```

**Syntax**

```
show session recovery status [ verbose ] [ | { grep grep_options | more } ]
```

- `recovery status`
  Displays the current status of the system’s ability to recover from a hardware or software fault that requires the recovery of home agent-based Mobile IP session(s).

- `verbose`
  Includes per-CPU Session Recovery status.

- `{ grep grep_options | more }`
  Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

  For details on the usage of the `grep` and `more` commands, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter.

**Usage**

View the session information for troubleshooting subscriber problems and for general monitoring for orphaned sessions.

**Example**

To display the session recovery status information, enter the following command:

```
show session recovery status
```

Adding the optional `verbose` keyword to this command provides more details.

```
show session recovery status verbose
```

**Important**: Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show session setuptime

Displays session setup time information for all sessions or sessions associated with the specified Access Gateway (AGW).

**Product**
- ePDG
- PDSN
- HNB-GW
- SGSN

**Privilege**
Operator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
show session setuptime [ epdg-only [ verbose ] | hnbw-only | pcf pcf_address | gprs-only | sgsn-address sgsn_address | sgsn-only ] [ | { grep grep_options | more } ]
```

Displays the call setup times aggregated into basic ranges of time.
- **epdg-only**: Display ePDG Session Statistics. **verbose**: Displays session setup times in verbose mode.
- **hnbw-only**: Filters and displays the call setup information for HNB-GW calls only.
- **pcf pcf_address**: displays call setup data for the packet control function whose IP address is specified as `pcf_address`. `pcf_address` must be specified using IPv4 dotted-decimal notation. The call setup times for all PCFs is displayed when no specified PCF is specified.
- **gprs-only**: Displays 2G call setup data for the for the SGSN for the MM and PDP contexts.
- **sgsn-address sgsn_address**: Displays call setup times for the specified SGSN. `sgsn_address` is the IP address of the SGSN and must be expressed in IPv4 dotted-decimal notation. This keyword is used by the GGSN.
- **sgsn-only**: Displays 3G call setup data for the for the SGSN for the MM and PDP contexts.

```
| { grep grep_options | more }
```

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the **Regulating a Command’s Output** section of the **Command Line Interface Overview** chapter.
Usage

View the session information to troubleshooting subscriber problems and for general monitoring for orphaned sessions.
When no keywords are specified, the information shown is cumulative for all sessions that have been facilitated by the system.

Example

The following command shows setup time statistics for all sessions from the PCF at IP address 192.168.10.3:

```
show session setuptime pcf 192.168.10.3
```
show session subsystem

Displays session information for system subsystems. If no keywords are specified, information for all subsystems is displayed.

Product
All

Privilege
Security Administrator, Administrator, Inspector, Operator

Mode
Exec
The following prompt is displayed in the Exec mode:
[local]host_name#

Syntax

show session subsystem [ full | facility facility [ all | instance id ] ] [ verbose ] [ | { grep grep_options | more }]

[ full | facility facility [ all | instance id ] ]

- **full**: Indicates that a full statistics summary of all subsystems is to be displayed.
- **facility facility**: Specifies the facility for which subsystem statistics is to be displayed where facility is specified as one of:
  - `a11mgr`: A11 Manager
  - `aaamgr`: Accounting and Authentication Manager
  - `aaaproxy`: AAA Proxy Manager
  - `alcapmgr`: ALCAP Manager
  - `asngwmgm`: ASN Gateway Manager
  - `asnpcmgr`: ASN Paging/Location-Registry Manager
  - `cscfmgr`: SIP CSCF Manager
  - `cscftmgr`: SIP CSCFTT manager
  - `dgmbmgr`: Diameter Gmb Application Manager
  - `diamproxy`: Diameter Proxy Application Manager [Release 12.0 and earlier versions only]
  - `egtpepgmgr`: EGTP Egress Demux Manager
  - `egtppinmgr`: EGTP Ingress Demux Manager
  - `famgr`: Foreign Agent Manager
  - `gtpcmgr`: GTP-C Manager
  - `gtpumgr`: GTP-U Demux Manager
  - `hamgr`: Home Agent Manager
  - `henbgwdemux`: Home eNodeB Gateway demux manager
  - `henbkgwmgm`: Home eNodeB Gateway Manager
show session subsystem

- **hnbmgr**: HNBGW HNB Manager
- **imsimgr**: SGSN IMSI Manager
- **ipsgmgr**: IP Services Gateway Manager
- **l2tpdemux**: L2TP Demux Manager
- **l2tpmgr**: L2TP Manager
- **linkmgr**: SGSN/SS7 Master Manager
- **magmgr**: Mobile Access Gateway Manager
- **megadiammgr**: MegaDiameter Manager
- **mmedemux**: MME Demux Manager
- **mmemgr**: MME Manager
- **mmgr**: SGSN/SS7 Master Manager
- **pdgmgr**: PDG Manager
- **phsgwmgr**: PHS Gateway Manager
- **phspcmgr**: PHS Paging Controller Manager
- **sessmgr**: Session Manager
- **sgtpcmgr**: SGSN GTP-C Manager

- **all | instance id**: the keyword `all` indicates all instances of the specified facility are to be displayed whereas the keyword `instance` specifies a specific instance for which information is to be displayed where `id` must be specified as an integer from 0 through 4294967295. If all or instance is not specified summary statistics are displayed.

**verbose**

Displays everything the `show session subsystem` command displays with the exception that the Setup Time statistics are reported in 100 millisecond increments from 100 ms up to 9600 ms.

```
| { grep grep_options | more }
```

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the `grep` and `more` commands, refer to the `Regulating a Command’s Output` section of the `Command Line Interface Overview` chapter.

**Usage**

View the session information to troubleshooting subscriber problems and for general monitoring for orphaned sessions.

If this command is entered with no keywords, the information displayed is cumulative for all sessions facilitated by the system.

**Example**

The following commands display the statistics information summarized for all sessions, then for the `famgr` facility (all sessions), and finally only for the session ID `127589` for the `hamgr` subsystem.

```
show session subsystem full

show session subsystem facility famgr all
```
show session subsystem facility hamgr instance 127589

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show session trace

Displays status and statistics for the session trace application.

Product

GGSN
MME
P-GW
SAEGW
S-GW

Privilege

Inspector

Mode

Exec

The following prompt is displayed in the Exec mode:

[local] host_name#

Syntax

show session trace { statistics | subscriber network-element { ggsn | mme | pgw | sgw } trace-ref value | tce-address ip_address tce-index num | tce-summary | trace-summary } [{ grep grep_options | more }]

| statistics |
| Displays summary statistics for the session trace subsystem. |

| subscriber network-element { ggsn | mme | pgw | sgw } trace-ref value |
| Displays status and statistics for a specified session trace using the network element type; GGSN, MME, P-GW, and S-GW, and a valid trace reference of 12 characters. |

| tce-address ip_address tce-index num |
| Displays status and statistics for an existing Trace Collection Entity (TCE) connection specified by its IP address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation. |
| tce-index num: Specifies a TCE index of the trace collection entity as an integer from 0 through 7. |

| tce-summary |
| Displays a summary of all active TCE connections. |

| trace-summary |
| Displays a summary of all active session traces. |

| { grep grep_options | more } |
| Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent. |
For details on the usage of the `grep` and `more` commands, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter.

### Usage

Use this command to display status and statistics for the session trace application.

### Example

The following command displays status and statistics for a subscriber session trace on a P-GW with a trace reference of 32223398765:

```bash
show session trace subscriber network-element pgw trace-ref 32223398765
```

The following command displays status and statistics for a subscriber session trace on an MME with a trace reference of 32221234567:

```bash
show session trace subscriber network-element mme trace-ref 32223398765
```

The following command displays status and statistics for a subscriber session trace on a GGSN with a trace reference of 1203398765:

```bash
show session trace subscriber network-element ggsn trace-ref 1203398765
```

---

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show session-event-record

Displays session event module statistics and file space usage information.

Product
S-GW
SAEGW

Privilege
Operator

Mode
Exec

The following prompt is displayed in the Exec mode:
[local] host_name#

Syntax

show session-event-record { file-space-usage | statistics }

file-space-usage
Displays session event module file storage limits and capacities.

statistics
Displays session event module statistics regarding the handling and transfer of event records to an external collection server.

Usage
View the session event information to troubleshoot handling and transfer problems and for general monitoring for file storage use.

Example
The following command displays the file storage limit and use for all event modules on the system:

show session-event-record file-space-usage
show sf

Displays switch fabric task (SFT) information associated with packet processing cards.

**Product**
All

**Privilege**
Inspector

**Syntax**

```sh
show sf stats sft [ historical ]
```

- `historical`
  Displays historical information regarding SFT performance.

**Usage**

Use this command to display information and statistics about the switch fabric task.

**Example**

The following command displays statistics for the SFT:

```
show sf stats sft
```
show sgs-service

Displays information and statistics about Visitor Location Register (VLR) SGs interface services configured on this system.

Product
MME

Privilege
Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show sgs-service { all | name name | offload-status [ service-name sgs_svc_name ] | statistics { all | name name } | vlr-status [ service-name sgs_svc_name ] [ vlr-name name ] [ full ] [ | { grep grep_options | more } ]

all
Displays information about all SGs interface services configured on this system.

display name name
Displays information about an existing SGs service specified as an alphanumeric string of 1 through 63 characters.

offload-status sgs_svc_name
Displays statistics for all VLRs flagged for offload for an existing SGs service specified as an alphanumeric string of 1 through 63 characters.

statistics { all | name name }
Displays statistics for SGs services configured on this system.
a ll: Displays statistics for all SGs services configured on this system.
name name: Displays statistics for an existing SGs service specified as an alphanumeric string of 1 through 63 characters.

vlr-status [ service-name name ] [ vlr-name name ] [ full ]
Displays status information about VLRs configured in SGs services on this system.

service-name sgs_svc_name: Displays names and states of VLRs configured in an existing SGs service specified as an alphanumeric string of 1 through 63 characters.

vlr-name name: Displays the name and state of an existing VLR configured in SGs services on this system and specified as an alphanumeric string of 1 through 63 characters.

full: Displays additional information about VLRs configured in SGs services on this system. Additional information includes ports, addresses and peer IDs.
**Usage**

Use this command to display information and statistics about SGs services configured on this system.

**Example**

The following command displays statistics for an SGs service named *sgs3*:

```
show sgs-service name sgs3
```

The following command displays VLR status information for a configured VLR named *vlr-main*:

```
show sgs-service vlr-status vlr-name vlr-main
```
show s4-sgsn statistics

Displays statistics related to S4 functionality on the SGSN.

**Product**
SGSN

**Privilege**
Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
show s4-sgsn statistics [ all | smgr-instance <instance_number> ]
```

- **all**
  Show all S4-SGSN statistics from all session managers.

- **smgr-instance**
  Show the statistics for a session manager instance of the SGSN service. `<instance_number>` must be specified as an integer between 1 and 65535.

**Important:** If no option is specified, then S4-SGSN statistics from all session managers will be added up and the cumulative totals will be shown.

**Usage**

Use this command to display information for S4-SGSN related services.

**Example**

The following commands displays and clear S4-SGSN-related statistics for all services on the system:

```
show s4-sgsn statistics all

clear s4-sgsn statistics all
```
show sgsn fsm-statistics

The output of this command provides information on 3G SGSN (both Gn and S4) application FSM statistics.

Product
SGSN

Privilege
Inspector, Operator, Administrator, Security Administrator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show sgsn fsm statistics { umts-sm | umts-pmm | all }

- **umts-sm**
  Displays 3G Session Management Access Side FSM statistics.

- **umts-pmm**
  Displays 3G Mobility Management PMM FSM statistics.

- **all**
  Displays all SGSN application FSM statistics.

Usage

Use this command to track 3G SGSN (both Gn and S4) application FSM statistics. The SGSN application FSM statistics will help collect the FSM usage information to quantify which events / state collisions happen most often in the field.

Example

Enter this command to display all SGSN FSM statistics:

```
show sgsn fsm statistics all
```
show sgsn sessmgr

Displays session manager (SessMGR) statistics specific to the SGSN service.

**Product**
SGSN

**Privilege**
Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

**Syntax**

```
show sgsn sessmgr { all | instance smgr_inst }
```

- **all**
  Displays all SessMGR statistics specific to the system’s SGSN services.

- **instance smgr_inst**
  Displays the statistics for a session manager instance of the SGSN service specified as an integer between 1 and 1000000.

**Usage**

Use this command to display information for SGSN services.

**Example**

The following command displays SGSN SessMGR statistics for all SGSN services on the system:

```
show sgsn sessmgr all
```
show sgsn-fast-path

Displays information related to SGSN fast-path.

Product
SGSN

Privilege
Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show sgsn-fast-path statistics [ all | smgr-instance smgr_inst ] [ | { grep grep_options | more } ]

all
Displays fast-path statistics for all session managers.

smgr-instance smgr_inst
For releases prior to 14.0, this keyword displays the fast-path statistics for a session manager instance specified as an integer between 1 and 65535.
For releases 14.0 and higher, this keyword displays the fast-path statistics for a session manager instance specified as an integer between 1 and 384.

| { grep grep_options | more }

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of the grep and more commands, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage
Use this command to display statistics for SGSN fast-path configurations.

Example
The following command displays fast-path statistics for all SGSN session managers:

    show sgsn sessmgr all
show sgsn-map-app

Displays collected statistics for the SGSN Mobile Application Part (MAP).

Product
SGSN

Privilege
Inspector

Mode
Exec
The following prompt is displayed in the Exec mode:

[local] host_name#

Syntax

show sgsn-map-app statistics [ | { grep grep_options | more } ]

all
Displays collected statistics for the SGSN MAP application.

| { grep grep_options | more }
Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of the grep and more commands, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage
Use this command to display statistics for the SGSN MAP application.

Example
The following command displays SGSN MAP statistics:

    show sgsn-map-app statistics
**show sgsn-mode**

Displays the SGSN global configuration.

**Product**

SGSN

**Privilege**

Inspector

**Mode**

Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
show sgsn-mode[ | { grep grep_options | more } ]
```

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the **Regulating a Command’s Output** section of the **Command Line Interface Overview** chapter.

**Usage**

Use this command to display the configuration created with the commands in the SGSN Global Configuration mode.

**Example**

The following command displays the SGSN global configuration:

```
show sgsn-mode
```
show sgsn-operator-policy

This command has been deprecated. Refer to the `show operator-policy` command.
show sgsn-pool

Displays collected pooling statistics for either GPRS services or SGSN services.

**Product**
SGSN

**Privilege**
Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

**Syntax**

```
show sgsn-pool statistics { gprs-service srvc_name | sgsn-service srvc_name} { nri-value nri_value | peer-non-broadcast-lac lac rac | target-load-in-progress [ smgr-instance smgr_instance | target-nri target_nri ] | target-offloaded-to-peer [ target-nri target_nri ] } [ | { grep grep_options | more } ]
```

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the `grep` and `more` commands, refer to the `Regulating a Command’s Output` section of the `Command Line Interface Overview` chapter.

**Usage**

Use this command to display the collected statistics for pooling in either GPRS or SGSN services. The outputs can be filtered to focus the statistics displayed.

**Example**

The following command displays the:

```
show sgsn-pool statistics sgsn-service sgsn1 nri-value 3
```
show sgsn-service

Displays information about the configured SGSN services in the current context.

Product
SGSN

Privilege
Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show sgsn-service { all | name srvc_name }

all
Displays information for all SGSN services in the current context.

name srvc_name
Displays information for an existing SGSN service specified as an alphanumeric string of 1 through 63 characters.

Usage

Use this command to display information for SGSN services.

Example

The following command displays information for all SGSN services in the current context:

show sgsn-service all

The following command displays information for an SGSN service in the current context that is named sgsn1:

show sgsn-service name sgsn1

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show sgtp-service

Displays information about the configured GPRS Tunnelling Protocol (SGTP) services in the current context, including GTP-C and GTP-U operational configuration.

Product
SGSN
PDG/TTG
MME

Privilege
Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax


- **all [ gtpu-table ]**
  Displays configuration information for all of the SGTP services defined for the current context.
  **gtpu-table**: Limits the output to GTPU information for all SGTP services.

- **ggsn-table [ smgr-instance smgr_instance ]**
  Displays GGSN information configured for the SGTP service(s) in the current context.
  **smgr-instance smgr_instance** enter an integer from 1 through 384 to limit the GGSN output to information for a specific session manager.

- **mbms-bearers**
  This keyword is specific to the SGSN and is not yet supported.

- **name srvc_name [ gtpu-table ]**
  Displays information for the specified SGTP service in the current context. **srvc_name** must be an alphanumeric string of 1 through 63 characters that identifies a configured SGTP service.
  **gtpu-table**: Limits the output to GTPU information for a specific SGTP service.

- **sgsn-table**
  Displays SGSN information configured for the SGTP service(s) in the current context.

Usage

Use this command to control the display of SGTP services information.
The following command displays information for all SGTP services in the current context:

```
show sgtp-service all
```

The following command displays the GGSN information in SGTP services in the current context:

```
show sgtp-service ggsn-table
```

The following command displays the SGSN information in SGTP services in the current context:

```
show sgtp-service sgsn-table
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference.*
show sgtpc statistics

Displays all statistics, for SGSN GPRS Tunnelling Protocol (SGTP) interface parameters, collected since the last restart or last use of a clear command.

Product
SGSN
PDG/TTG
MME

Privilege
Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:
[local]host_name#

Syntax

```
show sgtpc statistics [ all | gsn-address ipv4_address | sgtp-service sgtp_srvc_name ] [ verbose ] [ | { grep grep_options | more } ]
```

| all |
| Displays configuration information for all of the SGTP services defined for the current context. |

| gsn-address ipv4_address |
| Displays statistics for an SGSN specified by its IP address in IPv4 dotted-decimal notation. This must be an existing and active interface. |

| sgtp-service sgtp_srvc_name |
| Displays statistics for an existing SGTP service specified as an alphanumeric string from 1 through 63 characters. |

| verbose |
| Causes the system to displays more detailed level of statistics. |

| | { grep grep_options | more } |
| Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent. |

For details on the usage of the grep and more commands, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage

Use this command to display information for SGSN services.

Example
The following command displays statistics for the SGTP service named `sgtp1`:

```bash
show sgtpc statistics sgtp-service sgtp1
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show sgtpu statistics

Displays all transmission and reception statistics for pre-defined and active GTP-U interfaces collected since the last restart or last use of a **clear** command.

**Product**
SGSN
PDG/TTG

**Privilege**
Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
show sgtpu statistics [ ggsn-address ipv4_address | gprs-service gprs_srvc_name nsei nse_id | iups-bind-address ipv4_address | iups-service iups_srvc_name | rnc-address ipv4_address | sgtp-service sgtp_srvc_name ] [ [ grep grep_options | more ] ]
```

- **ggsn-address ipv4_address**
  Displays statistics for the GGSN specified by its IP address in IPv4 dotted-decimal notation.

- **gprs-service gprs_srvc_name nsei nse_id**
  Displays NSEI-based GTPU statistics associated with an existing GPRS service specified as an alphanumeric string of 1 through 63 characters.
  
  **nsei nse_id**: Specifies a GPRS NSEI as an integer from 0 through 65535.

- **iups-bind-address ipv4_address**
  Displays SGSN GPRS Tunnelling Protocol (SGTP) statistics for an Iu GTPU interface specified by its IP address in IPv4 dotted-decimal notation.

- **iups-service iups_srvc_name**
  Displays statistics for an existing IuPS service specified as an alphanumeric string of 1 through 63 characters.

- **rnc-address ipv4_address**
  Displays statistics for a Radio Network Controller (RNC) identified by its IP address in IPv4 dotted-decimal notation.

- **sgtp-service sgtp_srvc_name**
  Displays statistics for an existing SGTP service specified as an alphanumeric string of 1 through 63 characters.
Pipe (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of the grep and more commands, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

**Usage**

Use this command to display statistics for the SGTPU interface.

**Example**

The following command displays GTP-U statistics for the traffic between an SGSN and a connected RNC:
```
show sgtpu statistics rnc-address 123.1.2.3
```
show sgw-service

Displays configuration settings and/or service statistics for Serving Gateway (S-GW) services on this system.

**Product**
S-GW
SAEGW

**Privilege**
Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

**Syntax**

```plaintext
show sgw-service { all | name service_name | statistics { all | name service_name } } [ | { grep grep_options | more } ]
```

- **all**
  Displays configuration information for all S-GW services configured on this system.

- **name service_name**
  Displays configuration information for an existing S-GW service specified as an alphanumeric string of 1 through 63 characters.

- **statistics { all | name service_name }**
  - **all**: Displays statistics for all S-GW services on this system or for a specified service.
  - **name service_name**: Displays statistics for an existing S-GW service specified as an alphanumeric string of 1 through 63 characters.

  | { grep grep_options | more } |
  Indicates the output of the command is to be piped (sent) to the command specified. A command to send output to must be specified.

  For details on the usage of the `grep` and `more` commands, refer to the Regulating a Command’s Output section in the Command Line Interface Overview chapter.

**Usage**

Use this command to view configuration settings and/or service statistics for S-GW services on this system.

**Example**

The following command displays service statistics for the S-GW service named `sgw1`:

```plaintext
show sgw-service statistics name sgw1
```
show sms statistics

Displays traffic statistics for the Short Message Service (SMS).

Product
SGSN

Privilege
Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show sms statistics [ gprs-only | name map_svc | sgsn-only ] [ verbose ] [ | { grep grep_options | more } ]

- **gprs-only**
  Displays only GPRS access type SMS statistics.

- **name map_svc**
  Displays statistics for an existing MAP service specified as an alphanumeric string of 1 through 63 characters.

- **sgsn-only**
  Displays only UMTS access type SMS statistics.

- **verbose**
  Causes the system to displays more detailed level of statistics.

- | { grep grep_options | more }
  Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

  For details on the usage of the **grep** and **more** commands, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage
Use this command to display traffic statistics for the SMS services.

Example
Use the following command to display SMS statistics for 3G traffic:

  show sms statistics sgsn-only
Important: Output descriptions for commands are available in the *Statistics and Counters Reference*.
show sndcp statistics

Displays statistics for the packet traffic going through the Subnetwork Dependent Convergence Protocol (SNDCP) layer.

**Product**
SGSN

**Privilege**
Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
show sndcp statistics [ gprs-service srvc_name ] [ verbose ] [ | { grep grep_options | more } ]
```

- **gprs-service srvc_name**
  Displays statistics for an existing GPRS service specified as an alphanumeric string of 1 through 63 characters.

- **verbose**
  Displays a more detailed level of statistics.

- `| { grep grep_options | more }`
  Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
  For details on the usage of the `grep` and `more` commands, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter.

**Usage**

Use this command to display SNDCP traffic statistics. Include the `gprs-service` keyword to filter the output to statistics for only one GPRS service.

**Example**

Use the following command to display all SNDCP layer traffic statistics:

```
show sndcp statistics verbose
```

Use the following command to display SNDCP layer traffic statistics for the `test1` GPRS service:

```
show sndcp statistics gprs-service test1
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*. 

---

Cisco ASR 5x00 Command Line Interface Reference

4670
show snmp

Displays information on the Simple Network Management Protocol (SNMP) servers and interfaces.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show snmp { accesses | communities | notifies | server | transports | trap { history [ url | varbind | verbose ] | statistics [ verbose | wide ] } [ | { grep grep_options | more } ] }

- **accesses**: Displays SNMP server usage statistics.
- **communities**: Displays SNMP community strings.
- **notifies**: Displays SNMP event trap and notification statistics.
- **server**: Displays SNMP server configuration information.
- **transports**: Displays trap destination configuration information.
- **trap { history [ url | varbind | verbose ] | statistics [ verbose | wide ] }**: Displays SNMP event trap history. **trap history** Displays up to 5,000 time-stamped trap records stored in a buffer. The buffer may be cleared by entering the **clear snmp history** command. **statistics**: Displays SNMP event trap and notification statistics. **url pathname**: Redirects output to a file. **varbind**: Displays varbind-based output which is easier to parse, but harder for an operator to read. **verbose**: Displays rows for every defined trap, even if never generated. **wide**: Displays trap statistical data in excess of 80 columns.
Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of the `grep` and `more` commands, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter.

**Usage**

Display SNMP information as part of system verification and troubleshooting.

**Example**

The following commands display the usage statistics, community string information, event trap and notification data, server information, and trap destination configuration, respectively.

```
show snmp communities
show snmp transport
show snmp server
show snmp accesses
show snmp notifies
show snmp trap history
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show srp

Displays the Service Redundancy Protocol (SRP) information.

Product
All products that support Interchassis Session Recovery (ICSR)

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show srp { audit-statistics [ all | instance number ] [ message-level | session-level ] | call-loss statistics | checkpoint statistics [ active | standby ] [ verbose ] | info | monitor [ all | authentication-probe | bfd | bgp | diameter ] | statistics } | [ grep grep_options | more ]

audit-statistics [ all | instance number ] [ message-level | session-level ]
Displays statistics of external audit.
all: Displays information for all Session Managers.
instance number: Displays information for an instance number of Session Manager, specified as an integer from 1 through 4294967295.
message-level: Displays message-level statistics.
session-level: Displays session-level statistics.

call-loss statistics
Displays history of lost calls during switchover.

checkpoint statistics [ active | standby ] [ verbose ]
Displays check pointing statistics on session redundancy data (session managers, current call recovery records, etc.).
active: Displays information for the active chassis.
standby: Displays information for the standby chassis.
verbose: Displays cumulative information for all session managers in tabular output.

info
Displays Service Redundancy Protocol information (context, chassis state, peer, connection state, etc.).

monitor [ all | authentication-probe | bfd | bgp | diameter ]
Displays SRP monitor information.
all: Displays monitor information for all types (authentication-probe, bgp, and diameter).
authentication-probe: Displays authentication probe monitor information.
bfd: Displays BFD monitor information.
**show srp**

- **bgp**: Displays BGP monitor information.
- **diameter**: Displays Diameter monitor information.

**statistics**

Displays SRP statistics (hello messages sent, configuration validation, resource messages, switchovers, etc.).

| { grep grep_options | more }

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the `grep` and `more` commands, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter.

**Usage**

The output of this command may be considered as part of a periodic system auditing program by verifying the Service Redundancy Protocol performance. For more information, refer to the *Interchassis Session Recovery* appendix of the *System Administration Guide* and the *Service Redundancy Protocol Configuration Mode* chapter of this guide.

**Example**

The following commands display Service Redundancy Protocol information:

- `show srp audit-statistics`
- `show srp call-loss statistics`
- `show srp checkpoint statistics`
- `show srp info`
- `show srp monitor`
- `show srp statistics`

**Important**: Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show ss7-routing-domain

This command displays the configuration information for the defined Signalling System #7 (SS7) routing domains. Since SS7 routing domains encompass a large number of operational parameters, this command enables you to narrow your displays to specific protocol parameters on a specific link.

Product
SGSN

Privilege
Security Administrator, Administrator, Inspector, Operator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show ss7-routing-domain { all | ss7rd_id { m3ua | mtp2 | mtp3 | qsaal | routes [ adjacent ] | sctp asp { all | instance asp_id } | sccf } }

show ss7-routing-domain ss7rd_id m3ua { statistics { gen | peer-server { all | id peer-server_id peer-server-process { all | instance psp_instance } } } | status { address-translation-table | destination-point-code { all | ss7_dpc } | gen | peer-server peer-server_id | peer-server-process instance psp_id | verbose } }

show ss7-routing-domain 1 sccf { statistics linkset { all | id linkset_id link { all | id link_id } } | status linkset { all | id linkset_id link { all | id link_id [ verbose ] } } }

ss7-routing-domain { all | ss7rd_id }

all: Displays information for all SS7 routing domains.
ss7rd_id: Displays information for the SS7 routing domain ID specified as an integer from 1 through 12.

m3ua
Displays statistics and status information for the SS7 MTP3 User Adaptation Layer (M3UA) in the specified SS7 routing domain.

mtp2
Displays statistics and status information for the SS7 Message Transfer Part-2 (MTP2) in the specified SS7 routing domain.

mtp3
Displays statistics and status information for the SS7 Message Transfer Part-3 (MTP3) in the specified SS7 routing domain.
qsaa1
Displays statistics and status information for the Service Specific Connection-Oriented Protocol (SSCOP) sub-layer of the Quasi Signaling Application Adaptation Layer (QSAAL) in the specified SS7 routing domain.

routes [ adjacent ]
Displays the destination point code (DPC) routing table.
adjacent: If this keyword is used with the routes keyword, access is provided to the statistics and status information for configured adjacent point codes.

sctp asp { all | instance asp_id }
Provides access to the status or statistics for the Stream Control Transmission Protocol (SCTP) application server processes (ASP) in the specified SS7 routing domain for all or a specified SCTP ASP instance.
• all: Displays the information for all SCTP application server process instances for a specific SS7 routing domain.
• instance asp_id: Displays the information for an SCTP application server process instance specified as an integer from 1 through 4.

sscf
Displays statistics and status information for the Service Specific Coordination Function (SSCF [q.2140]) in the specified SS7 routing domain.

peer-server [ all | id peer-server_id ]
Filters the information for the specific protocol in the SS7 routing domain for all or a specific peer server ID.
• all: Displays the information for all peer servers for a specific protocol.
• id peer-server_id: Indicates the specific linkset identifier as an integer from 1 through 49.

peer-server-process [ all | instance instance_id ]
Filters the information for the specific protocol in the SS7 routing domain for all or a specific instance of peer-server process.
• all: Displays the information for all peer server process instances for a specific protocol.
• instance instance_id: Specifies a peer server process instance as an integer from 1 through 4.

destination-point-code [ all | dest_point_code]
Filters the information for the specific protocol in the SS7 routing domain for all or a specific DPC.
• all: Displays the information for all DPCs in the SS7 routing domain.
• dest_point_code: Specifies a DPC in the SS7 routing domain.

gen
Displays general information for the specific protocol in the specified SS7 routing domain.

verbose
Enables the display of maximum information for a protocol.
linkset [ all | id linkset_id ]
Filters the information for the specific protocol in SS7 routing domain for all or a specific link set.
- **all**: Displays the information for all linkset for a specific protocol.
- **id linkset_id**: Specifies a linkset identifier as an integer from 1 through 49.

link [ all | id link_id ]
Filters the information for a specified protocol in the SS7 routing domain for all or a specific link set.
- **all**: Displays the information for all links for a specific protocol.
- **id link_id**: Specifies a linkset identifier as be an integer from 1 through 16.

**Usage**
Use this command to display the SS7 routing domain and different layer protocol information for SGSN service.

**Example**
Displays the information/statistics for all SCTP application server processes of peer server ID 17 and peer server process instance 1 in SS7 routing domain 12:

```
show ss7-routing-domain 12 sctp asp all status peer-server id 17 peer-server-process instance 1
```

**Important**: Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show ssh key

Displays the secure shell (SSH) public key information.

**Product**
All

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
show ssh key [ type { v1-rsa | v2-rsa | v2-dsa } ] [ | { grep grep_options | more } ]
```

- Specifies the type of SSH key information to display. If type is not specified, information for all types is displayed.
  - **v1-rsa**: SSH v1 RSA host key only
  - **v2-rsa**: SSH v2 DSA host key only
  - **v2-dsa**: SSH v2 RSA host key only

- Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
  - For details on the usage of the `grep` and `more` commands, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

**Usage**

Show the secure shell key information for all types to verify installed keys.

**Example**

The following command shows information for all SSH V1 and SSH V2 keys:

```
show ssh key
```

The following command shows information for only SSH V2 RSA host keys:

```
show ssh key type v2-rsa
```
show ssl cipher-suite

Displays information related to Secure Sockets Layer (SSL) cipher suites since the last restart or clear command. A cipher suite contains the cryptographic algorithms supported by the client.

**Product**
SCM (P-CSCF, A-BG)

**Privilege**
Security Administrator, Administrator, Inspector, Operator

**Mode**
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

**Syntax**

```
show ssl cipher-suite [ name name ] [ | { grep grep_options | more } ]
```

- **name name**
  Displays information related to the SSL cipher suite specified as an alphanumeric string of 1 through 127 characters.

- | { grep grep_options | more }
  Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
  For details on the usage of the `grep` and `more` commands, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

**Usage**
Use this command to display information related to SSL cipher suites.

**Example**
The following command displays information for the SSL cipher suite `ssl_cipher_suite_1`:

```
show ssl cipher-suite name ssl_cipher_suite_1
```
show ssl connection

Displays information pertaining to Secure Sockets Layer (SSL) connections on the Proxy Call Session Control Function (P-CSCF).

Product
SCM (P-CSCF, A-BG)

Privilege
Security Administrator, Administrator, Inspector, Operator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show ssl connection [ list | summary [ service-name name ] ] [ name name ] [ | { grep grep_options | more } ]

- **list**
  Lists the SSL connections on the P-CSCF.

- **summary**
  Displays state and statistical information for the SSL connections on the P-CSCF.

- **service-name name**
  Lists the SSL connections on the P-CSCF for the specified P-CSCF service, or displays state and statistical information for the SSL connections on the P-CSCF for the specified P-CSCF service.
  name must be an alphanumeric string of 1 through 63 characters.

- **name name**
  Displays state and statistical information for the SSL connection specified as an alphanumeric string of 1 through 127 characters.

  | { grep grep_options | more }
  Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
  For details on the usage of the **grep** and **more** commands, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage

Use this command in Exec Mode to display information and statistics pertaining to SSL connections. If the **summary** keyword is not used, detailed information is displayed.

Example

The following command displays SSL connection information for the P-CSCF service **pcscf_tls_1**: 

show ssl connection list service-name pcscf_tls_1
show ssl map

Displays information related to configured Secure Sockets Layer (SSL) maps/templates since the last restart or clear command.

Product
SCM (P-CSCF, A-BG)

Privilege
Security Administrator, Administrator, Inspector, Operator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show ssl map [ map-type ssl-subscriber-template ] [ name name ] [ | { grep grep_options | more } ]

map-type ssl-subscriber-template
Displays information related to configured SSL maps/templates for the SSL map/template type ssl-subscriber-template.

name name
Displays information related to configured SSL maps/templates for the map/template name specified as an alphanumeric string of 1 through 127 characters.

| { grep grep_options | more }
Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of the grep and more commands, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage
Use this command to display information related to configured SSL maps/templates.

Example
The following command displays information related to configured SSL maps/templates for the SSL map/template ssl_template_1:

show ssl map name ssl_template_1
show ssl statistics

Displays statistics for Secure Sockets Layer (SSL) since the last restart or clear command.

Product
SCM (P-CSCF, A-BG)

Privilege
Security Administrator, Administrator, Inspector, Operator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show ssl statistics [ service-name name ] [ | { grep grep_options | more } ]

service-name name
Displays SSL statistics for the Proxy Call Session Control Function (P-CSCF) service. specified as an alphanumeric string of 1 through 127 characters.

| { grep grep_options | more } |
Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the grep and more commands, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage
Use this command to display SSL statistics.

Example

The following command displays SSL statistics for all P-CSCF services:

show ssl statistics
show subscribers

Displays information for subscriber sessions that are defined by specified keywords. Command keywords are base commands that display distinctive types of data. Filter keywords are a superset of command keywords that modify or filter the output of the base commands.

**Important:** Not all filter keywords are available for all command keywords. CLI Help displays available filter keywords based on: the platform type (ASR 5000 or ASR 5500), the products that are licensed to run on the platform, and the preceding command keyword and subsequent filter keywords.

**Product**
All

**Privilege**
Security Administrator, Administrator, Inspector, Operator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local] host_name#
```

**Syntax**

```
show subscribers [ command_keyword ] [ filter_keywords ] [ | { grep grep_options | more } ]
```

**command_keyword**

The following keywords are base commands that each have a distinct display output. Only one command keyword can be entered on the command line.

**aaa-configuration**

Displays Authentication Authorization and Accounting (AAA) configuration information for subscriber sessions defined by the specified filter keywords. The following filter keywords are valid with this command:

```
active, active-charging-service, all, apn, asn-peer-address, asngw-service, asnpd-service, bandwidth-policy, bearer-establishment, bng-service, callid, card-num, cbb-policy, ccoa-only, configured-idle-timeout, connected-time, dhcp-server, dormant, ebi, enodeb-address, epdg-address, fa, fa-service, firewall, fw-and-nat, ggsn-service, gprs-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, hnbgw-only, hsgw-service, idle-time, imsi-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-address, l3-tunnel-remote-address, lac, lac-service, lma-service, lns, lns-service, long-duration-time-left, mag-service, mip-udp-tunnel-only, mipv6a-service, mme-address, mme-service, msid, nemo-only network-requested, network-type, pcf, pdg-service, pdif-service, psdn-service, pgw-address, plmn-type, profile-id, profile-name, qci, rx-data, slu-state, s5-proto, session-time-left,
```
Exec Mode show Commands (Q-S)

```bash
show subscribers

sgsn-address, sgsn-service, sgw-address, sgw-service, tx-data, username, verbose, grep, more
```

## access-flows { accounting | dynamic | pre-provisioned | static }

Shows the ip-flows for the subscribers defined by the specified filter keywords.
- **accounting**: displays the accounting type of access flows for a subscriber.
- **dynamic**: displays the dynamic type of access flows for a subscriber.
- **pre-provisioned**: displays the pre-provisioned type of access flows for a WiMAX subscriber.
- **static**: displays the static type of access flows for a subscriber.

The following filter keywords are valid with this command:

active, active-charging-service, all, apn, asn-peer-address, asngw-service, asnp-service, callid, card-num, ccoa-only, configured-idle-timeout, connected-time, dhcp-server, dormant, epdg-address, fa, fa-service, flow-type, ggsn-service, gprs-service, gsm-traffic-class, ha, ha-ipsec-only, ha-service, hnbgw-only, hsgw-service, idle-time, imsi, ip-address, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-address, l3-tunnel-remote-address, lac, lac-service, lma-service, lns, lns-service, long-duration-time-left, mag-service, mip-udp-tunnel-only, mme-address, mme-service, msid, msisdn, network-requested, network-type, pcf, pdg-service, pdif-service, pdsn-service, pgw-address, plmn-type, rulebase, rx-data, session-time-left, sgsn-address, sgsn-service, sgw-address, sgw-service, tx-data, username, verbose, grep, more

## access-type { lxcdma | ehrpd | lte | undetermined | wcdma | wifi | wired }

Displays active subscribers using a specific type of UE.
- **lccdma**: 1XCDMA – Wireless CDMA 1x high speed internet service
- **ehrpd**: eHRPD – Enhanced High Rate Packet Data
- **evdo**: EvDO – EVolution-Data Optimized
- **lte**: LTE – Long Term Evolution
- **undetermined**: undefined
- **wcdma**: WCDMA – Wideband Code Division Multiple Access
- **wifi**: WiFi – Wireless local area network
- **wired**: wired

The following filter keywords are valid with this command:

access-type, bearer-establishment, bng-service, callid, card-num, configured-idle-timeout, csclf-service, domain, ebi, enodeb-address, fa, firewall, fw-and-nat, gtp-version, gtpu-bind-address, gtpu-service, ha, hnbgw-service, idle-time, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, long-duration-time-left, mipv6ha-service, msid, nat, network-type, profile-id, profile-name, qci, rx-data, slu-state,
Exec Mode show Commands (Q-S)

**show subscribers**

security-type, session-time-left, sgw-address, smgr-instance, tx-data, ue-type, username, grep, more

**active**

Displays active subscribers. When no Filter Keywords are specified, the output is a summary of all active subscribers. When Filter Keywords are specified, the percentage is displayed as graphs in which one is displayed using a high sampling rate, a 10-second interval between samples, and a low sampling rate, a 15-minute interval between samples.

The following filter keywords are valid with this command:

apn, asn-peer-address, asngw-service, asncmp-service, bearer-establishment, bng-service, callid, card-num, ccoa-only, configured-idle-timeout, connected-time, dhcp-server, ebi, epdg-address, fa, fa-service, firewall, fw-and-nat, ggsn-service, gprs-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipse-only, ha-service, hsgw-service, idle-time, imei, ims-auth-service, imsi, ip-address, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, lac, lac-service, lma-service, ins, lns-service, long-duration-time-left, mag-service, mme-address, mme-service, msid, msisdn, nat, nemo-only, network-requested, pcf, pdg-service, pfif-service, pdsn-service, pgw-address, plmn-type, profile-id, profile-name, qci, rx-data, slu-state, session-time-left, sgsn-address, sgsn-service, smgr-instance, sgw-address, sgw-service, tx-data, username, grep, more

**active-charging-service acs_service**

Displays information for subscribers being processed by the active charging service specified as an alphanumeric string of 1 through 15 characters.

The following filter keywords are valid with this command:

active-charging-service, bandwidth-policy, bearer-establishment, bng-service, callid, card-num, ccb-policy, configured-idle-timeout, connected-time, ebi, enodeb-address, epdg-address, fa, firewall, fw-and-nat, gtp-version, gtpu-bind-address, gtpu-service, ha, idle-time, ims-auth-service, imsi, ip-address, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-address, long-duration-time-left, mag-service, mipv6ha-service, msid, nat, network-type, profile-id, profile-name, qci, rulebase, rx-data, slu-state, s5-proto, session-time-left, sgw-address, smgr-instance, tx-data, username, grep, more

**activity**

Displays subscriber link activity percentage. When no Filter Keywords are specified, the output is a summary of all subscriber activity. When Filter Keywords are specified, the link activity percentage is displayed as graphs in which one is displayed using a high sampling rate, a 10-second interval between samples, and a low sampling rate, a 15-minute interval between samples.

The following filter keywords are valid with this command:

active, all, apn, ASN-peer-address, asngw-service, asncmp-service, bearer-establishment, bng-service, callid, card-num, ccoa-only, configured-idle-timeout, connected-time, dhcp-server, dormant, ebi, enodeb-address, epdg-address, fa, fa-service, firewall, fw-and-nat,
The following filter keywords are valid with this command:

- `ip_address` Displays information for subscribers on an ASN
- `asn` Displays subscribers currently facilitated by the Access Point name (APN) configured on the SGSN or GGSN.
- `apn` Displays all current subscribers who have either active or dormant sessions.

### all ip_address
Displays all current subscribers who have either active or dormant sessions.

### apn apn_string
Displays subscribers currently facilitated by the Access Point name (APN) configured on the SGSN or GGSN.

The following filter keywords are valid with this command:

- `activecharging-service`, `apn`, `bandwidth-policy`, `bearer-establishment`, `bng-service`, `callid`, `card-num`, `cbp-policy`, `ccoa-only`, `configured-idle-timeout`, `connected-time`, `dhcp-server`, `dormant`, `ebi`, `enodeb-address`, `epdg-address`, `fa`, `fa-service`, `firewall`, `fw-and-nat`, `ggsn-service`, `gprs-service`, `gsm-traffic-class`, `gtp-version`, `gtpu-bind-address`, `gtpu-service`, `ha`, `ha-ipse-only`, `ha-service`, `hsgw-service`, `idle-time`, `imei`, `ims-auth-service`, `imsi`, `ip-address`, `ip-alloc-method`, `ip-pool`, `ipv6-prefix`, `13-tunnel-local-addr`, `13-tunnel-remote-addr`, `lac`, `lac-service`, `lma-service`, `lms`, `lms-service`, `long-duration-time-left`, `mag-service`, `mme-address`, `mme-service`, `msid`, `msisdn`, `nat`, `nemo-only`, `network-requested`, `pcf`, `pdg-service`, `pdif-service`, `pdsn-service`, `pgw-address`, `plmn-type`, `profile-id`, `profile-name`, `qci`, `rx-data`, `session-time-left`, `sgsn-address`, `sgsn-service`, `sgw-address`, `sgw-service`, `smgr-instance`, `tx-data`, `username`, `grep`, `more`

### asn-peer-address ip_address
Displays information for subscribers on an ASN-GW trusted peer.

The following filter keywords are valid with this command:

- `asn-peer-address`, `asngw-service`, `bearer-establishment`, `bng-service`, `callid`, `card-num`, `configured-idle-timeout`, `connected-time`, `ebi`, `enodeb-address`, `fa`, `fa-service`, `firewall`, `full`, `fw-and-nat`, `gtp-version`, `gtpu-bind-address`, `gtpu-service`, `ha`, `idle-time`, `ims-auth-service`, `imsi`, `ip-address`, `ip-alloc-method`, `ip-pool`, `ipv6-address`, `ipv6-prefix`, `13-tunnel-local-address`, `13-tunnel-remote-address`, `lac`, `lac-service`, `lma-service`, `lms`, `lms-service`, `long-duration-time-left`, `mipv6ha-service`, `msid`, `nat`, `network-type`, `profile-id`, `profile-name`, `qci`, `rx-data`, `slu-state`, `s5-proto`, `session-time-left`, `sgsn-address`, `sgsn-service`, `sgw-address`, `smgr-instance`, `tx-data`, `username`, `grep`, `more`
The following filter keywords are valid with this command:

- `aaa-configuration`, `access-flows`, `active`, `activity`, `all`, `asn-peer-address`, `asngw-service`, `bearer-establishment`, `bng-service`, `callid`, `card-num`, `configured-idle-timeout`, `connected-time`, `counters`, `data-rate`, `dormant`, `ebi`, `enodeb-address`, `fa`, `fa-service`, `firewall`, `full`, `fw-and-nat`, `gtp-version`, `gtp-bind-address`, `gtpu-service`, `ha`, `idle-time`, `ims-auth-service`, `insi`, `ip-address`, `ip-alloc-method`, `ip-pool`, `ipv6-address`, `ipv6-prefix`, `l3-tunnel-local-address`, `l3-tunnel-remote-address`, `long-duration-time-left`, `mipv6ha-service`, `msid`, `nat`, `network-type`, `policy`, `profile-id`, `profile-name`, `qci`, `rx-data`, `slu-state`, `s5-proto`, `session-time-left`, `sgw-address`, `smgr-instance`, `subscription`, `summary`, `tft`, `tx-data`, `username`, `wfl`, `grep`, `more`

### asngw-service service_name

Displays counters for subscribers accessing the ASN-GW service.

- `service_name` must be an existing service and be from 1 to 63 alphanumeric characters.

The following filter keywords are valid with this command:

- `asn-peer-address`, `asngw-service`, `bearer-establishment`, `bng-service`, `callid`, `card-num`, `configured-idle-timeout`, `connected-time`, `ebi`, `enodeb-address`, `fa`, `fa-service`, `firewall`, `full`, `fw-and-nat`, `gtp-version`, `gtpu-service`, `ha`, `idle-time`, `ims-auth-service`, `insi`, `ip-address`, `ip-alloc-method`, `ip-pool`, `ipv6-address`, `ipv6-prefix`, `l3-tunnel-local-address`, `l3-tunnel-remote-address`, `long-duration-time-left`, `mipv6ha-service`, `msid`, `nat`, `network-type`, `profile-id`, `profile-name`, `qci`, `rx-data`, `slu-state`, `s5-proto`, `session-time-left`, `sgw-address`, `smgr-instance`, `tx-data`, `username`, `grep`, `more`

### bandwidth-policy policy_name

Show information for subscribers associated with the specified Active Charging bandwidth policy. Must be followed by the name of an existing bandwidth policy specified as an alphanumeric string of 1 through 63 characters.

The following filter keywords are valid with this command:

- `access-type`, `active-charging-service`, `bandwidth-policy`, `bearer-establishment`, `bng-service`, `callid`, `card-num`, `cbb-policy`, `configured-idle-timeout`, `connected-time`, `cskf-service`, `domain`, `ebi`, `enodeb-address`, `epdg-address`, `fa`, `firewall`, `fw-and-nat`, `gtp-version`, `gtpu-bind-address`, `gtpu-service`, `ha`, `hnbgw-service`, `hsgw-service`, `idle-time`, `ims-auth-service`, `insi`, `ip-address`, `ip-alloc-method`, `ip-pool`, `ipv6-address`, `ipv6-prefix`, `l3-tunnel-local-addr`, `l3-tunnel-remote-addr`, `lma-service`, `long-duration-time-left`, `mag-service`, `mipv6ha-service`, `msid`, `nat`, `network-type`, `profile-id`, `profile-name`, `qci`, `rulebase`, `rx-data`, `slu-state`, `security-type`, `session-time-left`, `sgw-address`, `smgr-instance`, `tx-data`, `ue-type`, `username`, `grep`, `more`
bearer-establishment \{ direct-tunnel | normal | pending \}

Selects Bearer Establishment type defined by the specified filter keywords.

- **direct-tunnel**: Select subscribers having direct tunnel established with the Radio Network Controller (RNC).
- **normal**: Select subscribers having bearer established with SGSN.
- **pending**: Select subscribers for whom bearer is not fully established.

The following filter keywords are valid with this command:

apn, asn-peer-address, asngw-service, asnpc-service, bearer-establishment, bng-service, callid, card-num, ccoa-only, configured-idle-timeout, connected-time, css-delivery-sequence, css-service, dhcp-server, ebi, enodeb-address, epdg-address, fa, fa-service, firewall, fw-and-nat, ggsn-service, gprs-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipseck-only, ha-service, hsgw-service, idle-time, imei, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, 13-tunnel-local-addr, 13-tunnel-remote-addr, lac, lac-service, lma-service, lns, lns-service, long-duration-time-left, mag-service, mip-udp-tunnel-only, mipv6ha-service, mme-address, mme-service, msid, msisdnn, nat, nemo-only, network-requested, network-type, pcf, pdq-service, pdif-service, pdns-service, pgw-address, plmn-type, rx-data, sla-state, s5-proto, session-time-left, sgn-address, sgw-service, sgw-address, sgw-service, smgr-instance, tx-data, username, grep, more

bng-service srvc_name

Displays current configuration the specified Broadband Network Gateway (BNG) service. The following filter keywords are valid with this command:

active, all, apn, asn-peer-address, asngw-service, asnpc-service, bearer-establishment, bng-service, callid, card-num, ccoa-only, configured-idle-timeout, connected-time, dhcp-server, dormant, ebi, enodeb-address, epdg-address, fa, fa-service, firewall, fw-and-nat, ggsn-service, gprs-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipseck-only, ha-service, hsgw-service, idle-time, imei, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, 13-tunnel-local-addr, 13-tunnel-remote-addr, lac, lac-service, lma-service, lns, lns-service, long-duration-time-left, mag-service, mme-address, mme-service, msid, msisdnn, nat, nemo-only, network-requested, pcf, pdq-service, pdif-service, pdns-service, pgw-address, plmn-type, rx-data, sla-state, s5-proto, session-time-left, sgn-address, sgw-service, sgw-address, smgr-instance, tx-data, username, grep, more

callid id

Displays subscriber information for the call ID specified as an 8-byte hexadecimal number.

The following filter keywords are valid with this command:

apn, asn-peer-address, asngw-service, asnpc-service, bearer-establishment, bng-service, callid, card-num, ccoa-only, configured-idle-timeout, connected-time, css-delivery-sequence, css-service, dhcp-server,
ebi, enodeb-address, epdg-address, fa, fa-service, firewall, fw-and-nat, ggsn-service, gprs-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, hsgw-service, idle-time, imei, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, lac, lac-service, lma-service, lns, lns-service, long-duration-time-left, mag-service, mip-udp-tunnel-only, mipv6ha-service, mmee-address, mmee-service, msid, mxisdn, nat, nemo-only, network-requested, network-type, pcf, pdg-service, pdif-service, pdns-service, pgw-address, plmn-type, rx-data, slu-state, s5proto, session-time-left, sgsn-address, sgsn-service, sgw-address, SGW-service, smgr-instance, tx-data, username, grep, more

card-num card_num

The slot number of the processing card by which the subscriber session is processed. The slot number is an integer from 1 through 7 and 10 through 16 on the ASR 5000, or 1 through 4 and 7 through 10 on the ASR 5500.
The following filter keywords are valid with this command:

apn, asn-peer-address, asngw-service, asnpc-service, bearer-establishment, bng-service, callid, card-num, ccoa-only, configured-idle-timeout, connected-time, cpu-num, css-delivery-sequence, css-service, dhcp-server, ebi, enodeb-address, epdg-address, fa, fa-service, firewall, fw-and-nat, ggsn-service, gprs-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, hsgw-service, idle-time, imei, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, lac, lac-service, lma-service, lns, lns-service, long-duration-time-left, mag-service, mip-udp-tunnel-only, mipv6ha-service, mmee-address, mmee-service, msid, mxisdn, nat, nemo-only, network-requested, network-type, pcf, pdg-service, pdif-service, pdns-service, pgw-address, plmn-type, rx-data, slu-state, s5proto, session-time-left, sgsn-address, sgsn-service, sgw-address, SGW-service, smgr-instance, tx-data, username, grep, more

cbb-policy policy_name

Show information for subscribers associated with the specified Active Charging Content Based Billing (CBB) policy. Must be followed by the name of an existing Active Charging CBB policy specified as an alphanumeric string of 1 through 63 characters.
The following filter keywords are valid with this command:

active, active-charging -service, all, apn, bandwidth-policy, bearer-establishment, bng-service, callid, card-num, ccoa-only, configured-idle-timeout, connected-time, dhcp-server, dormant, ebi, enodeb-address, epdg-address, fa, fa-service, firewall, fw-and-nat, ggsn-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, hnbgw-only, hsgw-service, idle-time, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-address, l3-tunnel-remote-address, lac, lac-service, lma-service, lns, lns-service, long-duration-time-left, mag-service, mip-udp-tunnel-only, mipv6ha-service, msid, nemo-only
Exec Mode show Commands (Q-S)

```
network-requested, network-type, pcf, pdsn-service, plmn-type, profile-id, profile-name, qci, rx-data, slu-state, s5 Proto, session-time-left, sgsn-address, sgsn-service, tx-data, username, verbose, grep, more

ccoa-only
Displays current configuration for all MIP-HA subscribers that registered with a collocated COA only. The following filter keywords are valid with this command:

access-type, active-charging-service, bandwidth-policy, bearer-establishment, bng-service, callid, card-num, cbb-policy, configured-idle-timeout, connected-time, domain, ebi, enodeb-address, epdg-address, fa, firewall, fw-and-nat, gtp-version, gtpu-bind-address, gtpu-service, ha, hnbgw-service, idle-time, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, 13-tunnel-local-addr, 13-tunnel-remote-addr, long-duration-time-left, mipv6ha-service, msid, nat, network-type, pcc-service, profile-id, profile-name, qci, rulebase, rx-data, slu-state, s5-Proto, security-type, session-time-left, sgsn-address, sgsn-service, sgw-address, smgr-instance, tx-data, username, grep, more

configuration { all | username name }
Displays current configuration for all subscribers or a specified subscriber.

configured-idle-timeout [ < | > | greater-than | less-than ] value
Shows the idle timeout that is configured for the specified subscriber. A value of 0 (zero) indicates that the subscribers idle timeout is disabled.

• <: Filters output so that only information less than the specified value is displayed.
• >: Filters output so that only information greater than the specified value is displayed.
• greater-than: Filters output so that only information greater than the specified value is displayed.
• less-than: Filters output so that only information less than the specified value is displayed.
• value: Used in conjunction with <, >, greater-than, less-than, If no other filtering options are specified only output matching value is displayed. If value is not specified all data is displayed. value must be an integer from 0 through 4294967295.

congestion_mgmt { not-required | required }
Shows the current subscribers for which congestion management is not-required or required. The following filter keywords are valid with this command:

active-charging-service, apn, asn-peer-address, asngw-service, asnpo-service, bandwidth-policy, bearer-establishment, bng-service, callid, card-num, cbb-policy, configured-idle-timeout, congestion_mgmt, connected-time, ebi, enodeb-address, epdg-address, fa, fa-service, firewall, fw-and-nat, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, hnbgw-service, hsgw-service, idle-time, ims-auth-service, imsi, interface-type, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, 13-tunnel-local-addr, 13-tunnel-remote-addr, lac-service, lma-service, lns, lns-service, long-duration-time-left, mag-service, mipv6ha-service, mme-address, mme-service, msid, nat, network-type, pcp, pgw-address, plmn-type, profile-id, profile-name, qci, rulebase, rx-data, slu-state, s5-Proto, saegw-service, session-time-left, sgw-address, sgw-service, smgr-instance, tx-data, username, wsg-service
```
show subscribers

connected-time [ < | > | greater-than | less-than ] value

Shows how long the subscriber has been connected.
- <: Filters output so that only information less than the specified value is displayed.
- <=: Filters output so that only information less than or equal to the specified value is displayed.
- >=: Filters output so that only information greater than or equal to the specified value is displayed.
- greater-than: Filters output so that only information greater than the specified value is displayed.
- less-than: Filters output so that only information less than the specified value is displayed.

value: Used in conjunction with <, >, greater-than, less-than. If no other filtering options are specified, only output matching value is displayed. If value is not specified, all data is displayed. value must be an integer from 0 through 4294967295.

counters

Shows the counters associated with the subscriber. The following filter keywords are valid with this command:

access-type, active, active-charging-service, all, apn, asn-peer-address, asngw-service, asnpc-service, bandwidth-policy, bearer-establishment, bng-service, callid, card-num, cbb-policy, ccoa-only, configured-idle-timeout, connected-time, cscf-service, dhcp-server, dns-proxy, domain, dormant, ebi, enodeb-address, epdg-address, fa, fa-service, firewall, fw-and-nat, ggsn-service, gprs-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, hnbgw-service, hsgw-service, idle-time, imei, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, lac, lac-service, lma-service, lns, lns-service, long-duration-time-left, mag-service, mipv6a-service, mme-address, mme-service, msd, msisdn, nat, nemo-only, network-requested, network-type, pcc-service, pcf, pdg-service, pdsn-service, pgw-address, plmn-type, profile-id, profile-name, qci, rulebase, rx-data, slu-state, s5-proto, security-type, session-time-left, sgsn-address, sgw-service, session-time-left, smgr-instance, tx-data, ue-type, username, grep, more

cscf-only

Displays information for Call Session Control Function (CSCF) subscribers only.
The following filter keywords are valid with this command:

aaa-configuration, access-flows, active, activity, all, bearer-establishment, callid, card-num, configured-idle-timeout, connected-time, counters, cscf-service, data-rate, dormant, fa, full, gtp-version, ha, idle-time, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, long-duration-time-left, mipv6a-service, msd, network-type, policy, rx-data, session-time-left, smgr-instance, subscription, summary, tft, tx-data, username, wfl
**cscf-service service_name**

Displays information for subscribers accessing the specified CSCF service.

*service_name* must be an existing service expressed as an alphanumeric string of 1 through 63 characters. The following filter keywords are valid with this command:

- bearer-establishment
- callid
- card-num
- configured-idle-timeout
- connected-time
- cscf-service
- fa
- gtp-version
- ha
- idle-time
- ims-auth-service
- imsi
- ip-address
- ip-alloc-method
- ip-pool
- ipv6-address
- ipv6-prefix
- 13-tunnel-local-addr
- 13-tunnel-remote-addr
- long-duration-time-left
- mipv6ha-service
- msid
- network-type
- rx-data
- session-time-left
- smgr-instance
- subscription
- tx-data
- username

**css-delivery-sequence**

*Important:* This is a restricted keyword. In StarOS 9.0 and later, this keyword is obsoleted.

**cscf-service csssvc_name**

*Important:* This is a restricted keyword. In StarOS 9.0 and later releases, this keyword is obsolete.

**data-rate**

Displays subscriber throughput data. This keyword is best used for individual subscriber output. The following filter keywords are valid with this command:

- access-type
- active
- active-charging-service
- all
- apn
- asn-peer-address
- asngw-service
- asspc-service
- bandwidth-policy
- bearer-establishment
- bng-service
- callid
- card-num
- cbb-policy
- ccoa-only
- configured-idle-timeout
- connected-time
- cscf-service
- dhcp-server
- domain
- dormant
- ebi
- enodeb-address
- epdg-address
- fa
- fa-service
- firewall
- fw-and-nat
- ggsn-service
- gprs-service
- graph
- gsm-traffic-class
- gtp-version
- gtpu-bind-address
- gtpu-service
- ha
- ipsec-only
- ha-service
- high
- hnbgw-service
- hsgw-only
- hsgw-service
- idle-time
- imei
- ims-auth-service
- imsi
- ip-address
- ip-alloc-method
- ip-pool
- ipv6-address
- ipv6-prefix
- 13-tunnel-local-addr
- 13-tunnel-remote-addr
- lac
- lac-service
- lma-service
- lns
- lns-service
- long-duration-time-left
- low
- mag-service
- mipv6ha-service
- mme-address
- mme-service
- msid
- msisdn
- network-requested
- network-type
- pcc-service
- pcf
- pdg-service
- pdif-service
- pdsm-service
- pgw-address
- pmln-type
- profile-id
- profile-name
- qci
- rulebase
- rx-data
- slu-state
- s5-proto
- security-type
- session-time-left
- sgsn-address
- sgsn-service
- pgw-address
- pgw-service
- smgr-instance
- summary
- tx-data
- ue-type
- username
- verbose
- grep
- more

**debug-info { callid id | msid id | username name }**

Displays internal call troubleshooting information for subscriber sessions defined by the specified keywords. *callid id:* Displays subscriber information for the call specified by *id*. The call ID must be specified as an 8-digit hexadecimal number.
• **msid id**: Displays information for the mobile user identified by `id`. `id` must be from 7 to 16 digits specified as an IMSI, MIN, or RMI. Wildcard characters $ and * are allowed. The * wildcard matches multiple characters and the $ wildcard matches a single character. If you do not want the wildcard characters interpreted as a wildcard enclose them in single quotes (‘‘). For example; ‘$’.

• **username name**: Displays information for connections for the subscriber identified by `name`. The user must have been previously configured. `name` must be a sequence of characters and/or wildcard characters (‘$’ and ‘*’) from 1 to 127 characters. The * wildcard matches multiple characters and the $ wildcard matches a single character. If you do not want the wildcard characters interpreted as wildcard enclose them in single quotes (‘‘). For example; ‘$’.

### dhcp-server `ipv4_address`
Displays subscribers based on a specific DHCP server where their IP address was allocated. Must be followed by IP address of the server, using IPv4 dotted-decimal notation.
The following filter keywords are valid with this command:

```
apn, bearer-establishment, bng-service, callid, card-num, ccoa-only, configured-idle-timeout, connected-time, dhcp-server, ebi, epdg-address, fa, fa-service, firewall, fw-and-nat, ggsn-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipse-only, ha-service, idle-time, imei, ims-auth-service, imsi, ip-address, ip-pool, ipv6-address, ipv6-prefix, 13-tunnel-local-addr, 13-tunnel-remote-addr, lac, lac-service, lns, lns-service, long-duration-time-left, msid, misdn, nat, nemo-only, network-requested, pcf, pdsn-service, plmn-type, profile-id, profile-name, qci, rx-data, slu-state, session-time-left, sgsn-address, sgsn-service, smgr-instance, tx-data, username, grep, more
```

### domain `name`
Displays all subscribers with an Address-of-Record (AoR) from the specified domain. `name` is an alphanumeric string of 1 through 79 characters.
The following filter keywords are valid with this command:

```
access-type, active-charging-service, all, apn, asn-peer-address, asngw-service, asnp-service, bandwidth-policy, bearer-establishment, bng-service, callid, card-num, ccb-policy, configured-idle-timeout, connected-time, csnof-service, dhcp-server, domain, ebi, enodeb-address, fa, firewall, fw-and-nat, ggsn-service, graph, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, hnbgw-service, hsgw-only, hsgw-service, idle-time, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, 13-tunnel-local-addr, 13-tunnel-remote-addr, long-duration-time-left, mipv6ha-service, msid, network-type, pcc-service, profile-id, profile-name, qci, rulebase, rx-data, slu-state, s5,proto, security-type, session-time-left, sgw-address, smgr-instance, summary, tx-data, ue-type, username, grep, more
```

### dormant `number`
Displays all dormant subscribers, those registered but not transmitting/receiving data.
The following filter keywords are valid with this command:

---

Cisco ASR 5x00 Command Line Interface Reference
access-type, active-charging-service, apn, asn-peer-address, asn-gw-service, asnp-c-service, bandwidth-policy, bearer-establishment, bng-service, call-id, card-num, ccb-policy, ccoa-only, configured-idle-timeout, connected-time, dhcp-server, domain, ebi, enodeb-address, epdg-address, fa, fa-service, firewall, fw-and-nat, ggsn-service, gprs-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, hnb-gw-service, hsgw-service, idle-time, imei, ima-auth-service, imsi, ip-address, ip-pool, ipv6-address, ipv6-prefix, 13-tunnel-local-addr, 13-tunnel-remote-addr, lac, lac-service, lma-service, lns, lns-service, long-duration-time-left, mag-service, mip-udp-tunnel-only, mipv6ha-service, mme-address, mme-service, msid, msisdn, nat, nemo-only, network-requested, network-type, pcc-service, pcf, ppg-service, pdif-service, pdsm-service, pgw-address, plmn-type, profile-id, profile-name, qci, rulebase, rx-data, sla-state, security-type, session-time-left, sgw-service, smgr-service, sgw-address, sgw-service, smgr-instance, tx-data, ue-type, username, grep, more

**ebi number**

Displays subscribers based on an EPS bearer identity. *number* specifies the EBI number and must be an integer value from 5 to 15.

The following filter keywords are valid with this command:

access-type, active-charging-service, apn, asn-peer-address, asn-gw-service, asnp-c-service, bandwidth-policy, bearer-establishment, bng-service, call-id, card-num, ccb-policy, ccoa-only, configured-idle-timeout, connected-time, dhcp-server, domain, ebi, enodeb-address, epdg-address, fa, fa-service, firewall, fw-and-nat, ggsn-service, gprs-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, hnb-gw-service, hsgw-service, idle-time, imei, ima-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, 13-tunnel-local-addr, 13-tunnel-remote-addr, lac, lac-service, lma-service, lns, lns-service, long-duration-time-left, mag-service, mipv6ha-service, mme-address, mme-service, msid, msisdn, nat, nemo-only, network-requested, network-type, pcc-service, pcf, ppg-service, pdif-service, pdsm-service, pgw-address, plmn-type, profile-id, profile-name, qci, rulebase, rx-data, sla-state, s5-ctrl-service, session-time-left, sgw-service, smgr-instance, tx-data, ue-type, username, grep, more

**enodeb-address ip_address**

Displays subscribers based on the eNodeB to which they are attached. *ip_address* must be a valid IP address of an existing eNodeB specified in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

The following filter keywords are valid with this command:

access-type, active-charging-service, apn, asn-peer-address, asn-gw-service, asnp-c-service, bandwidth-policy, bearer-establishment, bng-service, call-id, card-num, ccb-policy, ccoa-only, configured-idle-timeout, connected-time, dhcp-server, domain, ebi, enodeb-address, epdg-address, fa, fa-service, firewall, fw-and-nat, ggsn-service, gprs-
The following filter keywords are valid with this command:

- apn, bearer-establishment, bng-service, callid, card-num, ccoa-only, configured-idle-timeout, connected-time, dhcp-server, ebi, enodeb-address, epdg-address, fa, fa-service, firewall, fw-and-nat, ggsn-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsecc-only, ha-service, hnbgw-service, hsgw-service, idle-time, imei, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, lac, lac-service, lma-service, lns, lns-service, long-duration-time-left, mag-service, mme-address, mme-service, msid, msisdn, nat, nemo-only, network-requested, network-type, pcc-service, pcf, pdg-service, pdif-service, pdsn-service, pgw-address, plmn-type, profile-id, profile-name, qci, rx-data, slu-state, s5-proto, session-time-left, sgsn-address, sgw-address, sgw-service, smgr-instance, tx-data, ue-type, username, grep, more

**epdg-address ipv4_ipv6_address**

Displays subscribers connected to the specified ePDG peer specified in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

The following filter keywords are valid with this command:

- apn, bearer-establishment, bng-service, callid, card-num, ccoa-only, configured-idle-timeout, connected-time, dhcp-server, ebi, enodeb-address, epdg-address, fa, fa-service, firewall, fw-and-nat, ggsn-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsecc-only, ha-service, idle-time, imei, ims-auth-service, imsi, interface-type, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, lac, lac-service, lns, lns-service, long-duration-time-left, mip-udp-tunnel-only, mipv6ha-service, mme-address, mme-service, msid, msisdn, nat, nemo-only, network-requested, network-type, pcf, pdg-service, pdif-service, pdsn-service, pgw-address, plmn-type, profile-id, profile-name, qci, rx-data, slu-state, s5-proto, session-time-left, sgsn-address, sgw-address, sgw-service, smgr-instance, tx-data, username, wsg-service, grep, more

**fa ipv4_address**

Displays subscribers for a specified Peer Foreign Agent. Must be followed by the IP address of a Remote FA, in IPv4 dotted-decimal notation.

The following filter keywords are valid with this command:

- access-type, active-charging-service, apn, asn-peer-address, asngw-service, asnp-center-service, bandwidth-policy, bearer-establishment, bng-service, callid, card-num, ccb-policy, ccoa-only, configured-idle-timeout, connected-time, csf-service, dhcp-server, domain, ebi, enodeb-address, epdg-address, fa, fa-service, firewall, fw-and-nat, ggsn-service, gprs-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsecc-only, ha-service, hnbgw-service, hsgw-service, idle-time, imei, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, lac, lac-service, lma-service, lns, lns-service, long-duration-time-left, mag-service, mipv6ha-service, mme-address, mme-service, msid, msisdn, nat, nemo-only, network-requested, network-type, pcc-service, pcf, pdg-service, pdif-service, pdsn-service, pgw-address, plmn-type, profile-id, profile-name, qci, rulebase, rx-data, slu-state, s5-proto, security-type, session-time-left, sgsn-address,
show subscribers

sgsn-service, sgw-address, sgw-service, smgr-instance, tx-data, ue-type, username, grep, more

epdg-only
Displays epdg-specific context information for the session.
The following filter keywords are valid with this command:

all, callid, card-num, configured-idle-timeout, connected-time, counters, data-rate, full, gtp-version, gtpu-bind-address, gtpu-service, idle-time, ip-address, ipv6-prefix, long-duration-time-left, network-type, qci, rx-data, session-time-left, smgr-instance, summary, tft, tx-data, username, grep, more

epdg-service srvc_name
Displays subscribers for a specified Evolved Packet Data Gateway service. Must be followed by ePDG service name expressed as an alphanumerical string of 1 through 63 characters.
The following filter keywords are valid with this command:

all, callid, card-num, configured-idle-timeout, connected-time, counters, data-rate, epdg-address, full, gtp-version, gtpu-bind-address, gtpu-service, idle-time, ip-address, ipv6-prefix, long-duration-time-left, network-type, qci, rx-data, session-time-left, smgr-instance, summary, tft, tx-data, username, grep, more

fa-only
Displays FA-specific context information for the session.
The following filter keywords are valid with this command:

aaa-configuration, access-flows, active, activity, all, asn-peergaddress, asngw-service, asnpc-service, bearer-establishment, callid, card-num, configured-idle-timeout, connected-time, counters, csccf-service, data-rate, dhcp-server, dormant, ebi, enodeb-address, epdg-address, fa, fa-service, firewall, full, fwand-nat, ggsn-service, gsm-traffic-class, gtp-version, gtpu-bindaddress, gtpu-service, ha, ha-ipsec-only, ha-service, idle-time, imei, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, 13-tunnel-local-addr, 13-tunnelremote-addr, lac, lac-service, long-duration-time-left, mag-service, mip-udp-tunnel-only, mipv6ha-service, msid, msisdn, nat, nemo-only, network-requested, network-type, pcf, pdif-service, pdns-service, pgw-address, plmn-type, policy, profile-id, profile-name, qci, rx-data, slu-state, s5proto, session-time-left, sgw-address, sgw-service, smgr-instance, subscription, summary, tft, tx-data, username, wfl, grep, more

fa-service srvc_name
Displays subscribers for a specified Foreign Agent service. Must be followed by FA service name expressed as an alphanumerical string of 1 through 63 characters.
The following filter keywords are valid with this command:
aaa-configuration, access-flows, active, activity, all, asn-peer-address, asngw-service, asnpc-service, bearer-establishment, bng-service, callid, card-num, ccoa-only, configuration, configured-idle-timeout, connected-time, counters, csclf-service, data-rate, debug-info, dhcp-server, dormant, ebi, enodeb-address, epdg-address, fa, fa-only, fa-service, firewall, full, fw-and-nat, ggsn-only, ggsn-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, idle-time, imei, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, lac, lac-only, lac-service, lns, lns-only, long-duration-time-left, mag-service, mip-udp-tunnel-only, mipv6ha-only, mipv6ha-service, msid, msisdn, nat, nemo-only, network-requested, network-type, pcf, pdif-service, pdsm-service, pgw-address, plmn-type, policy, profile-id, profile-name, qci, rx-data, slu-state, s5-proto, session-time-left, sgsn-address, sgw-address, sgw-service, smgr-instance, subscription, summary, tft, tx-data, username, wfi, grep, more

firewall { not-required | required }
Displays information for subscribers based on whether or not firewall processing is required.
The following filter keywords are valid with this command:
apn, asn-peer-address, asngw-service, asnpc-service, bearer-establishment, bng-service, callid, card-num, ccoa-only, configured-idle-timeout, connected-time, dhcp-server, ebi, epdg-address, fa, fa-service, firewall, fw-and-nat, ggsn-service, gprs-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, hsgw-service, idle-time, imei, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv4, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, lac, lac-service, lma-service, lns, lns-service, long-duration-time-left, mag-service, mme-service, mme-service, msid, msisdn, nat, nemo-only, network-requested, network-type, pcf, pdg-service, pdif-service, pdsm-service, pgw-address, plmn-type, policy, profile-id, profile-name, qci, rx-data, slu-state, s5-proto, session-time-left, sgsn-address, sgw-address, sgw-service, smgr-instance, tx-data, username, grep, more

fng-only
Displays Femto Network Gateway (FNG) context information for the session.
The following filter keywords are valid with this command:

aaa-configuration, access-flows, active, activity, all, bearer-establishment, bng-service, callid, card-num, configured-idle-timeout, connected-time, counters, data-rate, dormant, ebi, enodeb-address, epdg-address, fa, fa-service, firewall, fng-service, full, fw-and-nat, gtp-version, gtpu-bind-address, gtpu-service, ha, idle-time, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, long-duration-time-left, mipv6ha-service, msid, nat, network-type, pdif-service, policy, profile-id, profile-name, qci, rx-data, slu-state, s5-proto, session-
time-left, sgw-address, smgr-instance, subscription, summary, tft, tx-data, username, wfl, grep, more

**fng-service srvc_name**

Displays information for subscribers accessing the specified FNG service.  
*service_name* must be an existing service expressed as an alphanumeric string of 1 through 63 characters.  
The following filter keywords are valid with this command:

- bearer-establishment, bng-service, callid, card-num, configured-idle-timeout, connected-time, ebi, enodeb-address, epdg-address, fa, fa-service, firewall, fng-service, full, fw-and-nat, gtp-version, gtpu-bind-address, gtpu-service, ha, idle-time, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, long-duration-time-left, mipv6ha-service, msid, nat, network-type, pdif-service, profile-id, profile-name, qci, rx-data, session-time-left, sgw-address, smgr-instance, subscription, summary, tft, tx-data, username, grep, more

**full**

Shows all available subscriber information. The following filter keywords are valid with this command:

- access-type, active, active-charging-service, all, apn, asn-peer-address, asngw-service, asnpc-service, bandwidth-policy, bearer-establishment, bng-service, callid, card-num, cbb-policy, ccoa-only, configured-idle-timeout, connected-time, csfcservice, dhcp-server, domain, dormant, ebi, enodeb-address, epdg-address, fa, fa-service, firewall, fw-and-nat, ggsn-service, gprs-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, hnbgw-service, hsgw-service, idle-time, imei, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, lac, lac-service, lns, ins-service, long-duration-time-left, mag-service, mip-udp-tunnel-only, mipv6ha-service, mme-address, mme-service, msid, network-requested, network-type, pcc-service, pcf, pdg-service, pdif-service, pdns-service, pgw-address, plmn-type, profile-id, profile-name, qci, rulebase, rx-data, slu-state, sl-proto, security-type, session-time-left, sgsn-address, sgsn-service, sgw-address, sgw-service, smgr-instance, tx-data, ue-type, username, grep, more

**fw-and-nat policy fw_nat_policy**

**Important:** This option is customer-specific and is only available in StarOS 8.1.

Displays information for subscribers using an existing Firewall-and-NAT policy specified as an alphanumeric string of 1 through 15 characters.

**ggsn-only**

Displays only GGSN-specific subscriber context information.  
The following filter keywords are valid with this command:
aaa-configuration, access-flows, active, activity, all, apn,
bearer-establishment, bng-service, callid, card-num, ccoa-only,
configured-idle-timeout, connected-time, counters, csinfo-service,
data-rate, dhcp-server, dormant, ebi, enodeb-address, epdg-
address, fa, fa-service, firewall, full, fw-and-nat, ggsn-service,
gprs-service, gsm-traffic-class, gtp-version, gtpu-bind-address,
gtpu-service, ha, ha-ipse-only, ha-service, idle-time, imei, ims-
auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-
address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr,
lac, lac-service, lns-service, lns, lns-only, long-duration-time-
left, mip-udp-tunnel-only, mipv6ha-service, msid, msisdn, nat,
nemo-only, network-requested, network-type, pcf, pdsn-service,
plmn-type, policy, profile-id, profile-name, qci, rx-data, slu-
state, s5-proto, session-time-left, sgsn-address, sgw-address,
smgr-instance, subscription, summary, tft, tx-data, username, wfl,
grep, more

ggsn-service srvc_name
Displays only subscribers for a specified GGSN service. Must be followed by the GGSN service name
expressed as an alphanumeric string of 1 through 63 characters.
The following filter keywords are valid with this command:

apn, bearer-establishment, bng-service, callid, card-num, ccoa-only,
configured-idle-timeout, connected-time, dhcp-server, dormant, ebi,
enodeb-address, epdg-address, fa, fa-service, firewall, fw-and-nat,
ggsn-service, gsm-traffic-class, gtp-version, gtpu-bind-address,
gtpu-service, ha, ha-ipse-only, ha-service, idle-time, imei, ip-address,
ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr,
l3-tunnel-remote-addr, lac, lac-service, lns-service, lns, lns-only, long-duration-time-
left, mip-udp-tunnel-only, mipv6ha-service, msid, msisdn, nat, nemo-
only, network-requested, network-type, pcf, pdsn-service, plmn-type,
policy, profile-id, profile-name, qci, rx-data, slu-state, s5-proto, session-
time-left, sgsn-address, sgw-address, smgr-instance, tx-data, username,
grep, more

gsm-traffic-class { background | conversational | interactive }
Displays subscribers associate with the specified 3GPP QoS traffic class.
The following filter keywords are valid with this keyword:

apn, bearer-establishment, bng-service, callid, card-num, ccoa-only,
configured-idle-timeout, connected-time, dhcp-server, ebi, enodeb-
address, epdg-address, fa, fa-service, firewall, fw-and-nat, ggsn-
service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service,
ha, ha-ipse-only, ha-service, idle-time, imei, ims-auth-service, imsi,
ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-
tunnel-local-addr, l3-tunnel-remote-addr, lac, lac-service, lns, lns-
service, long-duration-time-left, mip-udp-tunnel-only, mipv6ha-service,
msid, msisdn, nat, nemo-only, network-requested, network-type, pcf, pdsn-
service, plmn-type, profile-id, profile-name, qci, rx-data, slu-state,
s5-proto, session-time-left, sgsn-address, sgw-address, smgr-instance,
tx-data, username, grep, more
The following filter keywords are valid with this command:

aaa-configuration, active, active-charging-service, activity, all, apn, callid, card-num, configured-idle-timeout, connected-time, counters, data-rate, full, ggsn-address, gprs-service, gsm-traffic-class, idle-time, imsi, msid, msisdn, partial, plmn-type, profile-name, rx-data, session-time-left, summary, tx-data, wide-format, grep, more

gprs-service srvc_name

Enter the name of the configured 2G GPRS service to display subscriber information specific to the named GPRS service for the SGSN.
srvc_name must be an alphanumeric string of 1 through 63 characters that identifies a configured GPRS service.
The following filter keywords are valid with this command:

apn, bearer-establishment, bng-service, callid, card-num, ccoa-only, configured-idle-timeout, connected-time, dhcp-server, dormant, ebi, enodeb-address, epdg-address, fa, fa-service, firewall, fw-and-nat, ggsn-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, idle-time, imei, ip-address, ip-pool, ipv6-address, ipv6-prefix, 13-tunnel-local-addr, 13-tunnel-remote-addr, lac, lac-service, lns, lns-service, long-duration-time-left, mipv6-prefix, mipv6-data, mipv6-ha-service, msid, msisdn, nat, nemo-only, network-requested, network-type, pcf, pdns-service, plmn-type, profile-id, profile-name, qci, rx-data, sla-state, s5-proto, session-time-left, sgsn-address, sgw-address, smgr-instance, tx-data, username, grep, more

gsm-traffic-class { background | conversational | interactive | streaming }

Displays information for subscriber traffic that matches the specified 3GPP traffic class.

• **background**: 3GPP QoS background class.
• **conversational**: 3GPP QoS conversational class.
• **interactive**: 3GPP QoS interactive class. Must be followed by a traffic priority.
• **streaming**: 3GPP QoS streaming class.
The following filter keywords are valid with this command:

apn, bearer-establishment, bng-service, callid, card-num, ccoa-only, configured-idle-timeout, connected-time, dhcp-server, ebi, enodeb-address, epdg-address, fa, fa-service, firewall, fw-and-nat, ggsn-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, idle-time, imei, ims-auth-service, ip-pool, ipv6-address, ipv6-prefix, 13-tunnel-local-addr, 13-tunnel-remote-addr, lac, lac-service, lns, lns-service, long-duration-time-left, mipv6-data, mipv6-ha-service, msid, msisdn, nat, nemo-only, network-requested, network-type, pcf, pdns-service, plmn-type, profile-id, profile-name,
qci, rx-data, slu-state, s5-proto, session-time-left, sgsn-address, sgsn-service, sgw-address, smgr-instance, tx-data, username, grep, more

gtp-version  { 0 | 1 }
Displays the specific GTP version number. Must be followed by one of the supported GTP versions (0 or 1). The following filter keywords are valid with this command:

apn, bearer-establishment, bng-service, callid, card-num, configured-idle-timeout, connected-time, ebi, enodeb-address, epdg-address, fa, firewall, fw-and-nat, gprs-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, hsgw-service, idle-time, imei, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, long-duration-time-left, mag-service, mipv6ha-service, msid, misdn, nat, network-type, nri, nsei, pdg-service, pdif-service, plmn-type, profile-id, profile-name, qci, rx-data, slu-state, s5-proto, session-time-left, sgsn-service, sgw-address, smgr-instance, tx-data, username, grep, more

gtpu-bind-address  ipv4_address
Displays the subscribers associated with the specified GTPU service bind address. Must be followed by an IPv4 address in dotted decimal notation. The following filter keywords are valid with this command:

access-type, active-charging-service, apn, asn-peer-address, asngw-service, asnpc-service, bandwidth-policy, bearer-establishment, bng-service, callid, card-num, ccb-policy, ccoa-only, configured-idle-timeout, connected-time, cscf-service, dhcp-server, domain, ebi, enodeb-address, epdg-address, fa, fa-service, firewall, fw-and-nat, ggsn-service, gprs-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-mipsec-only, ha-service, hnbgw-service, hsgw-service, idle-time, imei, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, lac, lac-service, lma-service, lns, ins-service, long-duration-time-left, mag-service, mip-udp-tunnel-only, mipv6ha-service, mme-address, mme-service, msid, msisdn, nat, nemo-only, network-requested, network-type, pcc-service, pcf, pdg-service, pdif-service, pdns-service, pgw-address, plmn-type, profile-id, profile-name, qci, rulebase, rx-data, slu-state, s5-proto, security-type, session-time-left, sgsn-address, sgw-address, gtpu-service, smgr-instance, tx-data, ue-type, username, grep, more

gtpu-service  svc_name
Displays the subscribers associated with an existing GTPU service specified as an alphanumeric string of 1 through 63 characters. The following filter keywords are valid with this command:

access-type, active-charging-service, apn, asn-peer-address, asngw-service, asnpc-service, bandwidth-policy, bearer-establishment, bng-service, callid, card-num, ccb-policy, ccoa-only, configured-idle-timeout, connected-time, cscf-service, dhcp-server, domain, ebi, enodeb-address, epdg-address, fa, fa-service, firewall, fw-and-nat, ggsn-service, gprs-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, hsgw-service, id, id, profile, pcc-service, pcf, pdg-service, pdif-service, pdns-service, pgw-address, plmn-type, profile-id, profile-name, qci, rulebase, rx-data, slu-state, s5-proto, security-type, session-time-left, sgsn-address, sgw-address, gtpu-service, smgr-instance, tx-data, ue-type, username, grep, more
service, gprs-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, hnbgw-service, hsgw-service, idle-time, imei, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, 13-tunnel-local-addr, 13-tunnel-remote-addr, lac, lac-service, lma-service, lns, lns-service, long-duration-time-left, mag-service, mip-udp-tunnel-only, mipv6ha-service, mme-service, mme-service, msid, msisdn, nat, nemo-only, network-requested, network-type, pcc-service, pf, pdg-service, pdif-service, pdsn-service, pgw-address, plmn-type, profile-id, profile-name, qci, rulebase, rx-data, slu-state, s5proto, security-type, session-time-left, sgsn-address, sgw-address, sgw-service, smgr-instance, tx-data, ue-type, username, grep, more

ha ipv4_address

Displays the subscribers associated with the specified Peer Home Agent. Must be followed by the IP address of a Remote HA in IPv4 dotted-decimal notation.

The following filter keywords are valid with this command:

access-type, active-charging-service, apn, asn-peer-address, asngw-service, asngw-service, bandwidth-policy, bearer-establishment, bng-service, callid, card-num, cbb-policy, ccoa-only, configured-idle-timeout, connected-time, csf-service, dhcp-server, domain, ebi, enodeb-address, epdg-address, fa, fa-service, firewall, fw-and-nat, ggsn-service, gprs-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, hnbgw-service, hsgw-service, idle-time, imei, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, 13-tunnel-local-addr, 13-tunnel-remote-addr, lac, lac-service, lma-service, lns, lns-service, long-duration-time-left, mag-services, mip-udp-tunnel-only, mipv6ha-service, mme-address, mme-service, msid, msisdn, nat, nemo-only, network-requested, network-type, pcc-service, pf, pdg-service, pdif-service, pdsn-service, pgw-address, plmn-type, profile-id, profile-name, qci, rulebase, rx-data, slu-state, s5proto, security-type, session-time-left, sgsn-address, sgw-address, sgw-service, smgr-instance, tx-data, ue-type, username, grep, more

ha-ipsec-only

Displays MIPHA subscribers with subscriber IPSec tunnel only.

The following filter keywords are valid with this command:

apn, bearer-establishment, bng-service, callid, card-num, ccoa-only, configured-idle-timeout, connected-time, dhcp-server, ebi, enodeb-address, epdg-address, fa, fa-service, firewall, fw-and-nat, ggsn-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, idle-time, imei, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, 13-tunnel-local-addr, 13-tunnel-remote-addr, lac, lac-service, lns, lns-service, long-duration-time-left, mip-udp-tunnel-only, mipv6ha-service, msid, msisdn, nat, nemo-only, network-requested, network-type, pf, pdg-service, pdif-service, plmn-type, profile-id, profile-name, qci, rx-data, slu-state,
The following filters/keywords are valid with this command:

- `apn`, `bearer-establishment`, `bng-service`, `callid`, `card-num`, `ccco-only`,
- `configured-idle-timeout`, `connected-time`, `dhcp-server`, `ebi`, `enodeb-address`, `epdg-address`, `fa`, `fa-service`, `firewall`, `fw-and-nat`, `ggsn-service`, `gsm-traffic-class`, `gtp-version`, `gtpu-bind-address`, `gtpu-service`,
- `ha`, `ha-ipsec-only`, `ha-service`, `idle-time`, `imei`, `ims-auth-service`, `imsi`,
- `ip-address`, `ip-alloc-method`, `ip-pool`, `ipv6-address`, `ipv6-prefix`, `tunnel-local-addr`, `tunnel-remote-addr`, `l3-tunnel-local-addr`, `l3-tunnel-remote-addr`, `l4`, `l4-service`, `l3`, `l5-service`,
- `long-duration-time-left`, `mip-udp-tunnel-only`, `mipv6ha-service`,
- `msid`, `msisdn`, `nat`, `nemo-only`, `network-requested`, `network-type`, `pcf`, `pdns-service`,
- `plmn-name`, `profile-id`, `profile-name`, `qci`, `rx-data`, `slu-state`,
- `s5-proto`, `session-time-left`, `sgsn-address`, `sgw-address`, `smgr-instance`,
- `tx-data`, `username`, `grep`, `more`

### ha-service `svc_name`

Displays the subscribers associated with an existing Home Agent service specified as an alphanumeric string of 1 through 63 characters.

The following filter keywords are valid with this command:

- `aaa-configuration`, `access-flows`, `access-type`, `active`, `active-charging-service`,
- `activity`, `bandwidth-policy`, `bearer-establishment`, `bng-service`, `callid`, `card-num`, `cbb-policy`,
- `configured-idle-timeout`, `connected-time`, `csf-service`,
- `data-rate`, `domain`, `ebi`, `enodeb-address`, `epdg-address`, `fa`, `firewall`, `full`, `fw-and-nat`,
- `gtp-version`, `gtpu-bind-address`, `gtpu-service`, `ha`, `hnbgw-service`,
- `idle-time`, `ims-auth-service`, `imsi`, `ip-address`, `ip-alloc-method`, `ip-pool`, `ipv6-address`,
- `ipv6-prefix`, `l3-tunnel-local-addr`, `l3-tunnel-remote-addr`, `l4`, `l4-service`,
- `l3`, `l5-service`, `long-duration-time-left`, `mipv6ha-service`,
- `msid`, `msisdn`, `nat`, `nemo-only`, `network-requested`, `network-type`, `pcf`,
- `pdns-service`, `plmn-name`, `profile-id`, `profile-name`, `qci`, `rx-data`, `slu-state`,
- `s5-proto`, `session-time-left`, `sgsn-address`, `sgw-address`, `smgr-instance`,
- `tx-data`, `username`, `grep`, `more`

### hnbgw-only

Displays HNB-GW subscriber session information.

The following filters/keywords are valid with this command:

- `aaa-configuration`, `access-flows`, `access-type`, `active`, `active-charging-service`,
- `activity`, `bandwidth-policy`, `bearer-establishment`, `bng-service`,
- `callid`, `card-num`, `cbb-policy`, `configured-idle-timeout`, `connected-time`,
- `counters`, `csf-service`, `data-rate`, `domain`, `ebi`, `enodeb-address`, `epdg-address`,
- `fa`, `firewall`, `full`, `fw-and-nat`, `gtp-version`, `gtpu-bind-address`,
- `gtpu-service`, `ha`, `hnbgw-service`, `idle-time`, `ims-auth-service`, `imsi`, `ip-address`,
- `ip-alloc-method`, `ip-pool`, `ipv6-address`, `ipv6-prefix`, `l3-tunnel-local-addr`, `l3-tunnel-remote-addr`, `l4`, `l4-service`,
- `l3`, `l5-service`, `long-duration-time-left`, `mipv6ha-service`,
- `msid`, `msisdn`, `nat`, `nemo-only`, `network-requested`, `network-type`, `pcf`,
- `pdns-service`, `plmn-name`, `profile-id`, `profile-name`, `qci`, `rx-data`, `slu-state`,
- `s5-proto`, `session-time-left`, `sgsn-address`, `sgw-address`, `smgr-instance`,
- `tx-data`, `username`, `grep`, `more`

### hnbgw-service `svc_name`

Displays subscriber information based on the HNB-GW service name.

`svc_name` must be an existing HNB-GW service expressed as an alphanumeric string of 1 through 63 characters.

The following filters/keywords are valid with this command:

- `access-type`, `active-charging-service`, `bandwidth-policy`, `bearer-establishment`, `bng-service`,
- `callid`, `card-num`, `cbb-policy`, `configured-idle-timeout`, `connected-time`,
- `csf-service`, `data-rate`, `domain`, `ebi`, `enodeb-address`, `epdg-address`, `fa`, `firewall`, `full`, `fw-and-nat`,
- `gtp-version`, `gtpu-bind-address`, `gtpu-service`, `ha`, `hnbgw-service`, `idle-time`, `ims-auth-service`,
- `imsi`, `ip-address`, `ip-alloc-method`, `ip-pool`, `ipv6-address`, `ipv6-prefix`,
- `l3-tunnel-local-addr`, `l3-tunnel-remote-addr`, `l4`, `l4-service`,
- `l3`, `l5-service`, `long-duration-time-left`, `mipv6ha-service`,
- `msid`, `msisdn`, `nat`, `nemo-only`, `network-requested`, `network-type`, `pcf`,
- `pdns-service`, `plmn-name`, `profile-id`, `profile-name`, `qci`, `rx-data`, `slu-state`,
- `s5-proto`, `session-time-left`, `sgsn-address`, `sgw-address`, `smgr-instance`,
- `tx-data`, `username`, `wfi`, `grep`, `more`
Exec Mode show Commands (Q-S)

Show subscribers

```
Exec Mode show Commands (Q-S)

show subscribers

hsgw-only
Displays HSGW subscriber session information.
The following filters/keywords are valid with this command:

aaa-configuration, access-flows, active, active-charging-only, all, bandwidth-policy, bearer-establishment, bng-service, callid, card-num, cbb-policy, configured-idle-timeout, connected-time, counters, data-rate, dormant, ebi, enodeb-address, epdg-address, fa, firewall, full, fw-and-nat, gtp-version, gtpu-bind-address, gtpu-service, ha, hsgw-service, idle-time, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, long-duration-time-left, mag-service, mipv6ha-service, msid, nat, network-type, pgw-address, policy, profile-id, profile-name, qci, rulebase, rx-data, slu-state, s5proto, session-time-left, sgw-address, smgr-instance, subscription, summary, tf, tx-data, username, wfl, grep, more

hsgw-service svc_name: Displays subscriber information based on the HSGW service name. svc_name must be an existing HSGW service expressed as an alphanumeric string of 1 through 63 characters.

hsgw-service svc_name
Displays subscriber information based on the HSGW service name. svc_name must be an existing HSGW service expressed as an alphanumeric string of 1 through 63 characters.
The following filters/keywords are valid with this command:

active-charging-service, bandwidth-policy, bearer-establishment, bng-service, callid, card-num, cbb-policy, configured-idle-timeout, connected-time, ebi, enodeb-address, epdg-address, fa, firewall, full, fw-and-nat, gtp-version, gtpu-bind-address, gtpu-service, ha, hsgw-service, idle-time, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, long-duration-time-left, mag-service, mipv6ha-service, msid, nat, network-type, profile-id, profile-name, qci, rulebase, rx-data, slu-state, s5proto, session-time-left, sgw-address, smgr-instance, subscription, summary, tf, tx-data, username, wfl, grep, more

idle-time
Displays current configuration for all subscribers within the specified idle-time interval.
• <: Filters output so that only information less than the specified value is displayed.
• <=: Filters output so that only information less than the specified value is displayed.
• >=: Filters output so that only information greater than the specified value is displayed.
• greater-than: Filters output so that only information greater than the specified value is displayed.
• less-than: Filters output so that only information less than the specified value is displayed.
```
show subscribers

- **value**: Used in conjunction with <, >, greater-than, less-than. If no other filtering options are specified only output matching **value** is displayed. If **value** is not specified all data is displayed. **value** must be an integer from 0 through 4294967295.

The following filter keywords are valid with this command:

```
epdg-address,
```

**imei imei_number**

Displays subscribers having the specified International Mobile Equipment Identity (IMEI/IMEISV) Number. Must be followed by **imei number**.

The following filter keywords are valid with this command:

```
apn, bearer-establishment, bng-service, callid, card-num, ccoa-only, configured-idle-timeout, connected-time, dhcp-server, ebi, enodeb-address, epdg-address, fa, fa-service, firewall, fw-and-nat, ggsn-service, gprs-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipse-only, ha-service, idle-time, imei, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, 13-tunnel-local-addr, 13-tunnel-remote-addr, lac, lac-service, lns, ins-service, long-duration-time-left, mip-up-tunnel-only, mipv6ha-service, mme-address, mme-service, msid, msisdn, nat, nemo-only, network-requested, network-type, pcf, psdn-service, plmn-type, profile-id, profile-name, qci, rx-data, slu-state, s5-_proto, session-time-left, sgsn-address, sgw-address, smgr-instance, tx-data, username, grep, more
```

**ims_auth-service svc_name**

Displays subscriber information based on the IMS authentication service name. **svc_name** must be an existing service expressed as an alphanumeric string of 1 through 63 characters.

The following filters/keywords are valid with this command:

```
access-type, active-charging-service, asngw-service, asnpa-service, bandwidth-policy, bearer-establishment, bng-service, callid, card-num, cbb-policy, ccoa-only, configured-idle-timeout, connected-time, csclf-service, dhcp-server, domain, ebi, enodeb-address, epdg-address, fa, fa-service, firewall, fw-and-nat, gprs-service, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipse-only, ha-service, hnbgw-service, hsgw-service, idle-time, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, 13-tunnel-local-addr, 13-tunnel-remote-addr, lac, lac-service, lma-service, lns, lns-service, long-duration-time-left, mag-service, mip-up-tunnel-only, mipv6ha-service, mme-address, mme-service, msid, msisdn, nat, nemo-only, network-requested, network-type, pcc-service, pcf, pdg-service, pdif-service, psdn-service, pgw-address, plmn-type, profile-id, profile-name, qci, rulebase, rx-data, slu-state, s5-_proto, security-type, session-time-left, sgsn-address, sgw-addr, sgw-service, smgr-instance, tx-data, ue-type, username, grep, more
```

Cisco ASR 5x00 Command Line Interface Reference
**imsi imsi**

Displays information specific to one subscriber or group of subscribers. Enter 1 to 15 digits to identify a specific subscriber’s IMSI (International Mobile Subscriber Identity).

The following filters/keywords are valid with this command:

- access-type
- active-charging-service
- apn
- asn-peer-address
- asngw-service
- asnpc-service
- bandwidth-policy
- bearer-establishment
- bng-service
- callid
- card-num
- ccb-policy
- ccoa-only
- configured-idle-timeout
- connected-time
- cscf-service
- dhcp-server
- domain
- ebi
- enodeb-address
- epdg-address
- fa
- fa-service
- firewall
- fw-and-nat
- ggsn-service
- gprs-service
- gsm-traffic-class
- gtp-version
- gtpu-bind-address
- gtpu-service
- ha
- ha-ipsec-only
- ha-service
- hbgw-service
- hsgw-service
- idle-time
- ims-auth-service
- imsi
- ip-address
- ip-alloc-method
- ip-pool
- ipv6-address
- ipv6-prefix
- 13-tunnel-local-addr
- 13-tunnel-remote-addr
- lac
- lac-service
- lma-service
- lns
- lns-service
- long-duration-time-left
- mag-services
- mip-up-tunnel-only
- mipv6a-service
- mm-e-address
- mm-e-service
- msid
- msisdn
- nat
- nemo-only
- network-requested
- network-type
- nsapi
- pcc-service
- pcf
- pdg-service
- pdif-service
- pdsm-service
- pgw-address
- plmn-type
- profile-id
- profile-name
- qci
- rulebase
- rx-data
- sla-state
- s5-proto
- security-type
- session-time-left
- sgsn-address
- sgsm-service
- sgw-service
- smgr-instance
- tx-data
- ue-type
- username
- grep
- more

**interface-type ( S2aGTP | S2bGTP | S5S8GTP )**

Specifies subscriber type as either S2a (eHRPD), S2b (ePDG) or S5/S8 (PMIPv6/GTP).

The following filter keywords are valid with this command:

- apn
- bearer-establishment
- bng-service
- callid
- card-num
- ccoa-only
- configured-idle-timeout
- congestion_mgmt
- connected-time
- dhcp-server
- ebi
- enodeb-address
- epdg-address
- epdg-address
- fa
- fa-service
- firewall
- fw-and-nat
- ggsn-service
- gprs-service
- gsm-traffic-class
- gtp-version
- gtpu-bind-address
- gtpu-service
- ha
- ha-ipsec-only
- ha-service
- idle-time
- imsi
- ims-auth-service
- imsi
- interface-type
- ip-address
- ip-alloc-method
- ip-pool
- ipv6-address
- ipv6-prefix
- 13-tunnel-local-addr
- 13-tunnel-remote-addr
- lac
- lac-service
- lns
- lns-service
- long-duration-time-left
- mip-udp-tunnel-only
- mipv6a-service
- mm-e-address
- mm-e-service
- msid
- msisdn
- nat
- nemo-only
- network-requested
- network-type
- pcf
- pcp
- pdsm-service
- plmn-type
- profile-id
- profile-name
- qci
- rx-data
- sla-state
- s5-proto
- session-time-left
- sgsn-address
- sgw-address
- smgr-instance
- tx-data
- username
- wsg-service
- grep
- more

**ip-address ipv4_address**

Displays the subscribers associated with the specified IPv4 address. Must be followed by the IP address in IPv4 dotted-decimal notation.

The following filter keywords are valid with this command:

- access-type
- active-charging-service
- apn
- asn-peer-address
- asngw-service
- asnpc-service
- bandwidth-policy
- bearer-establishment
- bng-service
- callid
- card-num
- ccb-policy
- ccoa-only
- configured-idle-timeout
- connected-time
- cscf-service
- dhcp-server
- domain
- ebi
- enodeb-address
- epdg-address
- fa
- fa-service
- firewall
- fw-and-nat
- ggsn-service
- gprs-service
- gsm-traffic-class
- gtp-version
- gtpu-bind-address
- gtpu-service
- ha
- ha-ipsec-only
- ha-service
- hbgw-service
- hsgw-service
- idle-time
- ims-auth-service
- imsi
- ip-address
- ip-alloc-method
- ip-pool
- ipv6-address
- ipv6-prefix
- 13-tunnel-local-addr
- 13-tunnel-remote-addr
- lac
- lac-service
- lns
- lns-service
- long-duration-time-left
- mip-udp-tunnel-only
- mipv6a-service
- mm-e-address
- mm-e-service
- msid
- msisdn
- nat
- nemo-only
- network-requested
- network-type
- pcf
- pcp
- pdsm-service
- plmn-type
- profile-id
- profile-name
- qci
- rx-data
- sla-state
- s5-proto
- session-time-left
- sgsn-address
- sgw-address
- smgr-instance
- tx-data
- username
- wsg-service
- grep
- more
The following filter keywords are valid with this command:

- **aaa-assigned**: Selects subscribers whose IP addresses were assigned by AAA.
- **dhcp**: Selects subscribers whose IP addresses were assigned by DHCP.
  - **relay-agent**: Selects subscribers whose IP addresses were assigned by the DHCP Relay Agent
  - **proxy-client**: Selects subscribers whose IP addresses were assigned by the DHCP Proxy Client
- **dynamic-pool**: Selects subscribers whose IP addresses were assigned from a dynamic IP address pool.
- **12tp-1ns-assigned**: Selects subscribers whose IP addresses were assigned by the Layer 2 Tunneling Protocol (LT2P) Network Server.
- **mip-ha-assigned**: Selects subscribers whose IP addresses were assigned by the Mobile IP Home Agent.
- **ms-provided-static**: Selects subscribers whose IP addresses were provided by the Mobile Station.
- **not-ms-provided-static**: Selects subscribers whose IP addresses were not provided by the Mobile Station.
- **static-pool**: Selects subscribers whose IP addresses were assigned from a static IP address pool.

The following filter keywords are valid with this command:

- access-type, active-charging-service, apn, asn-peer-address, asngw-service, asnpc-service, bandwidth-policy, bearer-establishment, bng-service, callid, card-num, ccb-policy, ccoa-only, configured-idle-timeout, connected-time, csnf-service, dhcp-server, domain, ebi, enodeb-address, epdg-address, fa, fa-service, firewall, fw-and-nat, ggsn-service, gprs-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, hnbgw-service, hsgw-service, idle-time, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, lac, lac-service, lma-service, lns, lns-service, long-duration-time-left, mag-service, mip-up-tunnel-only, mipv6ha-service, mme-address, mme-service, msid, msisdn, nat, nemo-only, network-requested, network-type, nsapi, pcc-service, pcf, pdg-service, pdif-service, psdn-service, pgw-address, plmn-type, profile-id, profile-name, qci, rulebase, rx-data, slu-state, s5-proto, security-type, session-time-left, sgsn-address, sgsn-service, sgw-address, sgw-service, smgr-instance, tx-data, ue-type, username, grep, more
The following filter keywords are valid with this command:

- pdif-service
- pdsn-service
- pgw-address
- plmn-type
- profile-id
- profile-name
- qci
- relay-agent
- rulebase
- rx-data
- slu-state
- s5-proto
- security-type
- session-time-left
- sgsn-address
- sgw-service
- sgw-address
- smgr-instance
- tx-data
- ue-type
- username
- grep
- more

**ip-pool ip_pool_name**

Displays subscriber information based on the IP pool name. *ip_pool_name* must be an existing IP pool name expressed as an alphanumeric string of 1 through 31 characters.

The following filter keywords are valid with this command:

- access-type
- active-charging-service
- apn
- asn-peer-address
- asngw-service
- asnpc-service
- bandwidth-policy
- bearer-establishment
- bng-service
- callid
- card-num
- cbb-policy
- ccoa-only
- configured-idle-timeout
- connected-time
- csclf-service
- dhcp-server
- domain
- ebi
- enodeb-address
- epdg-address
- fa
- fa-service
- firewall
- fw-and-nat
- ggsn-service
- gprs-service
- gsm-traffic-class
- gtp-version
- gtpu-bind-address
- gtpu-service
- ha
- ha-ipsec-only
- ha-service
- hnbgw-service
- hsgw-service
- idle-time
- ims-auth-service
- imsi
- ip-address
- ip-alloc-method
- ip-pool
- ipv6-address
- ipv6-prefix
- 13-tunnel-local-addr
- 13-tunnel-remote-addr
- lac
- lac-service
- lma-service
- lns
- lns-service
- long-duration-time-left
- mag-service
- mip-up-tunnel-only
- mipv6ha-service
- mme-address
- mme-service
- msid
- msisdn
- nat
- nemo-only
- network-requested
- network-type
- nsapi
- pcc-service
- pcf
- pdg-service
- pdif-service
- pdsn-service
- pgw-address
- plmn-type
- profile-id
- profile-name
- qci
- rulebase
- rx-data
- slu-state
- s5-proto
- security-type
- session-time-left
- sgsn-address
- sgw-service
- sgw-address
- sgw-service
- smgr-instance
- tx-data
- ue-type
- username
- grep
- more

**ipcf-only**

Displays Intelligent Policy Control Function (IPCF) subscriber session information.

**ipsg-only**

Displays IP Services Gateway (IPSG) subscriber session information.

The following filter keywords are valid with this command:

- epdg-address

**ipv6-address ipv6_address**

Displays the subscribers associated with the specified IPv6 address. Must be followed by the IP address in IPv6 colon-separated-hexadecimal notation.

The following filter keywords are valid with this command:

- apn
- asn-peer-address
- asngw-service
- asnpc-service
- bearer-establishment
- bng-service
- callid
- card-num
- ccoa-only
- configured-idle-timeout
- connected-time
- csclf-service
- dhcp-server
- ebi
- enodeb-address
- epdg-address
- fa
- fa-service
- firewall
- fw-and-nat
- ggsn-service
- gprs-service
- gsm-traffic-class
- gtp-version
- gtpu-bind-address
- gtpu-service
- ha
- ha-ipsec-only
- ha-service
- hsgw-service
- idle-time
- imei
- ims-auth-service
- imsi
- ip-address
- ip-alloc-method
- ip-pool
- ipv6-address
- ipv6-prefix

Cisco ASR 5x00 Command Line Interface Reference
The following filter keywords are valid with this command:

access-type, active-charging-service, apn, asn-peer-address, asngw-service, asnpc-service, bandwidth-policy, bearer-establishment, bng-service, callid, card-num, cbb-policy, ccoa-only, configured-idle-timeout, connected-time, csf-service, dhcp-server, domain, ebi, enodeb-address, epdg-address, fa, fa-service, firewall, fw-and-nat, ggsn-service, gprs-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsecoonly, ha-service, hnbgw-service, hsgw-service, idle-time, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, lac, lac-service, lma-service, lns, lns-service, long-duration-time-left, mag-service, mip-up-tunnel-only, mipv6ha-service, mme-address, mme-service, msid, msisdn, nat, nemo-only, network-requested, network-type, nsapi, pcc-service, pcf, pdg-service, pdif-service, pdsn-service, pgw-address, plmn-type, profile-id, profile-name, qci, rx-data, slu-state, s5-proto, session-time-left, sgn-neighbor, sgn-address, sgw-address, smgw-instance, tx-data, username, grep, more

**ipv6-prefix ipv6_prefix**

Displays the subscribers associated with the specified IPv6 address prefix. Must be followed by an IPv6 address prefix in the format xx:xx:xx::/len

The following filter keywords are valid with this command:

access-type, active-charging-service, apn, asn-peer-address, asngw-service, asnpc-service, bandwidth-policy, bearer-establishment, bng-service, callid, card-num, cbb-policy, ccoa-only, configured-idle-timeout, connected-time, csf-service, dhcp-server, domain, ebi, enodeb-address, epdg-address, fa, fa-service, firewall, fw-and-nat, ggsn-service, gprs-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, hnbgw-service, hsgw-service, idle-time, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, lac, lac-service, lma-service, lns, lns-service, long-duration-time-left, mag-service, mip-up-tunnel-only, mipv6ha-service, mme-address, mme-service, msid, msisdn, nat, nemo-only, network-requested, network-type, nsapi, pcc-service, pcf, pdg-service, pdif-service, pdsn-service, pgw-address, plmn-type, profile-id, profile-name, qci, rulebase, rx-data, slu-state, s5-proto, security-type, session-time-left, sgn-neighbor, sgn-address, sgw-address, smgw-instance, tx-data, ue-type, username, grep, more

**l3-tunnel-local-addr ipv4_address**

Displays subscriber information based on the layer 3 tunneling interface. Must be followed by an IP address of the local interface, using IPv4 dotted-decimal notation.

The following filter keywords are valid with this command:

access-type, active-charging-service, apn, asn-peer-address, asngw-service, asnpc-service, bandwidth-policy, bearer-establishment, bng-service, callid, card-num, cbb-policy, ccoa-only, configured-idle-timeout, connected-time, csf-service, dhcp-server, domain, ebi, enodeb-address, epdg-address, fa, fa-service, firewall, fw-and-nat, ggsn-service, gprs-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, hnbgw-service, hsgw-service, idle-time, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, lac, lac-service, lma-service, lns, lns-service, long-duration-time-left, mag-service, mip-up-tunnel-only, mipv6ha-service, mme-address, mme-service, msid, msisdn, nat, nemo-only, network-requested, network-type, nsapi, pcc-service, pcf, pdg-service, pdif-service, pdsn-service, pgw-address, plmn-type, profile-id,
### show subscribers

Profile-name, qci, rulebase, rx-data, slu-state, s5-proto, security-type, session-time-left, sgsn-address, sgsn-service, sgw-address, sgw-service, smgr-instance, tx-data, ue-type, username, grep, more

#### 13-tunnel-remote-addr ipv4_address

Displays subscriber information based on the layer 3 tunneling interface. Must be followed by an IP address of the remote interface, using IPv4 dotted-decimal notation.

The following filter keywords are valid with this command:

- access-type, active-charging-service, apn, asn-peer-address, asngw-service, asnpcc-service, bandwidth-policy, bearer-establishment, bng-service, callid, card-num, ccb-policy, ccoa-only, configured-idle-timeout, connected-time, csacf-service, dhcp-server, domain, ebi, enodeb-address, epdg-address, fa, fa-service, firewall, fw-and-nat, ggsn-service, gprs-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, hnbgw-service, hsgw-service, idle-time, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, 13-tunnel-local-addr, 13-tunnel-remote-addr, lac, lac-service, lma-service, lns, lns-service, long-duration-time-left, mag-service, mip-up-tunnel-only, mipv6ha-service, mme-address, mme-service, msid, msisdn, nat, nemo-only, network-requested, network-type, nsapi, pcc-service, pcf, pdg-service, pdif-service, pdms-service, pgw-address, plmn-type, profile-id, profile-name, qci, rulebase, rx-data, slu-state, s5-proto, security-type, session-time-left, sgsn-address, sgsn-service, sgw-service, smgr-instance, tx-data, ue-type, username, grep, more

#### lac ipv4_address

Displays subscriber information based on the Peer L2TP Access Concentrator (LAC). Must be followed by the IP address of a Remote LAC in IPv4 dotted-decimal notation.

The following filter keywords are valid with this command:

- apn, bearer-establishment, bng-service, callid, card-num, ccoa-only, configured-idle-timeout, connected-time, dhcp-server, ebi, enodeb-address, epdg-address, fa, fa-service, firewall, fw-and-nat, ggsn-service, gprs-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, idm, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, 13-tunnel-local-addr, 13-tunnel-remote-addr, lac, lac-service, lns, lns-service, long-duration-time-left, mip-up-tunnel-only, mipv6ha-service, msid, msisdn, nat, nemo-only, network-requested, network-type, pcf, pdm-service, plmn-type, profile-id, profile-name, qci, rulebase, rx-data, slu-state, s5-proto, session-time-left, sgsn-address, sgsn-service, sgw-address, smgr-instance, tx-data, ue-type, username, grep, more

#### lac-only

Displays subscriber information based on the L2TP Access Concentrator (LAC) context information for the session.
**lac-service svc_name**

Displays subscriber information based on an existing LAC service name expressed as an alphanumeric string of 1 through 63 characters.

The following filter keywords are valid with this command:

- apn, bearer-establishment, bng-service, callid, card-num, ccoa-only, configured-idle-timeout, connected-time, dhcp-server, ebi, enodeb-address, epdg-address, fa, fa-service, firewall, fw-and-nat, ggsn-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, idle-time, imei, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, lac, lac-service, lns, lns-service, local-tunnel-id, long-duration-time-left, mip-udp-tunnel-only, mipv6ha-service, msid, msisdn, nat, nemo-only, network-requested, network-type, pcf, pdsn-service, plmn-type, profile-id, profile-name, qci, remote-tunnel-id, rx-data, slu-state, s5proto, session-time-left, sgsn-address, sgw-address, smgr-instance, tx-data, username, grep, more

**lma-only**

Displays Local Mobility Anchor (LMA) specific context information for the session.

**lma-service svc_name**

Displays subscriber information based on the LMA service name. *svc_name* must be an existing LMA service expressed as an alphanumeric string of 1 through 63 characters.

**lns ipv4_address**

Displays subscriber information based on the L2TP Network Server (LNS). Must be followed by the IP address of an LNS in IPv4 dotted-decimal notation.

The following filter keywords are valid with this command:

- apn, bearer-establishment, bng-service, callid, card-num, ccoa-only, configured-idle-timeout, connected-time, dhcp-server, ebi, enodeb-address, epdg-address, fa, fa-service, firewall, fw-and-nat, ggsn-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, idle-time, imei, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, lac, lac-service, lns, lns-service, local-tunnel-id, long-duration-time-left, mip-udp-tunnel-only, mipv6ha-service, msid, msisdn, nat, nemo-only, network-requested, network-type, pcf, pdsn-service, plmn-type, profile-id, profile-name, qci, remote-tunnel-id, rx-data, slu-state, s5proto, session-time-left, sgsn-address, sgw-address, smgr-instance, tx-data, username, grep, more

**lns-only**

Displays LNS specific information only.

**lns-service svc_name**

Displays subscriber information based on an existing L2TP Network Server (LNS) service name expressed as an alphanumeric string of 1 through 63 characters.
The following filter keywords are valid with this command:

- bearer-establishment, bng-service, callid, card-num, configured-idle-duration, connected-time, ebi, enodeb-address, epdg-address, fa, firewall, fw-and-nat, gtp-version, gtpu-bind-address, gtpu-service, ha, idle-time, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, lac, lac-service, lns-service, local-tunnel-id, long-duration-time-left, mipv6ha-service, msid, nat, network-type, profile-id, profile-name, qci, remote-tunnel-id, rx-data, s1u-data, s5-proto, session-time-left, sgw-address, smgr-instance, tx-data, username, grep, more

```
long-duration-time-left [< | > | greater-than | less-than ] value
```

Shows how much time is left for the maximum duration of a specified subscriber session.
- `<`: Filters output so that only information less than the specified value is displayed.
- `>`: Filters output so that only information greater than the specified value is displayed.
- `greater-than`: Filters output so that only information greater than the specified value is displayed.
- `less-than`: Filters output so that only information less than the specified value is displayed.
- `value`: Used in conjunction with `<`, `>`, greater-than, less-than. If no other filtering options are specified only output matching `value` is displayed. If `value` is not specified all data is displayed. `value` must be an integer from 0 through 4294967295.

```
mag-only
```

Displays Mobile Access Gateway (MAG) subscriber session information.

```
mag-service svc_name
```

Displays subscriber information based on the Mobile Access Gateway (MAG) service name. `svc_name` must be an existing MAG service expressed as an alphanumeric string of 1 through 63 characters.

```
mag-service svc_name
```

Displays subscriber information based on the Mobile Access Gateway (MAG) service name. `svc_name` must be an existing MAG service expressed as an alphanumeric string of 1 through 63 characters.

```
mip-udp-tunnel-only
```

Displays Mobile IP Home Agent (MIP-HA) subscriber information for subscribers that negotiated MIP-UDP tunnels.

The following filter keywords are valid with this command:

- apn, bearer-establishment, bng-service, callid, card-num, ccoa-only, configured-idle-duration, connected-time, dhcp-server, ebi, enodeb-address, epdg-address, fa, fa-service, firewall, fw-and-nat, ggsn-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, idle-time, imei, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, lac, lac-service, lns, lns-service, long-duration-time-left, mip-udp-tunnel-only, mipv6ha-service, msid, msisdn, nat, nemo-only, network-requested, network-type, pcf, pdns-service, plmn-type, profile-id, profile-name, qci, rx-data, s1u-state, s5-proto, session-time-left, sgsn-address, sgw-address, smgr-instance, tx-data, username, grep, more
mipv6ha-only
Displays MIP-HA-IPv6 context information for the session.
The following filters/keywords are valid with this command:

aaa-configuration, access-flows, access-type, active, active-charging-service, activity, all, apn, asn-peer-address, asngw-service, asnpv-service, bandwidth-policy, bearer-establishment, bng-service, callid, card-num, ccb-policy, ccoa-only, configured-idle-timeout, connected-time, counters, csf-service, data-rate, dhcp-server, domain, dormant, ebi, enodeb-address, epdg-address, fa, fa-service, firewall, full, fw-and-nat, ggsn-address, gprs-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, hnbgw-service, hsgw-service, idle-time, imei, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, lac, lac-service, lma-service, lns, lns-service, long-duration-time-left, mag-service, mipv6ha-service, mme-address, mme-service, msid, nat, network-requested, network-type, pcc-service, pcf, pdg-service, pdif-service, pgw-address, policy, profile-id, profile-name, qci, rulebase, rx-data, slu-state, s5_proto, security-type, session-time-left, sgsn-address, sgsn-service, sgw-address, sgw-service, smgr-instance, subscription, summary, tft, tx-data, ue-type, username, wfi, grep, more

mipv6ha-service svc_name
Displays subscriber information based on an existing MIP Home Agent IPv6 service name expressed as an alphanumeric string of 1 through 63 characters.
The following filter keywords are valid with this command:

access-type, active-charging-service, apn, asn-peer-address, asngw-service, asnpv-service, bandwidth-policy, bearer-establishment, bng-service, callid, card-num, ccb-policy, ccoa-only, configured-idle-timeout, connected-time, csf-service, dhcp-server, domain, ebi, enodeb-address, epdg-address, fa, fa-service, firewall, fw-and-nat, ggsn-service, gprs-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, hnbgw-service, hsgw-service, idle-time, imei, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, lac, lac-service, lma-service, lns, lns-service, long-duration-time-left, mag-service, mipv6ha-service, mme-address, mme-service, msid, nat, network-requested, network-type, pcc-service, pcf, pdg-service, pdif-service, pgw-address, policy, profile-id, profile-name, qci, rulebase, rx-data, slu-state, s5_proto, security-type, session-time-left, sgsn-address, sgsn-service, sgw-address, sgw-service, smgr-instance, tx-data, ue-type, username, grep, more

mme-address
Displays subscriber information based on the Mobility Management Entity (MME) IP address. ip_address must be an existing MME IP address and be entered in IPv4 dotted-decimal notation or IPv6 colon-separated-hexadecimal notation.
The following filter keywords are valid with this command:
 bearer-establishment, bng-service, callid, card-num, configured-idle-timeout, connected-time, ebi, enodeb-address, epdg-address, fa, firewall, fw-and-nat, gtp-version, gtpu-bind-address, gtpu-service, ha, idle-time, imei, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, 13-tunnel-local-addr, 13-tunnel-remote-addr, long-duration-time-left, mipv6ha-service, mme-address, mme-service, msid, msisdn, nat, network-type, profile-id, profile-name, qci, rx-data, slu-state, s5-proto, session-time-left, sgw-address, smgr-instance, tx-data, username, grep, more

**mme-only**

Displays MME subscriber session information.

**mme-service svc_name**: Displays subscriber information based on the MME service name. *svc_name* must be an existing MME service expressed as an alphanumeric string of 1 through 63 characters.

**mme-address ip_address**: Displays subscriber information based on the MMM IP address. *ip_address* must be an existing MME IP address entered in IPv4 dotted-decimal notation or IPv6 colon-separated-hexadecimal notation.

The following filter keywords are valid with this command:

 bearer-establishment, bng-service, callid, card-num, configured-idle-timeout, connected-time, ebi, enodeb-address, epdg-address, fa, firewall, fw-and-nat, gtp-version, gtpu-bind-address, gtpu-service, ha, idle-time, imei, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, 13-tunnel-local-addr, 13-tunnel-remote-addr, long-duration-time-left, mipv6ha-service, mme-address, mme-service, msid, msisdn, nat, network-type, profile-id, profile-name, qci, rx-data, slu-state, s5-proto, session-time-left, sgw-address, smgr-instance, tx-data, username, grep, more

**msg-only**

**Important**: This keyword is not supported in this release.

**msg-service msg_service_name**

**Important**: This keyword is not supported in this release.

**msid msid**

For this SGSN-specific keyword, enter the MSID (Mobile Station IDentifier) to display information specific to one subscriber’s equipment by entering the MSID.

The following filter keywords are valid with this command:

 apn, asn-peer-address, asngw-service, asnpc-service, bearer-establishment, bng-service, callid, card-num, ccoa-only, configured-idle-timeout, connected-time, dhcp-server, ebi, enodeb-address, epdg-address, fa, fa-service, firewall, fw-and-nat, ggsn-service, gprs-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, hsgw-service, idle-time, imei, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix,
show subscribers

13-tunnel-local-addr, 13-tunnel-remote-addr, lac, lac-service, lma-service, lns, lns-service, long-duration-time-left, mag-service, mip-udp-tunnel-only, mipv6ha-service, mme-address, mme-service, msid, msisdn, nat, nemo-only, network-requested, network-type, pcf, pdg-service, pdif-service, pdsn-service, pgw-address, plmn-type, profile-id, profile-name, qci, rx-data, sla-state, s5-proto, session-time-left, sgsn-address, sgw-address, sgw-service, smgr-instance, tx-data, username, grep, more

**msisdn msisdn**

For this SGSN-specific keyword, enter the MSISDN (Mobile Station ISDN number - unique SIM phone number) to display information specific to one subscriber’s equipment by entering the MSISDN.

The following filter keywords are valid with this command:

apn, bearer-establishment, bng-service, callid, card-num, ccoa-only, configured-idle-timeout, connected-time, dhcp-server, ebi, enodeb-address, epdg-address, fa, fa-service, firewall, fw-and-nat, ggsn-service, gprs-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, idle-time, imei, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, 13-tunnel-local-addr, 13-tunnel-remote-addr, lac, lac-service, lns, lns-service, long-duration-time-left, mip-udp-tunnel-only, mipv6ha-service, mme-address, mme-service, msid, msisdn, nat, nemo-only, network-requested, network-type, pcf, pdsn-service, plmn-type, profile-id, profile-name, qci, rx-data, sla-state, s5-proto, session-time-left, sgsn-address, sgw-address, smgr-instance, tx-data, username, grep, more

**nat { not-required | required }**

Displays information for subscribers based on whether or not Network Address Translation (NAT) processing is required.

The following filter keywords are valid with this command:

access-type, active-charging-service, apn, asn-peer-address, asngw-service, asnpc-service, bandwidth-policy, bearer-establishment, bng-service, callid, card-num, cbb-policy, ccoa-only, configured-idle-timeout, connected-time, cs.cf-service, dhcp-server, domain, ebi, enodeb-address, epdg-address, fa, fa-service, firewall, fw-and-nat, ggsn-service, gprs-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, hnbgw-service, hsgw-service, idle-time, imei, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, 13-tunnel-local-addr, 13-tunnel-remote-addr, lac, lac-service, lma-service, lns, lns-service, long-duration-time-left, mag-service, mip-up-tunnel-only, mipv6ha-service, mme-address, mme-service, msid, msisdn, nat, nat-ip, nat-realm, nemo-only, network-requested, network-type, pcc-service, pcf, pdg-service, pdif-service, pdsn-service, pgw-address, plmn-type, profile-id, profile-name, qci, rulebase, rx-data, sla-state, s5-proto, security-type, session-time-left, sgsn-address, sgw-address, sgw-service, smgr-instance, tx-data, ue-type, username, grep, more
nemo-only
Displays information on MIP-HA subscribers that are mobile routers (Network Mobility).
The following filter keywords are valid with this command:

- apn, bearer-establishment, bng-service, callid, card-num, ccoa-only, configured-idle-timeout, connected-time, dhcp-server, ebi, enodeb-address, epdg-address, fa, fa-service, firewall, fw-and-nat, ggsn-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, idle-time, imei, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, lac, lac-service, lns, lns-service, long-duration-time-left, mip-udp-tunnel-only, mipv6ha-service, msid, msisdn, nat, nemo-only, network-requested, network-type, pcf, pdsn-service, plmn-type, profile-id, profile-name, qci, rx-data, slu-state, s5proto, session-time-left, sgsn-address, sgw-address, smgr-instance, tx-data, username, grep, more

network-requested
Selects the currently active subscribers whose sessions were initiated by a GGSN network requested to create a PDP context.
The following filter keywords are valid with this command:

- access-type, active-charging-service, apn, bandwidth-policy, bearer-establishment, bng-service, callid, card-num, cbb-policy, ccoa-only, configured-idle-timeout, connected-time, csclf-service, dhcp-server, domain, ebi, enodeb-address, epdg-address, fa, fa-service, firewall, fw-and-nat, ggsn-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, hnbgw-service, idle-time, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, lac, lac-service, lns, lns-service, long-duration-time-left, mip-up-tunnel-only, mipv6ha-service, msid, msisdn, nat, nemo-only, network-requested, network-type, nsapi, pcc-service, pcf, pdsn-service, plmn-type, profile-id, profile-name, qci, rulebase, rx-data, slu-state, s5proto, security-type, session-time-left, sgsn-address, sgw-address, smgr-instance, tx-data, ue-type, username, grep, more

network-type { gre | ipip | ipsec | ipv4 | ipv4-pmipv6 | ipv4v6 | ipv4v6-pmipv6 | ipv6 | ipv6-pmipv6 | l2tp | mobile-ip | proxy-mobile-ip }
Selects the currently active subscribers based on network service access type.

- **gre**: Generic Routing Encapsulation
- **ipip**: IP-in-IP
- **ipsec**: IPsec
- **ipv4**: IPv4 only
- **ipv4-pmipv6**: IPv4 and/or Proxy Mobile IPv6 (PMIP)
- **ipv4v6**: IPv4 and/or IPv6
- **ipv4v6-pmipv6**: IPv4, IPv6 and/or Proxy Mobile IPv6
• ipv6: IPv6 only
• ipv6-pmipv6: IPv6 and/or Proxy Mobile IPv6 (PMIP)
• 12tp: Layer 2 Tunneling Protocol
• mobile-ip: Mobile IP (MIP)
• proxy-mobile-ip: Proxy Mobile IPv6 (PMIP)

The following filter keywords are valid with this command:

apn, asn-peer-address, asngw-service, asnpc-service, bearer-establishment, bng-service, callid, card-num, ccoa-only, configured-idle-timeout, connected-time, dhcp-server, ebi, enodeb-address, epdg-address, fa, fa-service, firewall, fw-and-nat, ggsn-service, gprs-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, hsgw-service, idle-time, imei, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, 13-tunnel-local-addr, 13-tunnel-remote-addr, lac, lac-service, lma-service, lns, lns-service, long-duration-time-left, mag-service, mip-udp-tunnel-only, mipv6ha-service, mme-address, mme-service, msid, msisdn, nat, nemo-only, network-requested, network-type, pcf, pdg-service, pdif-service, pdn-service, pgw-address, plmn-type, profile-id, profile-name, qci, rx-data, slu-state, s5proto, session-time-left, sgsn-address, sgw-address, sgw-service, smgr-instance, tx-data, username, grep, more

**pcc-service name**

Displays statistics for users associated with an existing Policy and Charging Control (PCC) service name expressed as an alphanumeric string of 1 through 63 characters.

**pcf [ < | > | less-than | greater-than] ipv4_address [ < | > | less-than | greater-than ]**

Displays information for subscribers connected via the packet control function (PCF) with a specific or range of IP addresses. The address must be specified using IPv4 dotted-decimal notation.

- `<`: Filters output so that only information less than the specified IPv4 address value is displayed.
- `>`: Filters output so that only information greater than the specified IPv4 address value is displayed.
- `less-than`: Filters output so that only information less than the specified IPv4 address value is displayed.
- `greater-than`: Filters output so that only information greater than the specified IPv4 address value is displayed.

Note: It is possible to define a limited range of IP addresses by using the less-than and greater-than options to define minimum and maximum values.

The following filter keywords are valid with this command:

<, apn, bearer-establishment, bng-service, callid, card-num, ccoa-only, configured-idle-timeout, connected-time, dhcp-server, ebi, enodeb-address, epdg-address, fa, fa-service, firewall, fw-and-nat, ggsn-service, gprs-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, idle-time, imei, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, 13-tunnel-local-addr, 13-tunnel-remote-addr, lac, lac-service, less-than, lns, lns-service, long-duration-time-left, mip-udp-tunnel-only, mipv6ha-
service, msid, msisdn, nat, nemo-only, network-requested, network-type, pcf, pdns-service, plmn-type, profile-id, profile-name, qci, rx-data, slu-state, s5-proto, session-time-left, sgsn-address, sgw-address, smgr-instance, tx-data, username, grep, more

**pdg-only**

Displays a summary of PDG subscriber statistics.
The following filters/keywords are valid with this command:

aaa-configuration, access-flows, active, activity, all, apn, bearer-establishment, bng-service, callid, card-num, configured-idle-timeout, connected-time, counters, data-rate, dormant, ebi, enodeb-address, epdg-address, fa, firewall, full, fw-and-nat, gtp-version, gtpu-bind-address, gtpu-service, ha, idle-time, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, 13-tunnel-local-addr, 13-tunnel-remote-addr, long-duration-time-left, mipv6ha-service, msid, nat, network-type, pdg-service, policy, profile-id, profile-name, qci, rx-data, slu-state, s5-proto, session-time-left, sgw-address, smgr-instance, subscription, summary, tft, tx-data, username, wfl, grep, more

**pdg-service name**

Displays statistics for users associated with an existing Packet Data Gateway (PDG) service name expressed as an alphanumeric string of 1 through 63 characters.
The following filters/keywords are valid with this command:

bearer-establishment, bng-service, callid, card-num, configured-idle-timeout, connected-time, ebi, enodeb-address, epdg-address, fa, firewall, fng-service, fw-and-nat, gtp-version, gtpu-bind-address, gtpu-service, ha, idle-time, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, 13-tunnel-local-addr, 13-tunnel-remote-addr, long-duration-time-left, mipv6ha-service, msid, nat, network-type, pdg-service, profile-id, profile-name, qci, rx-data, slu-state, s5-proto, session-time-left, sgw-address, smgr-instance, tx-data, username, grep, more

**pdif-only**

Displays a summary of Packet Data Interworking Function (PDIF) subscriber statistics.
The following filters/keywords are valid with this command:

aaa-configuration, access-flows, active, activity, all, apn, bearer-establishment, bng-service, callid, card-num, configured-idle-timeout, connected-time, counters, data-rate, dormant, ebi, enodeb-address, epdg-address, fa, fa-service, firewall, fng-service, full, fw-and-nat, gtp-version, gtpu-bind-address, gtpu-service, ha, idle-time, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, 13-tunnel-local-addr, 13-tunnel-remote-addr, long-duration-time-left, mipv6ha-service, msid, nat, network-type, pdif-service, policy, profile-id, profile-name, qci, rx-data, slu-state, s5-proto, session-time-left, sgw-address, smgr-instance, subscription, summary, tft, tx-data, username, wfl, grep, more
**show subscribers**

Displays connection statistics for users associated with a specific PDIF service name.

The following filters/keywords are valid with this command:

- bearer-establishment, bng-service, callid, card-num, configured-idle-timeout, connected-time, ebi, enodeb-address, epdg-address, fa, fa-service, firewall, fw-and-nat, gtp-version, gtpu-bind-address, gtpu-service, ha, idle-time, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, 13-tunnel-local-addr, 13-tunnel-remote-addr, long-duration-time-left, mipv6ha-service, msid, nat, network-type, pdif-service, profile-id, profile-name, qci, rx-data, slu-state, s5,proto, session-time-left, sgw-address, smgr-instance, tx-data, username, grep, more

**pdif-service name**

**pdsn-only**

Displays a summary of Packet Data Serving Node (PDSN) subscriber statistics.

The following filters/keywords are valid with this command:

- aaa-configuration, access-flows, active, activity, all, apn, bandwidth-policy, bearer-establishment, bng-service, callid, card-num, ccoa-only, configured-idle-timeout, connected-time, counters, data-rate, dhcp-server, dormant, ebi, enodeb-address, epdg-address, fa, fa-service, firewall, full, fw-and-nat, ggsn-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsecc-only, ha-service, idle-time, imei, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, 13-tunnel-local-addr, 13-tunnel-remote-addr, lac, lac-service, lns, lns-service, long-duration-time-left, mipv6ha-service, msid, nat, nemo-only, network-requested, network-type, pcf, pdif-service, pimm-type, policy, profile-id, profile-name, qci, rx-data, slu-state, s5/proto, session-time-left, sgw-address, sgw-address, smgr-instance, subscription, summary, tft, tx-data, username, wfl, grep, more

**pdif-service name**

Displays statistics for users associated with an existing PDSN service name expressed as an alphanumeric string of 1 through 63 characters.

The following filter keywords are valid with this command:

- apn, bearer-establishment, bng-service, callid, card-num, ccoa-only, configured-idle-timeout, connected-time, dhcp-server, ebi, enodeb-address, epdg-address, fa, fa-service, firewall, fw-and-nat, ggsn-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsecc-only, ha-service, idle-time, imei, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, 13-tunnel-local-addr, 13-tunnel-remote-addr, lac, lac-service, lns, lns-service, long-duration-time-left, mag-address, mip-udp-tunnel-only, mipv6ha-service, msid, msisdn, nat, nemo-only, network-requested, network-type, pcf, pdif-service, pimm-type, policy, profile-id, profile-name, qci, rx-data, slu-state, s5/proto, session-time-left, sgw-address, sgsn-service, sgw-address, smgr-instance, subscription, summary, tft, tx-data, username, grep, more
**show subscribers**

Displays information about the subscribers connected to the specified P-GW.

**ip_address** must be specified by its IP address using dotted-decimal notation for IPv4 or colon separated notation for IPv6.

The following filters/keywords are valid with this command:

- active-charging-service
- apn
- bandwidth-policy
- bearer-establishment
- bng-service
- callid
- card-num
- cbb-policy
- configured-idle-timeout
- connected-time
- ebi
- enodeb-address
- epdg-address
- fa
- firewall fw-and-nat
- gtp-version
- gtpu-bind-address
- gtpu-service
- ha
- idle-time
- ims-auth-service
- imsi
- ip-address
- ip-alloc-method
- ip-pool
- ipv6-address
- ipv6-prefix
- 13-tunnel-local-addr
- 13-tunnel-remote-addr
- lac-service
- lma-service
- lns
- long-duration-time-left
- mag-service
- mipv6-ha-service
- msid
- nat
- network-type
- pgw-address
- plmn-type
- profile-id
- profile-name
- qci
- rule-base
- rx-data
- slu-state
- s5-proto
- saegw-service
- session-time-left
- sgw-address
- sgw-service
- smgr-instance
- summary

**pgw-only**

Displays PDN-Gateway (P-GW) subscriber session information.

The following filters/keywords are valid with this command:

- all
- apn
- callid
- card-num
- ebi
- epdg-address
- full
- imsi
- interface-type
- ip-address
- ip-alloc-method
- ip-pool
- ipv6-address
- ipv6-prefix
- network-type
- pgw-service
- plmn-type
- profile-id
- profile-name
- qci
- rule-base
- rx-data
- slu-state
- s5-proto
- saegw-service
- session-time-left
- sgw-address
- sgw-service
- smgr-instance
- summary

**epdg-address ip_address**: Displays subscriber information based on the ePDG IP address. **ip_address** must be an existing ePDG IP address.

**interface-type**: Interface type of subscriber.

- **S2bGTP**: Interface type S2b GTP.
- **S5S8GTP**: Interface type S5/S8 GTP.

**pgw-service svc_name**: Displays subscriber information based on the P-GW service name. **svc_name** must be an existing P-GW service expressed as an alphanumeric string of 1 through 63 characters.

**qci number**: Displays subscriber session information based on the QoS Class Identifier (QCI) value assigned to the subscriber. **number** must be an integer value from 0 to 9.

**sgw-address ip_address**: Displays subscriber information based on the S-GW IP address. **ip_address** must be an existing S-GW IP address.

**plmn-type [ home | roaming | visiting ]**

Displays subscriber information based on the type of Public Land Mobile Network (PLMN).

- **home**: For GGSN/PGW, shows all the subscribers of charging type HOME.
- **roaming**: For GGSN/PGW, shows all the subscribers of charging type ROAMING.
- **visiting**: For GGSN/PGW, shows all the subscribers of charging type VISITING.

The following filter keywords are valid with this command:
show subscribers

The following filter keywords are valid with this command:

- access-type, active-charging-service, all, apn, asn-peer-address, asngw-service, asnpc-service, bandwidth-policy, bearer-establishment, bng-service, callid, card-num, cbb-policy, ccoa-only, configured-idle-timeout, connected-time, dhcp-server, ebi, enodeb-address, epdg-address, fa, fa-service, firewall, fw-and-nat, ggsn-service, gprs-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, idle-time, imei, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, 13-tunnel-local-addr, 13-tunnel-remote-addr, lac, lac-service, lma-service, lns, lns-service, long-duration-time-left, mis-dup-tunnel-only, mipv6ha-service, msid, msisdn, nat, nemo-only, network-requested, network-type, pcf, pdsm-service, pdsn-service, profile-id, profile-name, qci, rx-data, sla-state, s5-proto, session-time-left, sgsn-address, sgw-address, smgr-instance, tx-data, username, grep, more

policy

Displays the current policies associated with the subscriber session.
The following filter keywords are valid with this command:

- access-type, active-charging-service, all, apn, asn-peer-address, asngw-service, asnpc-service, bandwidth-policy, bearer-establishment, bng-service, callid, card-num, cbb-policy, ccoa-only, configured-idle-timeout, connected-time, csclf-service, dhcp-server, domain, dormant, ebi, enodeb-address, epdg-address, fa, fa-service, firewall, fw-and-nat, ggsn-service, gprs-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-ipsec-only, ha-service, hnbgw-service, hsgw-service, idle-time, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, 13-tunnel-local-addr, 13-tunnel-remote-addr, lac, lac-service, lma-service, lns, lns-service, long-duration-time-left, mag-service, mis-dup-tunnel-only, mipv6ha-service, mme-address, mme-service, msid, msisdn, nat, nemo-only, network-requested, network-type, naapi, pcc-service, pcf, pdg-service, pdif-service, pdsm-service, pgw-address, pdsn-service, profile-id, profile-name, qci, rulebase, rx-data, sla-state, s5-proto, security-type, session-time-left, sgsn-address, sgw-address, smgr-instance, tx-data, ue-type, username, grep, more

profile-id id_number

Displays subscriber session information based on the profile-id granted for the flow. *id_number* must be an integer from 0 to 4294967295.

profile-name name

Displays subscriber session information based on an existing policy profile name expressed as an alphanumeric string of 1 through 63 characters.

qci number

Displays subscriber session information based on the QoS Class Identifier (QCI) value assigned to the subscriber. *number* must be an integer value from 0 to 9.
**rulebase name**
Displays subscriber session information based on the named Active Charging System rulebase. *name* must be an alphanumeric string of 1 through 63 characters.

**rx-data [ < | > | greater-than | less-than ] value**
The number of bytes received by the specified subscriber.
- **<**: Filters output so that only information less than the specified value is displayed.
- **>**: Filters output so that only information greater than the specified value is displayed.
- **greater-than**: Filters output so that only information greater than the specified value is displayed.
- **less-than**: Filters output so that only information less than the specified value is displayed.
- **value**: Used in conjunction with <, >, greater-than, less-than. If no other filtering options are specified only output matching value is displayed. If value is not specified all data is displayed. value must be an integer from 0 through 18446744073709551615.

**slu-state { active | idle | idle-active }**
Displays session information based on the subscriber’s S1-U state. The S1-U interface is the interface from the eNodeB to the S-GW.
- **active**: Displays session information for subscribers with an S1-U state set to active.
- **idle**: Displays session information for subscribers with an S1-U state set to idle.
- **idle-active**: Displays session information for subscribers with an S1-U state set to idle-active.

**s5-proto { gtp | pmip }**
Displays subscriber session information based on the S5 interface protocol used. This interface provides user plane tunneling and tunnel management between S-GW and P-GW. Choose either GPRS Tunneling Protocol (GTP) or Proxy Mobile IPv6 (PMIP).

**saegw-only**
Displays System Architecture Evolution Gateway (SAEGW) subscriber session information.
The following filters/keywords are valid with this command:

```
aaa-configuration, access-flows, active, active-charging-service, activity, all, apn, bandwidth-policy, bearer-establishment, bng-service, callid, card-num, cbb-policy, co-located, configured-idle-timeout, connected-time, counters, data-rate, dormant, ebi, enodeb-address, epdg-address, fa, firewall, full, fw-and-nat, gtp-version, gtpu-bind-address, gtpu-service, ha, idle-time, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, 13-tunnel-local-addr, 13-tunnel-remote-addr, lac-service, lma-service, lns, long-duration-time-left, mipv6ha-service, msid, nat, network-type, pgw-address, pgw-anchored, plmn-type, policy, profile-id, profile-name, qci, rulebase, rx-data, slu-state, s5-proto, saegw-service, session-time-left, sgw-address, sgw-anchored, smgr-instance, subscription, summary, tft, tx-data, username, wfi
```

- **co-located**: Shows only co-located subscribers which have both S-GW and P-GW functions.
- **pgw-anchored**: Shows only PGW-anchored subscribers.
● **saegw-service** *svc_name*: Displays subscriber information based on the SAEGW service name. *svc_name* must be an existing SAEGW service expressed as an alphanumeric string of 1 through 63 characters.

● **sgw-anchored**: Shows only SGW-anchored subscribers.

---

**saegw-service** *svc_name*

Displays subscriber information based on the SAEGW service name. *svc_name* must be an existing SAEGW service expressed as an alphanumeric string of 1 through 63 characters.

The following filters/keywords are valid with this command:

- active-charging-service
- apn
- bandwidth-policy
- bearer-establishment
- bng-service
- billid
- card-num
- cbb-policy
- configured-idle-timeout
- connected-time
- ebi
- enodeb-address
- epdg-address
- fa
- firewall
- fw-and-nat
- gtp-version
- gtpu-bind-address
- gtpu-service
- ha
- idle-time
- ims-auth-service
- imsi
- ip-address
- ip-aloc-method
- ip-pool
- ipv6-address
- ipv6-prefix
- l3-tunnel-local-addr
- l3-tunnel-remote-addr
- lac-service
- lma-service
- lns
- long-duration-time-left
- mipv6ha-service
- msid
- nat
- network-type
- pgw-address
- pimm-type
- profile-id
- profile-name
- qci
- rulebase
- rx-data
- slu-state
- s5-proto
- saegw-service
- session-time-left
- sgw-address
- smgr-instance
- tx-data
- username

---

**security-type** { ipsec | tls }

Displays subscriber information based on the specified type of security.

- **ipsec**: IPSec
- **tls**: Transport Layer Security

---

**session-time-left** [ < | > | greater-than | less ] *value*

How much session time is left for the specified subscriber.

- **<**: Filters output so that only information less than the specified value is displayed.
- **>**: Filters output so that only information greater than the specified value is displayed.
- **greater-than**: Filters output so that only information greater than the specified value is displayed.
- **less-than**: Filters output so that only information less than the specified value is displayed.

- **value**: Used in conjunction with <, >, greater-than, less-than. If no other filtering options are specified only output matching value is displayed. If value is not specified all data is displayed. value must be an integer from 0 through 4294967295.

---

**sgsn-address** *ipv4_address*

This SGSN-only keyword displays only subscriber context information for the specified interface. Must be followed by the IP address of the interface, using IPv4 dotted-decimal notation.

The following filter keywords are valid with this command:

- apn
- callid
- card-num
- connected-time
- idle-time
- gprs-service
- gsm-traffic-class
- gtp-version
- imsi
- msid
- msisdn
- nri
- nsei
- saegw-service
- smgr-instance
**sgsn-only**

This SGSN-only keyword displays only 3G SGSN-specific subscriber context information. The following filter keywords are valid with this command:

- aaa-configuration, active, active-charging-service, activity, all, apn, calid, card-num, configured-idle-timeout, connected-time, counters, data-rate, fa, full, ggsn-address, gsm-traffic-class, idle-time, imei, imsi, msid, partial, plmn-type, profile-name, rnc, rx-data, session-time-left, sgsn-service, summary, tx-data, wide-format, grep, more

**sgsn-service service_name**

For this SGSN-only keyword, enter the name of the configured 3G SGSN service to display subscriber information specific to the named SGSN service. The following filter keywords are valid with this command:

- apn, bearer-establishment, bng-service, calid, card-num, configured-idle-timeout, connected-time, ebi, enodeb-address, epdg-address, fa, firewall, fw-and-nat, gprs-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, idle-time, imei, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, long-duration-time-left, mipv6ha-service, msid, msisdn, nat, network-type, nri, plmn-type, profile-id, profile-name, qci, rx-data, slu-state, s1-u-proto, session-time-left, sgsn-service, sgw-address, summary, tx-data, username, grep, more

**sgw-address ip_address**

For this MME-only keyword, enter the IP address of the peer S-GW to display information about the subscribers connected to the specified S-GW. `ip_address` must be specified by its IP address using IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

**sgw-only**

Displays S-GW subscriber session information. The following filters/keywords are valid with this command:

- all, full, summary

- **sgw-service svc_name**: Displays subscriber information based on an existing S-GW service specified as an alphanumeric string of 1 through 63 characters.

- **pgw-address ip_address**: Displays subscriber information based on an existing P-GW specified by its IP address in IPv4 dotted-decimal notation.

**sgw-service svc_name**

Displays subscriber information based on an existing S-GW service specified as an alphanumeric string of 1 through 63 characters. The following filter keywords are valid with this command:

- epdg-address,
show subscribers

```
smgr-instance instance_id
```

Displays subscription information associated with the Session Manager identifier express as an integer from 1 through 4294967295.
The following filter keywords are valid with this command:

```
epdg-address,
```

```
subscription { aor address | callid id | full }
```

Displays subscription information for defined subscribers, based on defined parameters.
- `<aor address>`: Clears session(s) by Address of Record.
- `<callid id>`: Specifies a Call Identification Number as an 8-digit hexadecimal number.
- `<full>`: Displays all available information.

```
summary
```

Displays only a summary of the subscriber information. The following filter keywords are valid with this command:

```
access-type, active, active-charging-service, activity, all, asn-peer-address, asngw-service, asnpc-service, apn, bandwidth-policy, bearer-establishment, callid, card-num, ccb-policy, configured-idle-timeout, connected-time, dhcp-server, domain, dormant, ebi, enodeb-address, epdg-address, fa, fa-service, firewall, fw-and-nat, ggsn-service, gprs-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-service, hnbgw-service, hsgw-service, idle-time, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, lac, lac-service, lma-service, lns, lns-service, long-duration-time-left, mag-services, mme-address, mme-service, mseg-service, msid, mxisdn, nat, network-requested, network-type, pcc-service, pcf, pdg-service, pdif-service, pdsn-service, pgw-address, plmn-type, profile-id, qci, rulebase, rx-data, slu-state, s5-proto, security-type, session-time-left, sgsn-address, sgw-address, sgw-service, smgr-instance, tx-data, ue-type, username, grep, more
```

tft

Displays the current Traffic Flow Template (TFT) associated with the subscriber session.
The following filter keywords are valid with this command:

```
active, all, apn, asn-peer-address, asngw-service, asnpc-service, bearer-establishment, bng-service, callid, card-num, ccoa-only, configured-idle-timeout, connected-time, dhcp-server, dormant, ebi, enodeb-address, epdg-address, fa, fa-service, firewall, fw-and-nat, ggsn-service, gprs-service, gsm-traffic-class, gtp-version, gtpu-bind-address, gtpu-service, ha, ha-service, hnbgw-service, hsgw-service, idle-time, imei, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, 13-tunnel-local-addr, 13-tunnel-remote-addr, lac, lac-service, lma-service, lns, lns-service, long-duration-time-left, mag-service, mip-udp-tunnel-only, mipv6a-service, mme-address, mme-service, msid, mxisdn, nat, nemo-only, network-requested, network-type, pcf, pdg-service, pdif-service, pdsn-service, pgw-address, plmn-type, profile-id, profile-name, qci, rx-data, slu-state,
Exec Mode show Commands (Q-S)

show subscribers

- s5_proto, session-time-left, sgsn-address, sgw-address, sgw-service, smgr-instance, tx-data, username, grep, more

**tx-data [ < | > | greater-than | less-than ] value**

The number of bytes transmitted by the specified subscriber.
- `<` : Filters output so that only information less than the specified value is displayed.
- `>` : Filters output so that only information greater than the specified value is displayed.
- `greater-than` : Filters output so that only information greater than the specified value is displayed.
- `less-than` : Filters output so that only information less than the specified value is displayed.
- `value` : Used in conjunction with `<`, `>`, `greater-than`, `less-than`. If no other filtering options are specified, only output matching `value` is displayed. If `value` is not specified, all data is displayed. `value` must be an integer from 0 through 18446744073709551615.

The following filter keywords are valid with this command:

- epdg-address,

**ue-type { ims | non-ims }**

Displays information for the subscribers based on User Equipment type.
- `ims` : IP Multimedia Subsystem
- `non-ims` : UE other than IMS

The following filter keywords are valid with this command:

- access-type, active-charging-service, bandwidth-policy, bearer-establishment, callid, card-num, cbb-policy, configured-idle-timeout, connected-time, csrf-service, domain, ebi, enodeb-address, epdg-address, fa, fa-service, firewall, fw-and-nat, gprs-service, gtp-version, gtpu-bind-address, gtpu-service, ha, hnbgw-service, idle-time, ims-auth-service, imsi, ip-address, ip-alloc-method, ip-pool, ipv6-address, ipv6-prefix, l3-tunnel-local-addr, l3-tunnel-remote-addr, long-duration-time-left, msid, nat, network-type, pcc-service, profile-id, qci, rulebase, rx-data, slu-state, s5,proto, security-type, session-time-left, sgw-address, smgr-instance, tx-data, ue-type, username, grep, more

**username name**

Displays information for connections for the subscriber identified by `name`. The user must have been previously configured. `name` must be a sequence of characters and/or wildcard characters (`$` and `*`) from 1 to 127 characters. The `*` wildcard matches multiple characters and the `$` wildcard matches a single character. If you do not want the wildcard characters interpreted as a wildcard enclose them in single quotes ( `` ). For example; `'$'`. The following filter keywords are valid with this command:

- epdg-address,

**wf1**

Displays subscriber information in wide format number 1. Wide format number 1 includes the following information for each listed subscriber session:
- Access Type
show subscribers

- Access Technology
- Call State
- Link Status
- Network Type
- Call ID
- MSID
- Username
- IP Address
- Time-Idle
- Access Peer Address
- Service Address
- Network Peer Address
- Connect Time

The following filter keywords are valid with this command:

```
epdg-address,
```

**filter_keywords**

The following keywords are filters that modify or filter the output of the Command Keywords. Not all filters are available for all Command Keywords. Multiple Filter Keywords can be entered on a command line. When multiple Filter Keywords are specified, the output conforms to all of the Filter Keywords specifications.

For example; if you enter the following command:

```
show subscribers counters ip-pool pool1 card=num 1
```

Counters for all subscriber sessions that were assigned an IP address from the IP pool named pool1 and also are being processed by the processing card in slot 1 is displayed. Information for all other subscribers is not displayed.

**active**

Only display information for those subscribers who currently have active sessions.

**active-charging-service** *acs_service*

Displays information for subscribers being processed by the active charging service specified as an alphanumeric string of 1 through 15 characters.

**activity**

Displays subscriber link activity percentage.

**all**

If no keywords are specified before *all*, information for all subscribers is displayed. If keywords are specified before *all*, all information is displayed with no further options being allowed.

**apn** *name*

Displays subscribers currently facilitated by the access point name (APN) configured on the SGSN or GGSN.
Exec Mode show Commands (Q-S)

show subscribers

- **asngw-only**
  Displays counters for subscribers accessing the ASN-GW service only.

- **asnpc-only**
  Displays counters for subscribers accessing the ASN Paging Controller and Location Registry service only.

- **bandwidth-policy policy_name**
  Displays information for subscribers associated with the specified Active Charging bandwidth policy.

- **bearer-establishment { direct-tunnel | normal | pending } id**
  Displays subscriber information for selected bearer establishment type.

- **bng-service srvc_name**
  Displays the current configuration for the specified Broadband Network Gateway (BNG) service.

- **callid id**
  Displays subscriber information for the call ID specified as an 8-byte hexadecimal number.

- **card-num card_num**
  The slot number of the processing card by which the subscriber session is processed. The slot number is an integer from 1 through 7 and 10 through 16 on the ASR 5000, or 1 through 4 and 7 through 10 on the ASR 5500.

- **cbb-policy policy_name**
  Displays information for subscribers associated with the specified Active Charging Content Based Billing (CBB) policy.

- **ccoa-only**
  Displays the subscribers that registered a MIP with CoA directly with the HA. This option is only valid when a MIPHA session license is enabled.

- **configuration { all | username name }**
  Displays current configuration for all subscribers or a specified subscriber.

- **configured-idle-timeout [ < | > | greater-than | less-than ] value**
  Shows the idle timeout that is configured for the specified subscriber. A value of 0 (zero) indicates that the subscribers idle timeout is disabled.

  - `<`: Filters output so that only information less than the specified value is displayed.
  - `>`: Filters output so that only information greater than the specified value is displayed.
  - `greater-than`: Filters output so that only information greater than the specified value is displayed.
  - `less-than`: Filters output so that only information less than the specified value is displayed.

  *value*: Used in conjunction with `<`, `>`, `greater-than`, `less-than`. If no other filtering options are specified only output matching value is displayed. If value is not specified all data is displayed. value must be an integer from 0 through 4294967295.
**connected-time [ < | > | greater-than | less-than ] value**

Shows how long the subscriber has been connected. `<`: Filters output so that only information less than the specified value is displayed.

- `<=`: Filters output so that only information less than or equal to the specified value is displayed.
- `>=`: Filters output so that only information greater than or equal to the specified value is displayed.
- `>`: Filters output so that only information greater than the specified value is displayed.
- `>=`: Filters output so that only information greater than the specified value is displayed.
- `value`: Used in conjunction with `<`, `>`, `greater-than`, `less-than`. If no other filtering options are specified only output matching `value` is displayed. If `value` is not specified all data is displayed. `value` must be an integer from 0 through 4294967295.

**counters keyword**

Displays the specified counter for the subscribers.

**cpu-num number**

Displays information for calls processed through the specified CPU number.

**cscf-only**

Displays information for Call Session Control Function (CSCF) subscribers only.

**cscf-service service_name**

Displays information for subscribers accessing an existing CSCF service specified as an alphanumeric string of 1 through 63 characters.

**dhcp-server address**

Displays subscribers currently accessing the system that have been provided an IP address by the DHCP server specified by its address. GGSN only.

**dns-proxy**

Displays all subscribers associated with a DNS proxy.

**domain name**

Displays all subscribers with an Address-of-Record (AoR) from the specified domain. `name` is an alphanumeric string of 1 through 79 characters.

**dormant**

Shows information for subscriber sessions that are dormant (not transmitting or receiving data).

**dormant**

Shows information for subscriber sessions that are dormant (not transmitting or receiving data).

**ebi number**

Displays subscribers based on an EPS bearer identity number.
show subscribers

**enodeb-address ip_address**
Displays subscribers based on the eNodeB to which they are attached.

**fa address**
Displays information for subscribers connected to the foreign agent specified by its IP address in IPv4 dotted-decimal notation.

**fa-only**
Only display FA-specific context information.

**fa-service name**
Displays information for subscribers connected to the named foreign agent (FA) service.

**firewall { not-required | required }**
Displays information for the specified subscribers:
- **not-required**: Subscribers for whom firewall processing is not required.
- **required**: Subscribers for whom firewall processing is required.

**firewall-policy fw_policy_name**
This keyword is obsolete.

**full**
Displays all available information for subscribers.

**fw-and-nat policy fw_nat_policy**

**Important**: This option is customer-specific and is only available in StarOS 8.1.

Displays information for subscribers using an existing Firewall-and-NAT policy specified as an alphanumeric string of 1 through 15 characters.

**ggsn-address ip_address**
Displays information for subscribers connected to an existing GGSN specified by its IP address in IPv4 dotted-decimal notation. SGSN only

**ggsn-preservation-mode**
Displays information for subscribers connected to the GGSN service with preservation mode enabled. GGSN only.

**ggsn-service name**
Displays information for subscribers connected to the named GGSN service. This keyword is for GGSN only.

**gprs-only**
Displays only 2G SGSN subscribers content. SGSN only.


**show subscribers**

- **gprs-service**  `srvc_name`
  Displays subscriber information for the named 2G GPRS service. SGSN only.

- **gsm-traffic-class** `{ background | conversational | interactive | streaming }`
  Displays information for subscriber traffic that matches the specified 3GPP traffic class.
  - **background**: 3GPP QoS background class.
  - **conversational**: 3GPP QoS conversational class.
  - **interactive**: 3GPP QoS interactive class. Must be followed by a traffic priority.
  - **streaming**: 3GPP QoS streaming class.

- **ha**  `address`
  Displays information for subscribers connected to the home agent specified by its IP address in IPv4 dotted-decimal notation.

- **ha-ipsec-only**
  Only displays information for subscriber sessions that are using IP-Security (IPSec).

- **ha-only**
  Only displays HA-specific context information.

- **ha-service**  `name`
  Displays information for subscribers connected to the named home agent service.

- **hnbgw-only**
  Displays counters for subscribers accessing the Home evolved NodeB Gateway (HNB-GW) service only.

- **idle-time** `{ < | > | greater-than | less-than } value`
  Displays how long the subscriber session has been idle or display subscriber sessions that meet the idle time criteria specified.
  - `<`: Filters output so that only information less than the specified value is displayed.
  - `>`: Filters output so that only information greater than the specified value is displayed.
  - `greater-than`: Filters output so that only information greater than the specified value is displayed.
  - `less-than`: Filters output so that only information less than the specified value is displayed.
  - `value`: Used in conjunction with `<`, `>`, greater-than, less-than. If no other filtering options are specified only output matching `value` is displayed. If `value` is not specified all data is displayed. `value` must be an integer from 0 through 4294967295.

- **imei**  `imei_number`
  Displays information for subscribers having the specified International Mobile Equipment Identity (IMEI/IMEISV) number.

- **ims-auth-service**  `service_name`
  Displays information for subscribers for an existing IMS Authorization Service name.
Exec Mode show Commands (Q-S)

show subscribers

imsi id
Displays the subscriber with the specified ID. The IMSI (International Mobile Subscriber Identity) ID is a 15-character string which identifies the subscriber’s home country and carrier. Wildcard characters $ and * are allowed. The * wildcard matches multiple characters and the $ wildcard matches a single character. If you do not want the wildcard characters interpreted as a wildcard enclose them in single quotes (’). For example; ‘$’.

ip-address [ < | > | greater-than | less-than ] address
Displays information for subscribers connected to the specified address.
 • <: Filters output so that only information for subscribers with an IP address lower than the specified address is displayed.
 • >: Filters output so that only information for subscribers with an IP address higher than the specified address is displayed.
 • greater-than: Filters output so that only information for subscribers with an IP address higher than the specified address is displayed.
 • less-than: Filters output so that only information for subscribers with an IP address lower than the specified address is displayed.
 • address: The address must be specified using IPv4 dotted-decimal notation. Used in conjunction with <, >, greater-than, less-than. If the IP address is specified without a qualifier, only subscribers with the specified IP address have their information displayed.

ip-alloc-method { aaa-assigned | dhcp [ relay-agent | proxy-client ] | dynamic-pool | l2tp-lns-assigned | mip-ha-assigned | ms-provided-static | not-ms-provided-static | static pool }
Displays the specific IP Allocation Method. Must be followed by one of the IP Allocation Methods:
 • aaa-assigned: Selects subscribers whose IP addresses were assigned by AAA.
 • dhcp: Selects subscribers whose IP addresses were assigned by DHCP.
   • relay-agent: Selects subscribers whose IP addresses were assigned by the DHCP Relay Agent
   • proxy-client: Selects subscribers whose IP addresses were assigned by the DHCP Proxy Client
 • dynamic-pool: Selects subscribers whose IP addresses were assigned from a dynamic IP address pool.
 • l2tp-lns-assigned: Selects subscribers whose IP addresses were assigned by the Layer 2 Tunneling Protocol (L2TP) Network Server.
 • mip-ha-assigned: Selects subscribers whose IP addresses were assigned by the Mobile IP Home Agent.
 • ms-provided-static: Selects subscribers whose IP addresses were provided by the Mobile Station.
 • not-ms-provided-static: Selects subscribers whose IP addresses were not provided by the Mobile Station.
 • static-pool: Selects subscribers whose IP addresses were assigned from a static IP address pool.
ip-pool name
Displays information for subscribers assigned addresses from an existing IP address pool or IP pool group.
name will be an IP address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation based on the call line setup for the specified pool.

ipv4
Displays information for subscribers with an IPv4 Firewall enabled/disabled.

ipv6
Displays information for subscribers with an IPv6 Firewall enabled/disabled.

ipv6-address address
Displays information for subscribers connected to the specified IPv6 address.

ipv6-prefix prefix
Displays information for subscribers connected to the specified IPv6 address prefix.

l3-tunnel-local-addr ip_address
A layer 3 tunneling interface specified by its IP address in IPv4 dotted-decimal notation.

l3-tunnel-remote-addr ip_address
A layer 3 tunneling peer specified by its IP address in IPv4 dotted-decimal notation.

lac address
Displays information for calls to the peer L2TP Access Concentrator (LAC) specified by its IP address.

lac-only
Displays LAC specific information only.

lac-service name [ local-tunnel-id id | remote-tunnel-id id ]
Displays information for calls associated with the LAC service specified as an alphanumeric string of 1 through 63 characters.

*local-tunnel-id id: Specifies a local tunnel from which to clear calls as an integer from 1 through 65535.
*remote-tunnel-id id: Specifies a remote tunnel from which to clear calls as an integer from 1 through 65535.

lns address
Displays information for calls to the peer L2TP Network Server (LNS) specified by its IP address.

lns-only
Displays LNS specific information only.
**lns-service name [ local-tunnel-id id | remote-tunnel-id id ]**

Displays information for calls associated with the LNS service specified as an alphanumeric string of 1 through 63 characters.

- **local-tunnel-id id**: Indicates a specific local tunnel from which to clear calls. *id* must be an integer from 1 through 65535.
- **remote-tunnel-id id**: Indicates a specific remote tunnel from which to clear calls. *id* must be an integer from 1 through 65535.

**local-tunnel-id identifier**

Displays information for a local tunnel identifier specified as an integer from 1 to 65535.

**long-duration-time-left [ < | > | greater-than | less-than ] value**

Shows how much time is left for the maximum duration of a specified subscriber session.

- **<**: Filters output so that only information less than the specified value is displayed.
- **>**: Filters output so that only information greater than the specified value is displayed.
- **greater-than**: Filters output so that only information greater than the specified value is displayed.
- **less-than**: Filters output so that only information less than the specified value is displayed.

- **value**: Used in conjunction with <, >, greater-than, less-than. If no other filtering options are specified only output matching value is displayed. If value is not specified all data is displayed. *value* must be an integer from 0 through 4294967295.

**mag-only**

Displays Mobile Access Gateway (MAG) subscriber session information.

**mag-service svc_name**

Displays subscriber information based on the Mobile Access Gateway (MAG) service name. *svc_name* must be an existing MAG service expressed as an alphanumeric string of 1 through 63 characters.

**mip-udp-tunnel-only**

Displays the subscribers that negotiated MIP-UDP tunneling with the HA.

This option is only valid when MIP NAT Traversal license is enabled.

**mipv6ha-only**

Displays MIPV6HA-specific context information for the session.

**mipv6ha-service service_name**

Displays specific configured MIPV6 Home Agent service. *service_name* must have been previously defined.

**msid id**

Displays information for the mobile user identified by *id*. *id* must be from 7 to 16 hexadecimal digits specified as an IMSI, MIN, or RMI. Wildcard characters $ and * are allowed. The * wildcard matches multiple characters and the $ wildcard matches a single character. If you do not want the wildcard characters interpreted as a wildcard enclose them in single quotes (‘ ’). For example: ‘$’.
In case of **enforce imsi-min equivalence** is enabled on the chassis and MIN or IMSI numbers supplied, this filter will show subscribers with a corresponding MSID (MIN or IMSI) whose lower 10 digits matches to lower 10 digits of the supplied MSID.

```
show subscribers msid ABCD0123456789 or
show subscribers msid 0123456789
```

will show any subscriber with a MSID that match the lower 10 digits of MSID supplied, for example, 0123456789.

**msisdn msisdn**

Displays information for the mobile user identified by the Mobile Subscriber ISDN Number (MSISDN). *msisdn* must be 7 to 16 digits; specified as an IMSI, MIN, or RMI.

**nat { not-required | required }**

Displays information for the specified subscribers.

- **not-required**: Subscribers for whom Network Address Translation (NAT) processing is not required.
- **required**: Subscribers for whom NAT processing is required.

**nat-ip nat_ip_address**

Displays information for the subscribers for whom NAT processing is enabled and are using the specified NAT IP address. *nat_ip_address* specifies the NAT IP address and must be in IPv4 dotted-decimal notation. **The nat-ip keyword is only available in StarOS 8.3 and later releases.**

**nat-realm nat_realm**

Displays information for the subscribers for whom NAT processing is enabled and are using the specified NAT realm. *nat_realm* specifies the NAT realm name and must be a string from 1 through 63 characters.

**network-requested**

Display information for currently active subscribers whose sessions were initiated by the GGSN network requested create PDP context procedure.

**network-type { gre | ipip | ipsec | ipv4 | ipv4-pmipv6 | ipv4v6 | ipv4v6-pmipv6 | ipv6 | ipv6-pmipv6 | l2tp | mobile-ip | proxy-mobile-ip }**

Selects the currently active subscribers based on network service access type.

- **gre**: Generic Routing Encapsulation
- **ipip**: IP-in-IP
- **ipsec**: IPSec
- **ipv4**: IPv4 only
- **ipv4-pmipv6**: IPv4 and/or Proxy Mobile IPv6 (PMIP)
- **ipv4v6**: IPv4 and/or IPv6
- **ipv4v6-pmipv6**: IPv4, IPv6 and/or Proxy Mobile IPv6
- **ipv6**: IPv6 only
- **ipv6-pmipv6**: IPv6 and/or Proxy Mobile IPv6 (PMIP)
- **l2tp**: Layer 2 Tunneling Protocol
- **mobile-ip**: Mobile IP (MIP)
show subscribers

•proxy-mobile-ip: Proxy Mobile IPv6 (PMIP)

nri nri_value
This SGSN-specific filter uses the configured network resource identifier (NRI) to identify a specific SGSN in a pool to fine-tuned the subscriber information to be displayed.

nri_value: enter an integer from 0 through 63
This filter can be used in combination with further refining filters.

nsapi nsap_id
Displays session information for the mobile user identified by Network Service Access Point Identifier (NSAPI) between MS and SGSN. NSAPI is also used as part of the tunnel identifier between GPRS Support Nodes (GSNs). The user identity IMSI and the application identifier (NSAPI) are integrated into the Tunnel IDentifier (GTPv0) (TID) or Tunnel Endpoint Identifier (GTPv1) (TEID) that uniquely identifies the subscriber’s sublink between the GSNs (SGSN and GGSN). The NSAPI is an integer value within the PDP context header.

nsap_id must be an integer from 5 through 15.

partial qos { negotiated | requested }
This filter is specific to the SGSN.
It limits the display of information to requested or negotiated QoS information for the subscriber.
This filter can be used in combination with further defining filters: active, active-charging-service, all, apn, callid, card-num, configured-idle-timeout, connected-time, ggsn-address, gprs-service, gsm-traffic-class, idle-time, imsi, msid, msisdn, negotiated, plmn-type, requested, rx-data, session-time-left, tx-data

pcc-service name
Displays statistics for users associated with an existing Policy and Charging Control (PCC) service name expressed as an alphanumeric string of 1 through 63 characters.

pcf [ < | > | less-than | greater-than] ipv4_address [ < | > | less-than | greater-than ] ipv4_address ]
Displays information for subscribers connected via the packet control function with a specific or range of IP addresses. The address must be specified using IPv4 dotted decimal notation.

•<: Filters output so that only information less than the specified IPv4 address value is displayed.
•>: Filters output so that only information greater than the specified IPv4 address value is displayed.
•less-than: Filters output so that only information less than the specified IPv4 address value is displayed.
•greater-than: Filters output so that only information greater than the specified IPv4 address value is displayed.

Note: It is possible to define a limited range of IP addresses by using the less-than and greater-than options to define minimum and maximum values.

pdsn-only
Show PDSN specific information only.

pdsn-service name
Displays information for subscribers connected to the packet data service name. The packet data service must have been previously configured.
plmn-type
Displays subscriber type (HOME, VISITING, or ROAMING).
This keyword is for the GGSN or the SGSN only.

policy
Displays the current policies associated with the subscriber session.

profile-id id_number
Displays subscriber session information based on the profile-id granted for the flow. id_number must be an integer from 0 to 4294967295.

profile-name profile_name
Displays the subscribers filtered with PCC profile named profile_name in particular IP-CAN session.

qci number
Displays subscriber session information based on the QoS Class Identifier (QCI) value assigned to the subscriber. number must be an integer value from 0 to 9.

relay-agent
Selects subscribers whose IP Addresses were assigned by the DHCP Relay Agent.

remote-tunnel-id identifier
Displays information for a remote tunnel identifier specified as an integer from 1 to 65535.

rnc id rnc_id mcc mcc_num mnc mnc_num
Displays information for subscribers connected to the SGSN via a specific RNC (radio network controller) identified by the RNC ID, the MCC (mobile country code), and the MNC (mobile network code). SGSN only

rulebase name
Selects subscribers associated with the specified Active Charging rulebase.

rx-data [ < | > | greater-than | less-than ] value
The number of bytes received by the specified subscriber.
• <: Filters output so that only information less than the specified value is displayed.
• >: Filters output so that only information greater than the specified value is displayed.
• greater-than: Filters output so that only information greater than the specified value is displayed.
• less-than: Filters output so that only information less than the specified value is displayed.
• value: Used in conjunction with <, >, greater-than, less-than. If no other filtering options are specified only output matching value is displayed. If value is not specified all data is displayed. value must be an integer from 0 through 18446744073709551615.

saegw-only
Displays System Architecture Evolution Gateway (SAEGW) subscriber session information only.
show subscribers

**saegw-service svc_name**
Displays subscriber information based on the SAEGW service name.
*svc_name* must be an existing SAEGW service expressed as an alphanumeric string of 1 through 63 characters.

**security-type { ipsec | tls }**
Displays subscriber information based on the specified type of security.
- **ipsec**: IPSec
- **tls**: Transport Layer Security

**session-time-left [ < | > | greater-than | less ] value**
How much session time is left for the specified subscriber.
- **<**: Filters output so that only information less than the specified value is displayed.
- **>**: Filters output so that only information greater than the specified value is displayed.
- **greater-than**: Filters output so that only information greater than the specified value is displayed.
- **less-than**: Filters output so that only information less than the specified value is displayed.
- **value**: Used in conjunction with <, >, greater-than, less-than. If no other filtering options are specified only output matching *value* is displayed. If *value* is not specified all data is displayed. *value* must be an integer from 0 through 4294967295.

**smgr-instance number**
Specific sessmgr instance. *number* must be in the range of 1 to 4294967295.

**sgsn-address address**
Shows information for subscribers whose PDP contexts are currently being facilitated by the SGSN specified by address. This command is for GGSN only.

**sgsn-service srvc_name**
Shows subscriber information for a specified 3G SGSN service. *srvc_name* must be an alphanumeric string of 1 through 63 characters that identifies a configured SGSN service. This command is for SGSN only.

**subscription { aor address | callid id | full }**
Displays subscription information for defined subscribers, based on defined parameters.
- **aor address**: Clears session(s) by Address of Record.
- **callid id**: Specifies a Call Identification Number as an 8-digit hexadecimal number.
- **full**: Displays all available information.

**tft**
Displays the current Traffic Flow Template (TFT) associated with the subscriber session.

**tx-data [ < | > | greater-than | less-than ] value**
The number of bytes transmitted by the specified subscriber.
• `<`: Filters output so that only information less than the specified value is displayed.
• `>`: Filters output so that only information greater than the specified value is displayed.
• `greater-than`: Filters output so that only information greater than the specified value is displayed.
• `less-than`: Filters output so that only information less than the specified value is displayed.
• `value`: Used in conjunction with `<`, `>`, greater-than, less-than. If no other filtering options are specified only output matching `value` is displayed. If `value` is not specified all data is displayed. `value` must be an integer from 0 through 18446744073709551615.

```
ue-type { ims | non-ims }
```

Displays information for the subscribers based on User Equipment type.

• `ims`: IP Multimedia Subsystem
• `non-ims`: UE other than IMS

```
username name
```

Displays information for connections for the subscriber identified by `name`. The user must have been previously configured. `name` must be a sequence of characters and/or wildcard characters ("$" and "*") from 1 to 127 characters. The * wildcard matches multiple characters and the $ wildcard matches a single character. If you do not want the wildcard characters interpreted as a wildcard enclose them in single quotes (‘) For example; ‘$’.

```
verbose
```

Display detailed information.

```
wide-format
```

Display detailed information in a wider screen format.

```
| { grep grep_options | more }
```

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the `grep` and `more` commands, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

**Usage**

Use this command to view information about subscriber sessions. The output of this command may be considered for part of a periodic system auditing program by verifying active and dormant subscribers. The Command Keywords may be used standalone to display detailed information or you may use one or more of the various Filter Keywords to reduce the amount of information displayed.

**Caution:** Executing this command may negatively impact performance if multiple instances are executed while the system is under heavy load and simultaneously facilitating multiple CLI sessions.

**Example**

The following command displays information for all subscriber sessions:
show subscribers all
The following command displays information for all ggsn-only subscriber sessions:
    show subscribers ggsn-only all
The following command displays information for all subscriber sessions in wide format 1:
    show subscribers wfl all
    show subscribers aaa-configuration
    show subscribers counters username ispluser1
The following command displays information for subscriber in GGSN service:
    show subscribers ggsn-only allshow subscribers ggsn-only full
The following command displays information for all subscriber with SGSN session having partial QoS requests:
    show subscribers sgsn-only partial qos requested
The following command displays information for all subscriber with MME session connected to MME service having IP address as 10.1.1.1:
    show subscribers mme-only mme-address 10.1.1.1

Important: Output descriptions for commands are available in the Statistics and Counters Reference.
show subscribers samog-only

Displays SaMOG specific context information for the session.

**Product**
SaMOG

**Privilege**
Inspector

**Syntax**

```
show subscribers samog-only [ [ all ] [ callid call_id ] [ card-num card_num ] [ connected-time [ < | > | greater-than | less-than ] connected_time ] [ full ] [ idle-time [ < | > | greater-than | less-than ] idle_time ] [ ip-address [ < | > | greater-than | less-than ] ipv4_address ] [ ipv6-prefix ipv6_prefix ] [ network-type { gre | ipip | ipsec | ipv4 | ipv4-pmipv6 | ipv4v6 | ipv4v6-pmipv6 | ipv6 | ipv6-pmipv6 | l2tp | mobile-ip | proxy-mobile-ip } ] [ session-time-left [ < | > | greater-than | less-than ] session_time_left ] [ smgr-instance smgr_instance ] [ summary ] [ username user_name ] [ | { grep grep_options | more } ]
```

**idle-time [ < | > | greater-than | less-than ] idle_time**

Displays how long the subscriber has been idle.

> and **greater-than** Specifies greater than. This must be followed by `idle_time`, an integer ranging from 0 and 4294967295.

< and **less-than** Specifies less than. This must be followed by `idle_time`, an integer ranging from 0 and 4294967295.

**ipv6-prefix ipv6_prefix**

Displays the subscribers associated with the specified IPv6 address prefix. Must be followed by an IPv6 address prefix in the format `xx:xx:xx::/len`

| [ grep grep_options | more } ]

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.

For details on using the `grep` and `more` commands, refer to the `Regulating a Command's Output` section of the Command Line Interface Overview chapter.
show subscribers wsg-service

Displays information for specific configured WSG service. This command must be followed by the WSG service name.

**Product**
SecGW (WSG)

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Mode**
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

**Syntax**

```bash
show subscribers wsg-service service_name [ | { grep grep_options | more } ]
```

*service_name*

Specifies the name of the WSG service as an alphanumeric string of 1 through 63 characters.

**Usage**

Use this command to displays information about selected WSG calls and services.

**Example**

The following command displays counter information for wsg-service wsg01:

```bash
show subscribers wsg-service wsg01 arg1
```
show super-charger

Lists subscribers with valid super-charger configuration. When super-charger is enabled for a subscriber, the SGSN handles 2G or 3G connections controlled by an operator policy and changes hand-off and location update procedures to reduce signaling traffic management (3GPP, TS.23.116).

Product
SGSN

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show super-charger { imsi imsi | all }

imsi
Defines a specific subscriber’s international mobile subscriber identity (IMSI) number.
imsi is a string of up to 15 digits that includes the MCC (mobile country code), the MNC (mobile network code) and the MSIN (mobile station identification number),

all
Instructs the SGSN to display super charger subscription information for all subscribers.

Usage

Use this command to determine if a single subscriber, identified by the IMSI, has a super charger configuration. Also, this command can display the list of all subscribers with a super charger configuration. If a subscriber has super charger as part of the configuration, subscriber data is backed up (using the IMSI Manager) after the subscriber detaches and the purge timer expires.

Example

The following command displays the super charger configuration information for the subscriber identified by the IMSI 90121882144672.

    show super-charger imsi 90121882144672
show supplementary-service statistics

Displays the statistics for Supplementary Service Information.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator, Operator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
show supplementary-service statistics
```

**Usage**
Use this command to display the Supplementary Service Information.

**Example**
The following command displays the Supplementary Service Information:

```
show supplementary-service statistics
```
show support collection

Displays information about when and where the Support Data Collector (SDC) stores its Support Data Record (SDR) files.

Product
All

Privilege
All

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show support collection [ definitions ] [ ! { grep grep_options | more } ]

definitions
Displays the list of default support record section definitions. This is the list of all valid record section definitions. The display also indicates whether the record section is enabled or disabled by default.

| ! { grep grep_options | more }

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.

For details on using the grep and more commands, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage

Use this command to display the status of SDR collection, collection times, SDR file names and sizes, as well as the date/time the files were written. If SDR collection has occurred this command displays the pathname where the files have been stored.

With the definitions option this command lists existing record sections and their associated CLI commands.

For additional information, refer to the descriptions of the support collection and support record commands in the Global Configuration Mode (L - S) Commands chapter. Also see the System Administration Guide.

Example

The following command displays the SDR collection information.

show support collection
show support details

Displays a comprehensive list of system information that is useful for troubleshooting purposes. In most cases, the output of this command is requested by the Technical Assistance Center (TAC).

**Important:** To improve output performance when executing the `show cli history` command, this command displays the `config` command but not the individual CLI commands within the config file.

**Product**
All

**Privilege**
All

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
show support details [ to file url] [ compress ] [ | { grep grep_options | more } ]
```

**to file url**

Specifies the location where a .tar file with the support detail information should be created. *url* may refer to a local or a remote file and must be entered using the following format:

For the ASR 5000:

```
```

```
tftp:// { host [ :port# ] } [ /directory ] /file_name
```

```
```

For the ASR 5500:

```
```

```
tftp:// { host [ :port# ] } [ /directory ] /file_name
```

```
```

**Important:** Do not use the following characters when entering a string for the field names below: “/” (forward slash), “:” (colon) or “@” (at sign).

```
directory is the directory name.
```
filename is the actual file of interest.
username is the user to be authenticated.
password is the password to use for authentication.
host is the IP address or host name of the server.
port# is the logical port number that the communication protocol is to use.
If the filename is not specified with a .tar extension, it is automatically appended to the filename when the file is created and a message is generated.
The content of the tar file is:
   • support_summary - An ASCII text file that contains the support detail information.
   • information.minicores.tar - A tar file that contains any minicore files found on the system. Minicore files contain memory core dumps that are captured during some events. These core dumps provide specific memory locations and other information about the event. This information is useful to the technical support team in identifying where and when an event occurred along with its probable cause.

compress
Generates a compressed .tar.gz file for the output of the command.

| { grep grep_options | more }

Pipes (sends) the output of this command to a specified command. You must specify a command to which the output of this command will be sent.
For details on using the grep and more commands, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage
Use this command to obtain extensive system information for use in troubleshooting. This command does the work of over 30 separate commands, which saves time and ensures that all of the information needed is collected and displayed in the same order every time.
In addition to the information provided, the show support details command includes information that is not otherwise accessible to users but that is helpful in the swift resolution of issues.

Example
The following command displays the system information on your console.

```
show support details
```

The following command displays the information on your console and also writes it to the local device (pcmcia1 in this case) and includes the mini core dumps, using the filename r-p_problem.tar:

```
show support details to file /pcmcia1/r-p_problem.tar
```

The following command displays the information on your console and also writes it to an FTP server (named host), placing the file in the dir directory and includes the mini core dumps, using the filename re_problem.tar:

```
show support details to file ftp://host/dir/re_problem.tar
```
show support record

Displays the output of one or more Support Data Records (SDRs) previously saved by the Support Data Collector (SDC). SDRs are displayed in the order of lowest record-id to highest record-id.

Product
All

Privilege
All

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show support record  
record-id [ to record-id ] [ section section_name ] [ | { grep grep_options | more } ]

record-id
Specifies a record-id as an integer from 0 through 65536.
Each SDR is identified by a time index called the record-id. For example, the most recent record is always
record-id 0 (filename = sdr.0.gz). The next older record is record-id 1 (filename = sdr.1.gz), and so on.
When a new record is collected it is given a record-id of 0. The previously most recent record is renamed to
record-id 1, and so on. The display includes the record-id along with the collection time-stamp.

to record-id
Specifies a the end point of a range of record-ids as an integer from 0 through 65536.

section section_name
Specifies the name of an existing record section as an alphanumerical string of 1 through 64 characters.

| { grep grep_options | more }

Pipes (sends) the output of this command to a specified command. You must specify a command to which the
output of this command will be sent.
For details on using the grep and more commands, refer to the Regulating a Command’s Output section of
the Command Line Interface Overview chapter.

Usage

Use this command to display the output of one or more SDRs. This information is a useful troubleshooting
tool when data is compared chronologically across several SDRs. For additional information refer to the
System Administration Guide.

Example

The following command displays the SDRs from 2 through 4:

   show support record 2 to 4
show system uptime

Displays the amount of time the system has been operational since its last down time (maintenance or otherwise).

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show system uptime [ | { grep grep_options | more } ]

uptime
Displays system up time in days (D), hours (H) and minutes (M).

| { grep grep_options | more }

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the grep and more commands, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage
Display the system up time to check for the possibility of anomalous behavior related to shorter or longer up times.

Example
The following command displays basic system basic information and up time.

    show system uptime
Chapter 132
Exec Mode show Commands (T-Z)

This chapter includes the commands show tacacs through show version.
The Exec Mode is the initial entry point into the command line interface system. Exec mode show commands are useful in troubleshooting and basic system monitoring.

Mode

Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
show tacacs

Displays information about all active Terminal Access Controller Access-Control System Plus (TACACS+) sessions.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show tacacs [ client | priv-lvl | session | summary ] [ | { grep grep_options | more } ]

show tacacs

This command provides the following TACACS+ information:

- Individual active session number with the following additional session-specific information:
  - login username
  - login tty
  - time of login
  - login server priority
  - current session state
  - current privilege level
  - remote client application (if applicable)
  - remote client ip address (if applicable)
  - last server reply status

- Total number of TACACS+ sessions

[ client | priv-lvl | session | summary ]

Optional filters are available for the output of the show tacacs command:

- **client** – Display information about the TACACS+ client.
- **priv-lvl** – Display TACACS+ priv-level authorization attributes for StarOS administrative levels.
- **session** – Display information about the TACACS+ sessions.
- **summary** – Display summary information about the TACACS+ sessions.
show tacacs

| { grep grep_options | more }

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of the `grep` and `more` commands, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter.

### Usage

Use this command to view detailed session information for all active TACACS+ sessions.

### Important:  This command is available on version 11.0 and later systems.

### Example

```
show tacacs
```
show task

Displays information about system tasks.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

```
show task { info | memory | resources | table } [ card card_num ] [ facility facility { all | instance id } ] [ process process_name all ] [ max ] [ | { grep grep_options | more } ] { info | memory | resources | table }
```

Specifies the type of information to be displayed and scope of tasks to include in output.

- `info`: Displays detailed task information.
- `memory`: Displays detailed task memory usage information.
- `resources`: Displays resource allocation and usage information for all tasks.
- `table`: Displays identification information in tabular format for all tasks.

```
card card_num
```

Default: all powered on cards.

Specifies a single card for which task information is to be displayed where `card_num` must be an integer from 1 to 48 for the ASR 5000 and 1 through 20 for the ASR 5500.

```
facility facility { all | instance id max }
```

Default: all facilities.

Specifies the list of facilities for which task information may be displayed. A specific instance of the facility may be displayed as specified by ID or all instances may be displayed. The value of `id` must be an integer from 0 through 10000000. `facility` must be one of:

- `a11mgr`: A11 Interface Manager facility
- `aaamgr`: AAA Manager Facility
- `aaaproxy`: AAA Proxy manager Facility
- `acctrl`: Active Charging Service (ACS) Controller Facility [Release 11.0 and earlier versions only]
- `acsmgr`: Active Charging Service (ACS) Manager Facility
- `afctrl`: Fabric Manager [ASR 5500 only]
- `afmgr`: Fabric Manager [ASR 5500 only]
- `alcapmgr`: ALCAP Manager
• **asngwmgr**: ASN Gateway Manager
• **asnpermgr**: ASN Paging/Location-Registry (ASN-PC) Manager
• **bdf**: Bidirectional Forwarding Detection
• **bgp**: Border Gateway Protocol (BGP) Facility
• **bngmgr**: BNG Manager
• **bulkstat**: Bulk Statistics Manager Facility
• **callhome**: Call Home Controller
• **cdrmod**: Charging Detail Record Module
• **cli**: Command Line Interface Facility
• **conproxy**: Proxy for connections from same card/chassis
• **cscfcpmgr**: CSCFCPMGR Logging Facility
• **cscfmg**: SIP CSCF Manager
• **cscftm**: SIP CSCFTT Manager
• **cspctrl**: Card Slot Port controller Facility
• **cssctrl**: Content Service Steering Controller
• **dcardct**: IPSec Daughter-card Controller Logging Facility
• **dcardmg**: IPSec Daughter-card Manager Logging Facility
• **dgmbmgr**: Diameter Gmb Application Manager
• **dhmgr**: Distributed Host Manager
• **diamproxy**: Diameter Proxy
• **drvctrl**: Driver Controller Facility
• **egtpegmgr**: EGTP Egress Demux Manager
• **egtpinmgr**: EGTP Ingress Demux Manager
• **evlogd**: Event Log Daemon Facility
• **famgr**: Foreign Agent Manager Facility
• **gtpcmgr**: GTP-C Protocol Logging facility (GGSN product only)
• **gtpum**: GTP-U Demux Manager
• **h248prt**: H.248 Protocol Task [Release 11.0 and earlier versions only]
• **hamgr**: Home Agent Manager Facility
• **hatcpu**: High Availability Task CPU Facility
• **hatsystem**: High Availability Task Facility
• **hdctrl**: HD Controller
• **henbgw**: Home eNodeB Gateway demux manager
• **henbgwmgr**: Home eNodeB Gateway Manager
• **hnbg**: HNBGW HNB Manager
• **hwctr**: Hardware Monitor Controller
• **hwmg**: Hardware Monitor Manager
• **imsimgr**: SGSN IMSI Manager
• **ipsecctrl**: IP Security Controller Facility
• **ipseemgr**: IP Security Manager Facility
• **ipsgmgr**: IP Services Gateway Facility
• **kvctrl**: KV Controller
• **kvmgr**: KV Manager
• **l2tpdemux**: L2TP Demultiplexor (LNS) Facility
• **l2tpmgr**: L2TP Manager Facility
• **lagmgr**: Link Aggregation Group (LAG) Manager
• **linkmgr**: SGSN/SS7 Link Manager
• **magmgr**: Mobile Access Gateway Manager
• **megadiammgr**: MegaDiameter Manager
• **mmedemux**: MME Demux Manager logging facility
• **mmemgr**: MME Manager logging facility
• **mmgr**: SGSN/SS7 Master Manager
• **mpls_sig**: Multiprotocol Label Switching
• **mptest**: Migration Performance Test on Packet Accelerator Card
• **netwstrg**: Network Storage Manager [Release 11.0 and earlier versions only]
• **npuctrl**: Network Processor Unit Control Facility
• **npudrv**: Network Processor Unit Driver Facility [ASR 5500 only]
• **npumgr**: Network Processor Unit Manager Facility
• **npusim**: Network Processor Unit Simulator [ASR 5500 only]
• **nputst**: Network Processor Unit Tester
• **nsctrl**: Charging Service Controller [Release 11.0 and earlier versions only]
• **nsmgr**: Charging Service Process Manager [Release 11.0 and earlier versions only]
• **orbs**: Object Request Broker System Facility
• **orbs**: Object Request Broker Notification Server Facility
• **ospf**: Open Shortest Path First Facility
• **ospfv3**: Open Shortest Path First (OSPFv3)
• **pdgmgr**: PDG Manager
• **phsgwmg**: PHS Gateway manager
• **phspcmgr**: PHS Paging Controller manager
• **rct**: Recovery Control Task Facility
• **rdt**: Redirect Task Facility
• **rip**: Routing Information Protocol Facility
• **rmctrl**: Resource Manager Controller Facility
• **rmmgr**: Resource Manager Facility
Exec Mode show Commands (T-Z)

show task

- `sct`: Shared Configuration Task Facility
- `sessctrl`: Session Controller Facility
- `sessmgr`: Session Manager Facility
- `sesstrc`: Session Trace Collection task
- `sft`: Switch Fabric Monitoring Task
- `sgtpcmgr`: SGSN GTPC Manager
- `sipcdprt`: SIP Call Distributor Task [Release 11.0 and earlier versions only]
- `sitmain`: System Initialization Task Main Facility
- `sitparent`: Card based system initialization facility that applies to packet processing cards and system management cards (SMC - ASR 5000, MIO - ASR 5500) [Replaces the sitpac, sitspc and sittac facilities]
- `snmp`: SNMP Protocol Facility
- `srdb`: Static Rating Database
- `testctrl`: Test Controller
- `testmgr`: Test Manager
- `threshold`: Threshold Server Facility
- `vpncntl`: Virtual Private Network Controller Facility
- `vpnmgr`: VPN Manager Facility
- `zebos`: ZEBOS™ OSPF Message Facility

`all`: Displays information for all instances of the specified facility.

`instance id`: Displays information for the facility instance specified as an integer from 0 through 10000000.

`process process_name all`

Display information for all instances of the specified process. must be one of the following process names:
- `ftpd`: File Transfer Protocol Daemon
- `inetd`: Internet Super-server Daemon
- `nsproc`: NetSpira Packet Processor
- `ntp`: Network Time Protocol Daemon
- `orbsd`: Object Request Broker Notification Server
- `ping`: Ping
- `pvmd-wraper`: NetSpira Messenger Daemon
- `pvmsg`: NetSpira Messenger Daemon
- `rlogin`: Remote Login
- `sftp-server`: Secure File Transfer Protocol Server
- `sitreap`: System Initialization Task Cleanup Process
- `sn_resolve`: DNS Resolver Process
- `ssh`: Secure Shell
- `sshd`: Secure Shell Daemon
show task

- **telnet**: Telnet
- **telnetd**: Telnet daemon
- **tftpd**: Trivial File Transfer Protocol Daemon
- **traceroute**: Traceroute

### max

Default: current usage levels are displayed. Displays the maximum usage levels for tasks as opposed to the current usage levels. **max** is valid only in conjunction with the **resources** keyword.

```
| { grep grep_options | more }
```

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the **grep** and **more** commands, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter.

### Usage

Display task information as part of system troubleshooting unexpected behavior.

**Important**: This command is not supported on all platforms.

### Example

The following commands provide some examples of the combinations of options that may be used to display task information.

```
show task info facility hatspc all
show task info facility hatspc instance 456
show task resources facility zebos all
show task table facility ospf
show task table card 8 facility cli all
show task table card 5 facility cli all
show task resources facility rip all max
```
show tacp statistics

This command displays the collected traffic statistics that have passed through the SS7 Transaction Capabilities Application Part (TCAP) layer.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator, Operator

**Mode**
Exec

The following prompt is displayed in the Exec mode:

```
[local]host_name#
```

**Syntax**

```
show tacp statistics [ camel-service [ all | name camel_srvc ] | map-service [ all | name map_srvc ] ] [ | { grep grep_options | more } ]
```

- `camel-service [ all | name camel_srvc ]`
  Displays TCAP statistics for either all Customized Applications for Mobile networks Enhanced Logic (CAMEL) services or only for the named CAMEL service.

- `map-service [ all | name mapl_srvc ]`
  Displays TCAP statistics for either all Mobile Application Part (MAP) services or only for the named MAP service.

  | { grep grep_options | more } |
  Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
  For details on the usage of the `grep` and `more` commands, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter.

**Usage**

Use this command to display the collected TCAP statistics for MAP or CAMEL services.

**Example**

The following command displays the collected statistics for a MAP service named `MAP-Tewk`.

```
show tacp statistics map-service name MAP-Tewk
```
show temperature

Displays the current temperature on all installed cards. Also displays the temperature of upper and lower fan trays. Temperature readings are acquired from sensors located on these components.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec
The following prompt is displayed in the Exec mode:

[local] host_name#

Syntax

show temperature [ verbose ] [ | { grep grep_options | more } ]

| { grep grep_options | more }

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of the grep and more commands, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

verbose
Indicates that the output is to contain detailed information.

Usage
Verify current temperature of components in chassis.

Example

    show temperature

    show temperature verbose
show terminal

Displays the current terminal settings for number of lines in length and number of characters in width.

**Product**
All

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Mode**
Exec
The following prompt is displayed in the Exec mode:

```
[local]host_name# 
```

**Syntax**

```
show terminal [ | { grep grep_options | more } ] 
```

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.
For details on the usage of the `grep` and `more` commands, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

**Usage**
Use this command to verify current terminal settings in case the output displayed appears to have line breaks/wraps in unexpected places.

**Example**

```
show terminal
```
show threshold

Displays thresholding information for the system.

**Product**
All

**Privilege**
Security Administrator, Administrator, Operator, Inspector

**Mode**
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

**Syntax**

```
show threshold [ default ]
```

[ default ]
Used to display the system’s thresholding default values.

**Usage**
Use this command to display information on threshold value configuration and activity.

**Example**
The following command displays configuration information pertaining to threshold values configured on the system:

```
show threshold
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference*. 
show timing

Displays the information configured to define a transmit timing source other than the system clock. The display includes related information (such as port status, timing source priority, timing alarms, etc.) for all of the ports configured for either Building Integrated Timing Supply (BITS) or line timing.

Product
SGSN

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show timing

Usage

Use this command to determine which line cards are recovering receive timing clocks.

Important: This command is not supported on all platforms.

Example

The following command displays timing configuration and status information for the timing-configured ports.

show timing
show upgrade

Displays the status of an on-going on-line software upgrade.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

```
show upgrade
```

Usage

Use this command to show the status of an on-going on-line software upgrade.

**Important:** This command is not supported on all platforms.
show url-blacklisting database

Displays URL Blacklisting static database configurations.

Product
CF

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show url-blacklisting database [ all | url url | facility acsmgr { all | instance instance } ] [ | { grep grep_options | more } ]

- **all**
  Displays configurations of all URL Blacklisting databases present in the default or override directory.

- **facility acsmgr { all | instance instance }**
  Displays configurations of URL Blacklisting database configuration per facility/ACSMgr instance.
  - **all**: Displays URL Blacklisting database configuration of all ACSMgrs.
  - **instance instance**: Displays URL Blacklisting database configuration for the instance number of the database specified as an integer from 1 through 1000000.

- **url url**
  Displays configurations of the URL Blacklisting database specified in the database’s URL expressed as an alphanumeric string of 1 through 512 characters.

  | { grep grep_options | more } |

  Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

  For details on the usage of the **grep** and **more** commands, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

Usage

Use this command to view configurations associated with in-memory and on-flash Blacklisting database. The **show url-blacklisting database** command displays the active database that is loaded, and is the one set by either the default or override CLI commands.

Example

The following command displays configurations of all the databases present in default or override directory, indicating one as Active and rest as Not Loaded:

```
show url-blacklisting database all
```
The following command displays configurations of the /flash/bl/optblk.bin database:

```
show url-blacklisting database url /flash/bl/optblk.bin
```

The following command displays database configuration for the ACSMgr instance 1:

```
show url-blacklisting database facility acsmgr instance 1
```

**Important:** Output descriptions for commands are available in the *Statistics and Counters Reference.*
show version

Displays the version information for the current system image or for a remote image.

Product
All

Privilege
Security Administrator, Administrator, Operator, Inspector

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show version [ url ] [ all | verbose ] [ | { grep grep_options | more } ]

url

Specifies the location of a configuration file for which to display version information. The url may refer to a local or a remote file and must be entered in the following format:

For the ASR 5000:


tftp:// { host [ :port# ] } [ /directory ] /file_name


For the ASR 5500:


tftp:// { host [ :port# ] } [ /directory ] /file_name


Important: Do not use the following characters when entering a string for the field names below: “/” (forward slash), “:” (colon) or “@” (at sign).

directory is the directory name.
filename is the actual file of interest.
username is the user to be authenticated.
password is the password to use for authentication.
host is the IP address or host name of the server.
port# is the logical port number that the communication protocol is to use.
show version

**all | verbose**

*all*: displays all image information.

*verbose*: displays detailed information. The *verbose* keyword may not be used in conjunction with a URL specification.

| { grep grep_options | more }

Pipes (sends) the output of the command to the command specified. You must specify a command to which the output will be sent.

For details on the usage of the *grep* and *more* commands, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter.

**Usage**

Display the version information to verify the image versions loaded in preparation for maintenance, upgrades, etc.

**Important**: This command is not supported on all platforms.

**Example**

The following commands display the version information with the basic level of output and the detailed level, respectively.

```plaintext
show version

show version verbose
```
show wsg-lookup

Displays the current priority settings of subnet components for site-to-site tunnels in WSG services.

**Product**
SecGW (WSG)

**Privilege**
Security Administrator, Administrator, Operator

**Mode**
Exec
The following prompt is displayed in the Exec mode:

[local]host_name#

**Syntax**

```
show wsg-lookup
```

**Usage**
Use this command to display current WSG lookup priority settings,

**Examples**

```
show wsg-lookup
```
show wsg-service

Displays information about WSG service calls and configured services.

Product
SecGW (WSG)

Privilege
Security Administrator, Administrator, Operator

Mode
Exec

The following prompt is displayed in the Exec mode:

[local]host_name#

Syntax

show wsg-service { all | name srvc_name | statistics [ name srvc_name | peer-address ip_address ] [ | { grep grep_options | more } ]

  all
  Displays information for all configured services.

  name srvc_name
  Displays information for the specified service name.

  statistics [ name srvc_name | peer-address ip_address ]
  Displays information collected for the WSG service since the last VPC-VSM reload or clear command.
  You can display information for all WSG services (default), for named service or for a specific peer IP address.
  The peer ip_address can be specified in IPv4 dotted decimal or IPv5 colon-separated hexadecimal notation.

  | { grep grep_options | more }
  Pipes (sends) the output of the command to the command specified. You must specify a command to which
  the output will be sent.
  For details on the usage of the grep and more commands, refer to the Regulating a Command’s Output
  section of the Command Line Interface Overview chapter.

Usage
This command displays information about all or a specified WSG service.

Example
The following command displays information about all WSG services:

  show wsg-service all
Chapter 133
FA Service Configuration Mode Commands

The Foreign Agent Service Configuration Mode is used to create and manage the Foreign Agent (FA) services associated with the current context.

Mode

Exec > Global Configuration > Context Configuration > FA Service Configuration

configure > context context_name > fa-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-fa-service)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
advertise

Configures agent advertisement parameters within the FA service.

Product

PDSN
GGSN
ASN-GW

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > Context Configuration > FA Service Configuration
configure > context context_name > fa-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-fa-service)#

Syntax

advertise {adv-delay seconds | adv-lifetime time | adv-interval { seconds | msec num } | num-adv-sent number | prefix-length-extn | reg-lifetime reg_time }

no advertise { prefix-length-extn | reg-lifetime }

default advertise adv-delay

---

no

Disables prefix-length-extn

---

no advertise reg-lifetime

Specifies that there is no limit to the registration lifetime that the FA service will allow in any Registration Request message from the mobile node.

default advertise adv-delay

Sets the initial delay for the unsolicited advertisement to the default value of 1000 ms.

---

advertise adv-delay seconds

Default: 1000
Sets the initial delay for the unsolicited advertisement.
seconds is the advertisement delay in milliseconds and must be an integer from 10 through 5000.

---

Important: This command is available for WiMAX CMIP calls only.

---

adv-lifetime time

Default: 9000
Specifies the FA agent advertisement lifetime. The agent advertisement lifetime is the amount of time that an FA agent advertisement remains valid in the absence of further advertisements. 

`time` is measured in seconds and can be configured to an integer from 1 through 65535.

```
adv-interval { seconds | msec num }
```

Default: 5 seconds
Specifies the amount of time between agent advertisements. `seconds` is the time in seconds and can be an integer from 1 through 1800. 

`msec num`: Configures agent advertisement Interval in milliseconds. `num` can be an integer from 100 through 1800000.

```
num-adv-sent number
```

Default: 5
Specifies the number of unanswered agent advertisements that the FA service sends upon PPP establishment before rejecting the session. 

`number` can be an integer from 1 through 65535.

```
prefix-length-extn
```

Default: Disabled
When enabled, the FA includes the FA-service address in the Router Address field of the Agent Advertisement and appends a Prefix Length Extension in Agent Advertisements with a prefix length of 32.

```
reg-lifetime reg_time
```

Default: 600
Specifies the longest registration lifetime that the FA service will allow in any Registration Request message from the mobile node. 

`reg_time` is measured in seconds and can be configured to an integer from 1 through 65534.

Usage
Use to tailor FA advertisements to meet your network needs and/or conditions.

Example
The following command configures the FA advertisement interval at 10 seconds, the advertise lifetime to 20000 seconds, and the maximum number of unanswered advertisements that will be set to 3.

```
advertise adv-interval 10 adv-lifetime 20000 num-adv-sent 3
```
**authentication aaa**

This configuration enables or disables the authentication parameters for the FA service to override dynamic keys from AAA with static keys to support MIP registration with an HA that does not support dynamic keys.

**Product**

FA

ASN-GW

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > FA Service Configuration

`configure > context context_name > fa-service service_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-fa-service)#
```

**Syntax**

```
[ no | default ] authentication aaa-distributed-mip-keys override
```

- **no**
  
  Disable the override of dynamic keys from AAA.

- **default**
  
  By default the override behavior is disabled and the system uses dynamic keys from AAA after successful EAP authentication. If EAP authentication fails, the system uses static keys by default.

**Usage**

Specify how the system will perform authentication of registration request messages. By default dynamic MN-HA and FA-HA keys from AAA after successful EAP authentication used by a PMIP client in WiMAX calls for MIP registration with HA. This configuration in FA service overrides the dynamic keys from AAA with static keys to support MIP registration with an HA that does not support dynamic keys.

**Example**

The following command configures the FA service to override use of AAA MIP keys and force the use of statically configured FA-HA SPI/key for WiMAX calls.

```
authentication aaa-distributed-mip-keys override
```
authentication mn-aaa

Specifies how the system handles authentication for mobile node re-registrations.

**Product**
- PDSN
- ASN-GW
- GGSN

**Privilege**
- Security Administrator, Administrator

**Mode**
- **Exec > Global Configuration > Context Configuration > FA Service Configuration**

`configure > context context_name > fa-service service_name`  

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-fa-service)#
```

**Syntax**

```
```

- **always**
  - Specifies that the FA service performs authentication each time a mobile node registers. This is the default setting.

- **ignore-after-handoff**
  - MN-AAA authentication is not done at the FA for a handoff Access Gateway (AGW).

- **init-reg**
  - MN-AAA and MN-FAC extensions are required only in initialization RRQ.

- **init-reg-except-handoff**
  - MN-AAA and MN-FAC extensions are not required in initialization RRQ after inter-Access Gateway (AGW) handoff.

- **renew-and-dereg-noauth**
  - Specifies that the FA service does not perform authentication for mobile node re-registration or deregistration authorization requests. Initial registration is handled normally.

- **renew-reg-noauth**
  - Specifies that the FA service does not perform authentication for mobile node re-registrations. Initial registration and de-registration are handled normally.
**optimize-retries**

Optimizes the number of Authentication retries sent to the AAA server. When an authentication request is pending for a MIP call at the AGW, if a retry RRQ is received from the mobile node, the AGW discards the old RRQ and keeps the most recent RRQ. Subsequently when the authentication succeeds, the AGW forwards the most recent RRQ to the HA. If the authentication fails, the AGW replies to the MN using the most recent RRQ.

**Usage**

Use this command to determine how the FA service handles mobile node reRegistrations. The system is shipped from the factory with the mobile AAA authentication set to always.

**Example**

The following command configures the FA service to perform mobile node authentication for every re-registration:

```
authentication mn-aaa always
```

The following command specifies that the FA service does not perform authentication for mobile node re-registrations:

```
authentication mn-aaa renew-reg-noauth
```
authentication mn-ha

Configures whether the FA service looks for a Mobile Network-Home Agent (MN-HA) authentication extension in the RRP (registration reply).

Product
PDSN
ASN-GW
GGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > FA Service Configuration
configure > context context_name > fa-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-fa-service)#

Syntax

authentication mn-ha { allow-noauth | always }

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>allow-noauth</td>
<td>Allows a reply that does not contain the auth extension.</td>
</tr>
<tr>
<td>always</td>
<td>A reply should always contain the auth extension to be accepted. This is the default setting.</td>
</tr>
</tbody>
</table>

Usage
Use this command to determine whether or not the FA service requires the MN-HA auth extension in the RRP.
The system is shipped from the factory with this set to always.

Example
The following command configures the FA service to require a reply to contain the authentication extension to be accepted:

authentication mn-ha always
bind

Binds the FA service to a logical IP interface serving as the Pi interface and specifies the maximum number of subscribers that can access this service over the interface.

**Product**
- PDSN
- ASN-GW
- GGSN
- PDIF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > FA Service Configuration

```console
configure > context context_name > fa-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-fa-service)#
```

**Syntax**

```
bind address address [ max-subscribers count ]

no bind address
```

- **address**
  Specifies the IP address (address) of the interface configured as the Pi interface. *address* is specified in IPv4 dotted-decimal notation.

- **max-subscribers max#**
  Default: 500000
  Specifies the maximum number of subscribers that can access this service on this interface.
  *count* can be configured to an integer from 0 through 500000.

**Important:** The maximum number of subscribers supported is dependant on the license key installed and the number of active packet processing cards installed in the system. Refer to the license key command for additional information.

**Usage**

Associate or tie the FA service to a specific logical IP address. The logical IP address or interface takes on the characteristics of an Pi interface. Only one interface can be bound to a service. The interface should be configured prior to issuing this command.

This command also sets a limit as to the number of simultaneous subscribers sessions that can be facilitated by the service/interface at any given time.

When configuring the **max-subscribers** option, be sure to consider the following:
The total number of interfaces you will configure for use as Pi interfaces

• The maximum number of subscriber sessions that all of these interfaces may handle during peak busy hours

• The average bandwidth for each of the sessions

• The type of physical port (10/100Base-T or 1000Base-Tx) that these interfaces will be bound to

Taking these factors into account and distributing your subscriber session across all available interfaces will allow you to configure your interfaces to optimally handle sessions without degraded performance. Use the `no bind address` command to delete a previously configured binding.

**Example**

The following command would bind the logical IP interface with the address of `192.168.3.1` to the FA service and specifies that a maximum of 600 simultaneous subscriber sessions can be facilitated by the interface/service at any given time.

```plaintext
bind address 192.168.3.1 max-subscribers 600
```

The following command disables a binding that was previously configured:

```plaintext
no bind address
```
challenge-window

Defines the number of recently sent challenge values that are considered valid by the FA.

Product
PDSN
ASN-GW
GGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > FA Service Configuration
configure > context context_name > fa-service service_name

Entering the above command sequence results in the following prompt:

[context_name] host_name(config-fa-service)#

Syntax

challenge-window number

number

Default: 2
The number of recently sent challenge values that are considered valid. number must be an integer from 1 through 5.

Usage
Use this command to set the number of recently sent challenge values that are considered valid by the FA.

Example
Set the challenge window to 3:

challenge-window 3
default subscriber

Specifies the name of a subscriber profile configured within the same context as the FA service from which to base the handling of all other subscriber sessions handled by the FA service.

Product
PDSN
ASN-GW
GGSN
PDIF

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > FA Service Configuration

configure > context context_name > fa-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-fa-service)#

Syntax

[ no ] default subscriber profile_name

profile_name

Specifies the name of the configured subscriber profile. profile_name is an alphanumeric string of 1 through 63 characters that is case sensitive.

Usage
Each subscriber profile specifies “rules” such as permissions, PPP settings, and timeout values.
By default, the FA service will use the information configured for the subscriber named default within the same context. This command allows for multiple FA services within the same context to apply different “rules” to sessions they process. Each set of rules can be configured under a different subscriber name which is pointed to by this command.
Use the no default subscriber profile_name command to delete the configured default subscriber.

Example
To configure the FA service to apply the rules configured for a subscriber named user1 to every other subscriber session it processes, enter the following command:

default subscriber user1
dynamic-ha-assignment

This command configures various dynamic HA assignment parameters.

Product
HA

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > FA Service Configuration

configure > context context_name > fa-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-fa-service)#

Syntax

[ default | no ] dynamic-ha-assignment [ aaa-override mn-supplied-ha-addr | allow-failover ]

default
Feature is disabled by default.

no
Removes the feature and returns it to the default setting of disabled.

aaa-override mn-supplied-ha-addr
Enables the system to override the mobile node supplied HA IP address with the AAA provided HA address.

allow-failover
Enables/disables a failover retry for dynamic HA assignment from the AAA server.

Usage
Use this command to override the mobile node supplied HA IP address with the AAA supplied HA address. Use this command to enable or disable the failover feature that allows the system to receive and use a newer HA address from the AAA server in cases where the original HA address is not responding. A AAA server may assign different HA addresses each time a retransmitted MIP RRQ is authenticated during the MIP session setup. When this configuration is enabled, if the FA gets a new HA address from AAA during setup, it discards the previous HA address and start using the new address. This allows the FA session to connect to an available HA during setup.

Example
The following command enables the failover feature that allows the system to receive and use a newer HA address from the AAA server:

    dynamic-ha-assignment allow-failover
**dynamic-mip-key-update**

When enabled, the FA service processes MIP_Key_Update_Request from the AAA server and allows dynamic MIP key updates (DMUs).

Default: Disabled

**Product**

PDSN  
ASN-GW  
GGSN

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > FA Service Configuration  
configure > context context_name > fa-service service_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-fa-service)#
```

**Syntax**

```
[ no ] dynamic-mip-key-update
```

```
no
```

The FA service rejects MIP_Key_Update_Request from the AAA server, not allowing dynamic MIP key updating to occur and terminates the call.

**Usage**

Use this command to enable or disable the DMU feature in the FA service.

**Example**

To enable DMU and allow dynamic updates of MIP keys, enter the following command:

```
dynamic-mip-key-update
```
encapsulation allow gre

Enables or disables the use of generic routing encapsulation (GRE) when establishing a Mobile IP (MIP) session. When enabled, if requested by a Mobile Node (MN), the FA requests the HA to use GRE encapsulation when establishing the MIP session. When disabled, the FA does not set the GRE bit in Agent Advertisements to the MN.

Default: GRE is enabled.

Product

- PDSN
- ASN-GW
- GGSN

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > Context Configuration > FA Service Configuration

configure > context context_name > fa-service service_name

Entering the above command sequence results in the following prompt:

[context_name] host_name(config-fa-service)#

Syntax

[ no ] encapsulation allow gre

Usage

Use to disable or re-enable the use of GRE encapsulation for MIP sessions.

Example

To re-enable GRE encapsulation for MIP sessions, enter the following command:

encapsulation allow gre
end

Exits the current configuration mode and returns to the Exec mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

```text
end
```

**Usage**

Use this command to return to the Exec mode.
**exit**

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
exit
```

**Usage**
Use this command to return to the parent configuration mode.
fa-ha-spi

Configures the security parameter index (SPI) between the FA service and the HA.

**Product**
- PDSN
- ASN-GW
- GGSN
- PDIF

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration > Context Configuration > FA Service Configuration

```bash
configure > context context_name > fa-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-fa-service)#
```

**Syntax**

```bash
fa-ha-spi remote-address { ha_ip_address | ip_addr_mask_combo } spi-number number { encrypted secret enc_secret | secret } [ description string | hash-algorithm { hmac-md5 | md5 | rfc2002-md5 } | monitor-ha | replay-protection { timestamp | nonce } | timestamp-tolerance tolerance ]
```

```bash
no fa-ha-spi remote-address { ha_ip_address | ip_addr_mask_combo } spi-number number
```

**remote-address**

```bash
ha_ip_address: Specifies the IP address of the HA in IPv4 dotted-decimal notation.
ip_addr_mask_combo: Specifies the IP address of the HA including network mask bits.
ip_addr_mask_combo must be specified IPv4 dotted-decimal notation with CIDR subnet mask bits (x.x.x.x/xx).
```

**spi-number**

Specifies the Security Parameter Index (SPI) which indicates a security context between the FA and the HA in accordance with RFC 2002.

```bash
number can be configured to an integer from 256 through 4294967295.
```

**encrypted secret**

```bash
enc_secret | secret
```

Configures the shared-secret between the FA service and the HA. The secret can be either encrypted or non-encrypted.

```bash
*encrypted secret enc_secret : Specifies the encrypted shared key (enc_secret) between the FA service and the HA. enc_secret must be an alphanumeric string of 1 through 254 characters that is case sensitive.
```
**Important:** The encrypted keyword is intended only for use by the system while saving configuration scripts. The system displays the encrypted keyword in the configuration file as a flag that the variable following the secret keyword is the encrypted version of the plain text secret key. Only the encrypted secret key is saved as part of the configuration file.

- **secret secret:** Specifies the shared key (secret) between the FA service and the HA. secret must be an alphanumeric string of 1 through 127 characters that is case sensitive.

**description string**

This is a description for the SPI. string must be an alphanumeric string of 1 through 31 characters.

**hash-algorithm { hmac-md5 | md5 | rfc2002-md5 }**

Default: hmac-md5

Specifies the hash-algorithm used between the FA service and the HA.
- **hmac-md5:** Configures the hash-algorithm to implement HMAC-MD5 per RFC 2002bis.
- **md5:** Configures the hash-algorithm to implement MD5 per RFC 1321.
- **rfc2002-md5:** Configures the hash-algorithm to implement keyed-MD5 per RFC 2002.

**monitor-ha**

Default: disabled

Enables the HA monitor feature for this HA address.
To set the behavior of the HA monitor feature, refer to the **ha-monitor** command in this chapter. To disable this command (if enabled) for this HA address, re-enter the entire fa-ha-spi command without the monitor-ha keyword.

**replay-protection { timestamp | nonce }**

Default: timestamp

Specifies the replay-protection scheme that should be implemented by the FA service for this SPI.
- **nonce:** Configures replay protection to be implemented using NONCE per RFC 2002. Nonce is an arbitrary number used only once to sign a cryptographic communication.
- **timestamp:** Configures replay protection to be implemented using timestamps per RFC 2002.

**Important:** This keyword should only be used in conjunction with Proxy Mobile IP support.

**timestamp-tolerance tolerance**

Default: 60

Specifies the allowable difference (tolerance) in timestamps that is acceptable. If the difference is exceeded, then the session will be rejected. If this is set to 0, then timestamp tolerance checking is disabled at the receiving end.

tolerance is measured in seconds and can be configured to an integer value from 0 through 65535.

**Important:** This keyword should only be used in conjunction with Proxy Mobile IP support.
More than one of the above keywords can be entered within a single command.

Usage
An SPI is a security mechanism configured and shared by the FA service and the HA. Please refer to RFC 2002 for additional information.
Though it is possible for FAs and HAs to communicate without SPIS being configured, the use of them is recommended for security purposes. It is also recommended that a “default” SPI with a remote address of 0.0.0.0/0 be configured on both the HA and FA to prevent hackers from spoofing addresses.

**Important:** The SPI configuration on the HA must match the SPI configuration for the FA service on the system in order for the two devices to communicate properly.

Example
A maximum of 2,048 SPIS can be configured per FA service.
Use the `no` version of this command to delete a previously configured SPI.

The following command configures the FA service to use an SPI of 512 when communicating with an HA with the IP address 192.168.0.2. The key that would be shared between the HA and the FA service is q397F65. When communicating with this HA, the FA service will also be configured to use the rfc2002-md5 hash-algorithm.

```bashfa-ha-spi remote-address 192.168.0.2 spi-number 512 secret q397F65 hash-algorithm rfc2002-md5
```

The following command deletes the configured SPI of 400 for an HA with an IP address of 172.100.3.200:

```bash
no fa-ha-spi remote-address 172.100.3.200 spi-number 400
```
**gre**

Configures Generic Routing Encapsulation (GRE) parameters.

**Product**
- PDSN
- ASN-GW
- GGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > FA Service Configuration

```
configure > context context_name > fa-service service_name
```

Entering the above command sequence results in the following prompt:
```
[context_name]host_name(config-fa-service)#!
```

**Syntax**

```
gre { checksum | checksum-verify | reorder-timeout timeout | sequence-mode { none | reorder } | sequence-numbers }
```

```
no gre { checksum | checksum-verify | sequence-numbers }
```

**no**
Disables the specified functionality.

---

**checksum**
Default: disabled
Enables the introduction of the checksum field in outgoing GRE packets.

---

**checksum-verify**
Default: disabled
Enables verification of the GRE checksum (if present) in incoming GRE packets.

---

**reorder-timeout timeout**
Default: 100
Configures maximum number of milliseconds to wait before processing reordered out-of-sequence GRE packets. `timeout` must be an integer from 0 through 5000.

---

**sequence-mode { none | reorder }**
Default: none
Configures how incoming out-of-sequence GRE packets should be handled.
`none`: Disables reordering of incoming out-of-sequence GRE packets.
`reorder`: Enables reordering of incoming out-of-sequence GRE packets.
sequence-numbers
Default: Disabled.
Enables insertion or removal of GRE sequence numbers in GRE packets.

Usage
Use this command to configure how the FA service handles GRE packets.

Example
To set maximum number of milliseconds to wait before processing reordered out-of-sequence GRE packets to 500 milliseconds, enter the following command:

```
gre reorder-timeout 500
```

To enable the reordering of incoming out of sequence GRE packets, enter the following command:

```
gre sequence-mode reorder
```
fa-monitor

Configures the behavior of the HA monitor feature.

Product

- PDSN
- ASN-GW
- FA
- HA

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > Context Configuration > FA Service Configuration
configure > context context_name > fa-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-fa-service)#

Syntax

[ default ] ha-monitor [ interval sec | max-inactivity-time sec | num-retry num ]
no ha-monitor

default

Restores the system default setting(s) for the command/keyword(s). This command is disabled by default.

no

Disables the HA monitoring feature for this FA service.

interval sec

Default: 30
Configures the time interval before the next monitoring request message is sent to the HA.
sec must be an integer from 1 through 3600.

max-inactivity-time sec

Default: 60
Specifies the maximum amount of time the system will wait without receiving MIP control traffic from a HA before the HA monitoring mechanism is triggered.
sec must be an integer from 30 through 600.

num-retry num

Default: 5
Configures the number of time the system will attempt to send HA monitor requests before determining the HA is down and a trap is initiated.
num must be an integer from 0 through 10.
Usage

Use this command to set parameters for the HA monitor feature. This feature allows the AGW/FA to monitor HAs with which it has MIP sessions. The monitoring feature is triggered when the AGW/FA does not receive any MIP traffic from a HA for a configured amount of time (max-inactivity-time). The AGW/FA starts sending special MIP RRQ monitor messages and waits for RRP monitor message responses from the HA. The RRQ monitor messages are addressed to the HA service address. The source address of the monitor-request messages is the FA service's IP address.

The actions taken during monitoring are comprised of the following:

- If no monitor response is received during the interval time (interval), the AGW retransmits the monitor message a configured number of times (num-retry).
- If no response is received after retransmitting for the number configured in num-retry, the HA is considered down. The AGW/FA sends a trap (HAUnreachable) to the management station. Monitoring of this HA is stopped until a MIP control message is received from the particular HA and when the AGW/FA sends a trap (HAreachable) to the management station and starts monitoring the HA again.
- When an HA receives the RRQ from an FA, it verifies the message and identifies it as a monitor message based on a special reserved NAI (in the message) and a Monitor HA CVSE in the RRQ. The HA responds with an RRP with Reply code 0x00 (accepted) and includes the Monitor HA CVSE. When the FA receives the RRP from the HA, it updates the activity for the peer HA to maintain the “up” state.

**Important:** This command only sets the behavior of the HA monitor feature. To enable the HA monitor feature for each HA address, refer to the `fa-ha-spi` command in this chapter. Up to 256 HAs can be monitored per system.

Example

The following commands set the HA monitor message interval to 45 seconds, the HA inactivity time to 60 seconds, and the number of HA monitor retries to 6:

```
ha-monitor interval 45
ha-monitor max-inactivity-time 60
ha-monitor num-retry 6
```
idle-timeout-mode

Controls whether Mobile IP data and control packets or only Mobile IP data resets the session idle timer.

Product

PDSN
ASN-GW
GGSN
PDIF

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > Context Configuration > FA Service Configuration

configure > context context_name > fa-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-fa-service)#

Syntax

idle-timeout-mode { aggressive | normal }

aggressive

Only Mobile IP data resets the session idle timer.

normal

Both Mobile IP data and control packets reset the session idle timer.

Usage

Use this command to control how the session idle timer is reset.

Example

The following command specifies that only Mobile IP data can reset the session idle timer:

idle-timeout-mode aggressive
ignore-mip-key-data

When this command is enabled, if the Dynamic Mobile IP Key Update (DMU) is not enabled and the mobile node (MN) sends a MIP_Key_Data CVSE, the FA ignores the MIP_Key_Data extension and the call is continued like a regular Mobile IP (MIP) call.

Product
PDSN
GGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > FA Service Configuration
configure > context context_name > fa-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-fa-service)#

Syntax

[ no ] ignore-mip-key-data

no
Disable ignoring of MIP key data.

Usage
When DMU is not enabled, use this command to ignore MIP key data sent by the MN and allow the call to continue normally.

Example
To enable the FA to ignore MIP key data sent by the MN, enter the following command:

ignore-mip-key-data
**ignore-stale-challenge**

Enables the system to accept RRQs with previously used challenges. This feature is disabled by default.

**Product**

PDSN

GGSN

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > FA Service Configuration

```bash
configure > context context_name > fa-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-fa-service)#
```

**Syntax**

```
[ no ] ignore-stale-challenge
```

**Usage**

Disables this feature. If an RRQ is received with a previously used challenge and there are RRQs pending on the same session, accept the RRQ if it has a new Identification in the retransmitted RRQ. All other RRQs received with previously used challenge are rejected with the Stale Challenge (106) error code.

**Example**

To enable this functionality in the FA service, enter the following command;

```
ignore-stale-challenge
```

To disable this functionality, enter the following command;

```
no ignore-stale-challenge
```
**ip local-port**

Configures the local User Datagram Protocol (UDP) port for the Pi interfaces’ IP socket on which to listen for Mobile IP Registration messages.

**Product**
- PDSN
- ASN-GW
- GGSN

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration > Context Configuration > FA Service Configuration

```
configure > context context_name > fa-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-fa-service)#
```

**Syntax**

```
ip local-port port#
```

- `port#`
  - Specifies the UDP port number.
  - `port#` can be an integer from 1 through 65535.

**Usage**

Specify the UDP port that should be used for communications between the FA service and the HA. The system defaults to using local port 434.

**Example**

The following command specifies a UDP port of 3950 for FA-to-HA communication on the Pi interface:

```
ip local-port 3950
```
**isakmp**

Configures support for IPSec within the FA-service.

**Product**
- PDSN
- ASN-GW
- GGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > FA Service Configuration

configure > context context_name > fa-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-fa-service)#

**Syntax**

```plaintext
isakmp { peer-ha ha_address { crypto map map_name [ [ encrypted ] secret secret ] } | default { crypto map map_name [ [ encrypted ] secret secret ] } } 

no isakmp { peer-ha peer_ip_address | default }
```

- **no**
  Deletes the reference to the crypto map for the specified HA, or deletes the reference for the default crypto map.

```plaintext
default { crypto map map_name [ [ encrypted ] secret preshared_secret ] }
```

Configures a crypto map for a peer HA.
- **ha_address**: The IP address of the HA with which the FA service will establish an IPSec SA. The address must be expressed in IPv4 dotted-decimal format.
- **crypto map map_name**: The name of a crypto map configured in the same context that defines the IPSec tunnel properties. `map_name` is the name of the crypto map expressed as an alphanumeric string of 1 through 127 characters.
- **encrypted**: This keyword is intended only for use by the system while saving configuration scripts. The system displays the `encrypted` keyword in the configuration file as a flag that the variable following the `secret` keyword is the encrypted version of the plain text secret key. Only the encrypted secret key is saved as part of the configuration file.
- **secret secret**: The pre-shared secret that will be used during the IKE negotiation. `preshared_secret` is the secret expressed as an alphanumeric string of 1 through 127 characters.

```plaintext
default { crypto map map_name [ [ encrypted ] secret secret ] }
```

Specifies the default crypto map to use when there is no matching crypto map configured for an HA address.
*crypto map map_name*: The name of a crypto map configured in the same context that defines the IPSec tunnel properties. map_name is the name of the crypto map expressed as an alphanumeric string of 1 through 127 characters.

*encrypted*: This keyword is intended only for use by the system while saving configuration scripts. The system displays the encrypted keyword in the configuration file as a flag that the variable following the secret keyword is the encrypted version of the plain text secret key. Only the encrypted secret key is saved as part of the configuration file.

*secret secret*: The pre-shared secret that will be used during the IKE negotiation. preshared_secret is the secret expressed as an alphanumeric string of 1 through 127 characters.

**Usage**

Use this command to configure the FA-service’s per-HA IPSec parameters. These dictate how the FA service is to establish an IPSec SA with the specified HA.

**Important:** For maximum security, the above command should be executed for every possible HA with which the FA service communicates.

A default crypto map can also be configured using the default keyword. The default crypto map is used in the event that the AAA server returns an HA address that is not configured as an isakmp peer-ha.

**Important:** For maximum security, the default crypto map should be configured in addition to peer-ha crypto maps instead of being used to provide IPSec SAs to all HAs.

**Example**

The following command creates a reference for an HA with the IP address 10.2.3.4 to a crypto map named map1:

```
isakmp peer-ha 10.2.3.4 crypto map map1
```

The following command deletes the crypto map reference for the HA with the IP address 10.2.3.4.

```
o isakmp peer-ha 10.2.3.4
```
limit-reg-lifetime

Enable the current default behavior of limiting the Mobile IP (MIP) lifetime to be smaller than the Idle, Absolute, or Long Duration timeouts. When disabled, this command allows a MIP lifetime that is longer than the Idle, Absolute or Long Duration timeouts.

Product
PDSN
ASN-GW
GGSN
PDIF

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > FA Service Configuration

configure > context context_name > fa-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-fa-service)#

Syntax

[ no | default ] limit-reg-lifetime

no

Allows a MIP lifetime that is longer than the Idle, Absolute or Long Duration timeouts.

default

Enables the default behavior of limiting the MIP lifetime to be smaller than the Idle, Absolute, or Long Duration timeouts.

Usage
Use the no keyword with this command to allow a MIP lifetime that is longer than the Idle, Absolute or Long Duration timeouts.

Use the base command or the keyword to reset the FA service to the default behavior of limiting the MIP lifetime to be smaller than the Idle, Absolute, or Long Duration timeouts.

Example
Configure the FA service to allow a MIP lifetime that is longer than the Idle, Absolute or Long Duration timeouts by entering the following command:

no limit-reg-lifetime

Configure the FA service to the default behavior of limiting the MIP lifetime to be smaller than the Idle, Absolute, or Long Duration timeouts by entering either of the following commands:

default limit-reg-lifetime
limit-reg-lifetime
**max-challenge-len**

For mobile subscribers, the FA generates a random number and sends it to the mobile node as part of the mobile authentication extension (Mobile-Foreign Authentication extension) as described in RFC 3012. This command sets the maximum length of the FA challenge in bytes.

**Product**
- PDSN
- ASN-GW
- GGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > FA Service Configuration
```
configure > context context_name > fa-service service_name
```

Entering the above command sequence results in the following prompt:
```
[context_name]host_name(config-fa-service)#
```

**Syntax**
```
max-challenge-len length
```

- `length`:
  - Default: 16
  - The maximum length, in bytes, of the FA challenge. This value must be an integer from 4 through 32.

**Usage**
Change the maximum allowed length of the randomly generated FA challenge its default of 16.

**Example**
Use the following command to change the maximum length of the FA challenge to 18 bytes:
```
max-challenge-len 18
```
mn-aaa-removal-indication

Enables the FA to remove the Mobile Network-Final Assembly Code (MN-FAC) and MN-AAA extensions from RRQs. This is disabled by default.

Product
PDSN
ASN-GW
GGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > FA Service Configuration

configure > context context_name > fa-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-fa-service)#

Syntax

[ no ] mn-aaa-removal-indication

no

Disable the removal of the MN-FAC and MN-AAA extensions from RRQs.

Usage
Enable this feature if there is no need to authenticate the subscriber at HA using MN-AAA extension.

Example
The following command enables the FA service to remove MN-FAC and MN-AAA extensions from RRQs:

mn-aaa-removal-indication
**multiple-reg**

Specifies the number of simultaneous Mobile IP sessions that will be supported for over a single PPP session.

**Product**
- PDSN
- ASN-GW
- GGSN

**Privilege**
Security Administrator, Administrator

**Mode**
```
Exec > Global Configuration > Context Configuration > FA Service Configuration
configure > context context_name > fa-service service_name
```
Entering the above command sequence results in the following prompt:
```
[context_name]host_name(config-fa-service)#
```

**Syntax**
```
multiple-reg number
```

**Usage**
- Use to support multiple registrations per subscriber.
- The system defaults to a setting of “1” for multiple simultaneous MIP sessions.

**Important:** The system will only support multiple Mobile IP sessions per subscriber if the subscriber’s mobile node has a static IP address. The system will only allow a single Mobile IP session for mobile nodes that receive a dynamically assigned IP address. In addition, because only a single Mobile IP or proxy-Mobile IP session is supported for IP PDP contexts, this parameter must remain at its default configuration.

**Example**
The following command configures the number of supported simultaneous registrations for subscribers using this FA service to 3.
```
multiple-reg 3
```
optimize tunnel-reassembly

Configures FA to HA optimization for tunnel reassembly.

**Product**
- PDSN
- ASN-GW
- GGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > FA Service Configuration

```bash
configure > context context_name > fa-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-fa-service)#
```

**Syntax**

```
[ no ] optimize tunnel-reassembly
```

**Usage**
Enabling this functionality fragments large packets prior to encapsulation for easier processing. Tunnel reassembly optimization is disabled by default.

> **Important:** You should not use this command without first consulting Cisco Systems Technical Support. This command applies to very specific scenarios where packet reassembly is not supported at the far end of the tunnel. There are cases where the destination network may either discard the data, or be unable to reassemble the packets.

> **Important:** This functionality works best when the FA service is communicating with an HA service running in a system. However, an FA service running in the system communicating with an HA from a different manufacturer will operate correctly even if this parameter is enabled.

**Example**

Use the `no` version of this command to disable tunnel optimization if it was previously enabled.

The following command enables tunnel reassembly optimization:

```
optimize tunnel-reassembly
```
private-address allow-no-reverse-tunnel

This command enables the FA to allow calls with private addresses and no reverse tunneling.

**Product**
- PDSN
- ASN-GW
- GGSN

**Privilege**
- Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > FA Service Configuration
configure > context context_name > fa-service service_name

Entering the above command sequence results in the following prompt:

```
[context_name] host_name(config-fa-service)#
```

**Syntax**

```
[ no ] private-address allow-no-reverse-tunnel
```

- **no**
  - Disables the functionality. This is the default setting.

**Usage**
Use this command to let the FA allow sessions with private addresses that do not have the reverse tunnel bit set.

**Example**
To enable sessions with private addresses and no reverse tunneling, enter the following command:

```
private-address allow-no-reverse-tunnel
```
proxy-mip

Configures parameters pertaining to Proxy Mobile IP support.

Product
PDSN
ASN-GW
GGSN
PDIF

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > FA Service Configuration

command > context context_name > fa-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-fa-service)#

Syntax

proxy-mip { allow | ha-failover [ max-attempts max_attempts | num-attempts-before-switching num_attempts | timeout seconds ] | max-retransmissions number | renew-percent-time renew-time | retransmission-timeout time }

no proxy-mip {allow | ha-failover }

default proxy-mip { allow | ha-failover | max-retransmissions | renew-percent-time | retransmission-timeout }

no

Disables FA service support for Proxy Mobile IP or HA failover for Proxy Mobile IP.

default

Restores the specified option to the default setting as described below.

allow

Default: Disabled
Enables FA service support for Proxy Mobile IP.

ha-failover [max-attempts max_attempts | num-attempts-before-switching num_attempts | timeout seconds ]

Default: Disabled
Enables HA failover for the Proxy Mobile IP feature.

*max-attempts max_attempts - Configures the maximum number of retransmissions of Proxy MIP control messages. max_attempts must be an integer from 1 through 10. Default is 4
**num-attempts-before-switching** *num_attempts* - Configures the total number of RRQ attempts (including retransmissions) before failing over to the alternate HA. *num_attempts* must be an integer from 1 through 5. Default is 2.

**timeout** *seconds* - Configures the retransmission timeout (in seconds) of Proxy MIP control messages when failover happens. *seconds* must be an integer from 1 through 50. Default is 2.

### max-retransmissions *number*

Default: 5  
Configures the maximum number re-try attempts that the FA service is allowed to make when sending Proxy Mobile IP Registration Requests to the HA.  
*number* is the maximum number of retries and can be configured to an integer from 1 through 4294967295.

### renew-percent-time *renew-time*

Default: 75  
Configures the amount of time that must pass prior to the FA sending a Proxy Mobile IP Registration Renewal Request.  
*renew-time* is entered as a percentage of the advertisement registration lifetime configured for the FA service. (Refer to the *advertise* command in this chapter). *renew-time* can be configured to an integer from 1 through 100.  
The following equation can be used to calculate *renew-time*:  
\[\text{renew-time} = \left(\frac{\text{duration}}{\text{lifetime}}\right) \times 100\]  
duration = The desired amount of time that can pass prior to the FA sending a Proxy Mobile IP Registration Renewal Request  
lifetime = The advertisement registration lifetime configured for the FA service.

duration / lifetime

### retransmission-timeout *time*

Default: 3  
Configures the maximum amount of time allowed by the FA for a response from the HA before re-sending a Proxy Mobile IP Registration Request message.  
*time* is measured in seconds and can be configured to an integer from 1 through 100.

---

**Usage**  
The *proxy-mip* command and its keywords configure the FA services support for Proxy Mobile IP.  
When enabled though the session license and feature use key, the system supports Proxy Mobile IP to provide a mobility solution for subscribers with mobile nodes (MNs) capable of supporting only Simple IP.  
In addition to the parameters configured via this command, the HA-FA SPI(s) must also be modified to support Proxy Mobile IP. Refer to the *fa-ha-spi* command for more information.

**Example**  
The following command configures the FA service to wait up to 5 seconds for an HA to respond prior to re-sending an a Mobile IP Registration Request message:

```
proxy-mip retransmission-timeout 5
```

If the advertisement registration lifetime configured for the FA service is 900 seconds and you want the system to send a Proxy Mobile IP Registration Renewal Request message after 500 seconds, then the following command must be executed:

```
proxy-mip renew-percent-time 50
```
Note that $50 = (450 / 900) \times 100$. 

reg-timeout

Configures the FA registration reply timeout.

Product
PDSN
ASN-GW
GGSN
PDIF

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > FA Service Configuration
configure > context context_name > fa-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-fa-service)#

Syntax

```plaintext
reg-timeout time
```

- **time**
  - Default: 45
  - time is measured in seconds and can be configured to an integer from 1 through 65535.

Usage

Configure the amount of time that the FA service will wait for a Registration Reply from an HA before the call is rejected with a reply code of 78H (registration Timeout).

Example

The following command configures a registration timeout of 10.

```plaintext
reg-timeout 10
```
reverse-tunnel

Enables the use of reverse tunneling for a Mobile IP (MIP) sessions when requested by the mobile node (MN).

**Product**

PDSN
ASN-GW
GGSN

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > FA Service Configuration

```
configure > context context_name > fa-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name] host_name(config-fa-service) #
```

**Syntax**

```
[ no ] reverse-tunnel
```

- **no**
  
  Indicates the reverse tunnel option is to be disabled. When omitted, the reverse tunnel option is enabled.

**Usage**

Reverse tunneling involves tunneling datagrams originated by the MN to the HA via the FA service. When an MN arrives at a foreign network, it listens for agent advertisements and selects an FA that supports reverse tunnels. The MN requests this service when it registers through the selected FA. At this time, the MN may also specify a delivery technique such as Direct or the Encapsulating Delivery Style.

The advantages of using reverse-tunneling:

- All datagrams from the mobile node seem to originate from its home network
- The FA can keep track of the HA that the mobile node is registered to and tunnel all datagrams from the mobile node to its HA

Use the **no** option of this command to disable reverse tunneling. If reverse tunneling is disabled, and the mobile node does not request it, then triangular routing is used. The system defaults to reverse tunnel enabled.

**Important:** If reverse tunneling is disabled on the system and an MN requests it, the call will be rejected with a reply code of 74H (reverse-tunneling unavailable).

**Example**

The following command disables reverse-tunneling support for the FA service:

```
no reverse-tunnel
```
revocation

Enables the MIP revocation feature and configures revocation parameters.

**Product**
- PDSN
- ASN-GW
- GGSN
- PDIF

**Privilege**
- Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > FA Service Configuration

configure > context context_name > fa-service service_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-fa-service)#
```

**Syntax**

```
revocation { enable | max-retransmission number | negotiate-i-bit | retransmission-timeout secs | trigger internal-failure }
```

```
no revocation enable | trigger internal-failure | negotiate-i-bit
```

---

**no**
Completedly disables registration revocation on the FA.
Disables sending revocation messages to the HA when a session is affected by an internal task failure.

**enable**
Enables the MIP registration revocation feature on the FA. When enabled, if revocation is negotiated with an HA, and a MIP binding is terminated, the FA can send a Revocation message to the HA. This feature is disabled by default.

**max-retransmission number**
Default: 3
Specifies the maximum number of retransmissions of a Revocation message before the revocation fails.
`number` must be an integer from 0 through 10.

**negotiate-i-bit**
Default: disabled
Enables the FA to negotiate the i-bit via PRQ/RRP messages and processes the i-bit revocation messages.

**retransmission-timeout secs**
Default: 3
Specifies the number of seconds to wait for a Revocation Acknowledgement from the HA before retransmitting the Revocation message. `secs` must be an integer from 1 through 10.

```
trigger internal-failure
```

Default: disabled
Enable sending a revocation message to the HA for all sessions that are affected by an internal task failure.

**Usage**

Use this command to enable or disable the MIP revocation feature on the FA or to change settings for this feature. Both the HA and the FA must have Registration Revocation enabled and FA/HA authorization must be in use for Registration Revocation to be negotiated successfully.

**Example**

The following command enables Registration Revocation on the FA:

```
revocation enable
```

The following command sets the maximum number of retries for a Revocation message to 6:

```
revocation max-retransmission 6
```

The following command sets the timeout between retransmissions to 10:

```
revocation retransmission-timeout 10
```
threshold reg-reply-error

Set an alarm or alert based on the number of registration reply errors per FA service.

Product
PDSN
ASN-GW
GGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > FA Service Configuration
configure > context context_name > fa-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-fa-service)#

Syntax

threshold reg-reply-error high_thresh [ clear low_thresh ]

no threshold reg-reply-error

no

Deletes the alert or alarm.

high_thresh

Default: 0
The high threshold number of registration reply errors that must be met or exceeded within the polling interval to generate an alert or alarm. high_thresh can be an integer from 0 through 100000.

**Important:** You must enter a value between 1 and 100000 to trigger an alert/alarm.

clear low_thresh

Default: 0
The low threshold number of registration reply errors that must be met or exceeded within the polling interval to clear an alert or alarm. low_thresh can be an integer from 0 through 100000.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Important:** You must enter a value between 1 and 100000 to trigger an alert/alarm.
**Usage**

Use this command to set an alert or an alarm when the number of registration reply errors is equal to or greater than a specified number of calls per second.

Alerts or alarms are triggered for the number of registration reply errors on the following rules:

- **Enter condition**: Actual number of registration reply errors > High Threshold
- **Clear condition**: Actual number of registration reply errors £ Low Threshold

**Example**

The following command configures a registration reply error threshold of **1000** and a low threshold of **500** for a system using the Alarm thresholding model:

```
threshold reg-reply-error 1000 clear 500
```
Chapter 134
Firewall-and-NAT Action Configuration Mode Commands

The Firewall-and-NAT Action Configuration Mode enables configuring Stateful Firewall (FW) and Network Address Translation (NAT) actions.

Mode

Exec > ACS Configuration > Firewall-and-NAT Action Configuration

`active-charging service service_name > fw-and-nat action action_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-fw-and-nat-action)#
```

Important: This configuration mode is only available in release 11.0 and later releases. This configuration mode must be used to configure Action-based Stateful Firewall and NAT features.

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
end

Ends the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
```
end
```

**Usage**
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Use this command to return to the parent configuration mode.
flow check-point

This command checkpoints all the flows matching the Firewall-and NAT action.

**Product**
NAT

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Firewall-and-NAT Action Configuration

`active-charging service service_name > fw-and-nat action action_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-fw-and-nat-action)#
```

**Syntax**

```
flow check-point [ data-usage data_usage [ and | or ] | time-duration duration [ and | or ] ]
{ default | no } flow check-point
```

- **default**
  Configures the default Firewall action.

- **no**
  Deletes the Firewall action configuration.

- **data-usage data_usage**
  Specifies the data usage in bytes.
  `data_usage` must be an integer from 1 through 4294967295.
  The maximum limit for data-usage is 4 GB.

- **time-duration duration**
  Specifies the time duration in seconds.
  `duration` must be an integer from 1 through 86400.
  The maximum limit for time-duration is 24 hours.

- **and | or**
  This option allows to configure only `data-usage` or `time-duration`, or a combination of `data-usage` and `time-duration`.

**Usage**

Use this command to enable/disable the check-pointing of NATed flows and control the type of flows that need to be check pointed based on specified criteria. Check pointing is done only for TCP and UDP flows.
Example

The following command checkpoints flows with data-usage set to 5000 bytes and time duration set to 300 seconds:

    flow check-point data-usage 5000 and time-duration 300
Chapter 135
Firewall-and-NAT Policy Configuration Mode Commands

The Firewall-and-NAT Policy Configuration Mode enables configuring Stateful Firewall (FW) and Network Address Translation (NAT) policies.

Mode

Exec > ACS Configuration > Firewall-and-NAT Policy Configuration

`active-charging service service_name > fw-and-nat policy policy_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-fw-and-nat-policy)#
```

**Important**: This configuration mode is only available in 8.1, 9.0, and later releases. This configuration mode must be used to configure Policy-based Stateful Firewall and NAT features.

**Important**: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
access-rule

This command creates and configures an access rule.

**Product**
PSF
NAT

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Firewall-and-NAT Policy Configuration

```
active-charging service service_name > fw-and-nat policy policy_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-fw-and-nat-policy)#
```

**Syntax**

```

default access-rule no-ruledef-matches { downlink | uplink } action

no access-rule priority priority
```

**default**

Configures the default setting.
Default: Uplink direction: permit; Downlink direction: deny

**no**

Removes the access rule specified by the priority.

**no-ruledef-matches**

Configures action on packets with no ruledef match.

**downlink**

Specifies to act on downlink packets with no ruledef match.

**uplink**

Specifies to act on uplink packets with no ruledef match.
**action**
Specifies action to take on downlink/uplink packets with no ruledef match.

**deny**
Specifies to deny packets.

**permit**
Specifies to permit packets and allow the creation of data flows.

**charging-action charging_action**
Specifies the charging action. Optionally, a charging action can be configured for deny action. If a packet matches the deny rule, action is taken as configured in the charging action. If a charging action is specified, the content-ID and billing-action configured in the charging action are used. Also, the flow may be terminated (instead of just discarding the packet), if so configured in the specified charging action. **charging_action** must be an alphanumeric string of 1 through 63 characters.

**bypass-nat**

**Important:** In 9.0 and later releases, this keyword is NAT license dependent.

Specifies to bypass NAT.

**nat-realm nat_realm**

**Important:** In 9.0 and later releases, this keyword is NAT license dependent.

Specifies the NAT realm to be used to perform NAT on subscriber packets matching the access ruledef. If the NAT realm is not specified, NAT will be bypassed. That is, NAT will not be performed on subscriber packets that are matching a ruledef with no NAT realm name configured in it. **nat_realm** must be an alphanumeric string of 1 through 31 characters.

**priority priority**
Specifies priority of an access ruledef in the Firewall-and-NAT policy. **priority** must be an integer from 1 through 65535 that is unique for each access ruledef in the Firewall-and-NAT policy.

**[ dynamic-only | static-and-dynamic ] access-ruledef ruledef_name**
Specifies the access ruledef name. Optionally, the ruledef type can also be specified.
- **dynamic-only**: Dynamic Ruledef—Predefined ruledef that can be enabled/disabled by the policy server, and is disabled by default.
- **static-and-dynamic**: Static and Dynamic Ruledef—Predefined ruledef that can be enabled/disabled by the policy server, and is enabled by default.
- **access-ruledef ruledef_name**: Specifies the access ruledef name. **ruledef_name** must be an alphanumeric string of 1 through 63 characters.
**trigger open-port** { **port_number** | range **start_port** to **end_port** } **direction** { **both** | **reverse** | **same** }

---

**Important:** In 9.0 and later releases, this keyword is Stateful Firewall license dependent.

Optionally a port trigger can be specified to be used for this rule to limit the range of auxiliary data connections (a single or range of port numbers) for protocols having control and data connections (like FTP). The trigger port will be the destination port of an association which matches a rule.

- **port_number:** Specifies the auxiliary port number to open for traffic, and must be an integer from 1 through 65535.
- **range start_port to end_port:** Specifies the range of port numbers to open for subscriber traffic.
  - **start_port** must be an integer from 1 through 65535.
  - **end_port** must be an integer from 1 through 65535, and must be greater than **start_port**.
- **direction** { **both** | **reverse** | **same** }: Specifies the direction from which the auxiliary connection is initiated. This direction can be same as the direction of control connection, or the reverse of the control connection direction, or in both directions.
  - **both**: Provides the trigger to open port for traffic in either direction of the control connection.
  - **reverse**: Provides the trigger to open port for traffic in the reverse direction of the control connection (from where the connection is initiated).
  - **same**: Provides the trigger to open port for traffic in the same direction of the control connection (from where the connection is initiated).

**Usage**

Use this command to add access ruledefs to the Firewall-and-NAT policy and configure the priority and actions for rule matching.

The policy specifies the rules to be applied on calls. The ruledefs in the policy have priorities, based on which priority matching is done.

For Stateful Firewall, the port trigger configuration is optional, and can be configured only if a rule action is permit. When a rule is matched and the rule action is permit, if the trigger is configured, the appropriate check is made. The trigger port will be the destination port of an association that matches the rule. Multiple triggers can be defined for the same port number to permit multiple auxiliary ports for subscriber traffic. When a rule is matched and if the rule action is deny, the action taken depends on what is configured in the specified charging action. If the flow exists, flow statistics are updated and action is taken as configured in the charging action:

- If the billing action is configured as Event Data Record (EDR) enabled, an EDR is generated.
- If the content ID is configured, UDR information is updated.
- If the flow action is configured as “terminate-flow”, the flow is terminated instead of just discarding the packet.

If the billing action, content ID, and flow action are not configured, no action is taken on the dropped packets.

**Important:** For Stateful Firewall, only the terminate-flow action is applicable if configured in the specified charging action.

Allowing/dropping of packets is determined in the following sequence:
Firewall-and-NAT Policy Configuration Mode Commands

• Check is done to see if the packet matches any pinholes. If yes, no rule matching is done and the packet is allowed.
• Access ruledef matching is done. If a rule matches, the packet is allowed or dropped as per the `access-rule priority` configuration.
• If no access ruledef matches, the packet is allowed or dropped as per the `access-rule no-ruledef-matches` configuration.

For a packet dropped due to access ruledef match or no match (first packet of a flow), the charging action applied is the one configured in the `access-rule priority` or the `access-rule no-ruledef-matches` command respectively.

For action on packets dropped due to any error condition after data session is created, the charging action must be configured in the `flow any-error charging-action` command in the ACS Rulebase Configuration Mode.

The GGSN can dynamically activate or deactivate dynamic ruledefs for a subscriber based on the rule name received from a policy server. At rule match, if a rule in the policy is a dynamic rule, and if the rule is enabled for the particular subscriber, rule matching is done for the rule. If the rule is disabled for the particular subscriber, rule matching is not done for the rule.

Example

For Stateful Firewall, the following command assigns a priority of 10 to the access ruledef `test_rule`, adds it to the policy, and permits port trigger to be used for the rule to open ports in the range of 1000 to 2000 in either direction of the control connection:

```
access-rule priority 10 access-ruledef test_rule permit trigger open-port range 1000 to 2000 direction both
```
**end**

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
```
end
```

**Usage**
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Usage
Use this command to return to the parent configuration mode.
### firewall dos-protection

This command configures Stateful Firewall protection for subscribers from Denial-of-Service (DoS) attacks.

**Important:** In release 8.0, this configuration is available in the ACS Configuration Mode. In release 8.1, for Rulebase-based Stateful Firewall configuration, this configuration is available in the ACS Rulebase Configuration Mode. In release 8.3, this configuration is available in the ACS Rulebase Configuration Mode.

**Product**
- PSF

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > ACS Configuration > Firewall-and-NAT Policy Configuration

```
active-charging service service_name > fw-and-nat policy policy_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-fw-and-nat-policy)#
```

**Syntax**

```
```

- **default firewall dos-protection**

  ```
  no
  ```

  Disables Stateful Firewall protection for subscribers against the specified Denial of Service (DoS) attack(s).

- **default**

  ```
  no
  ```

  Disables Stateful Firewall protection for subscribers against all DoS attacks.

- **all**

  ```
  no all
  ```

  Enables Stateful Firewall protection for subscribers against all DoS attacks supported by the Stateful Firewall service. The IPv6 extension headers will be enabled only if the `firewall validate-ip-options` command is enabled in the Firewall-and-NAT policy configuration.

- **flooding { icmp | tcp-syn | udp }**

  ```
  no flooding { icmp | tcp-syn | udp }
  ```

  Enables protection against the specified flooding attack:
  - **icmp**: Enables protection against ICMP Flood attack.
  - **tcp-syn**: Enables protection against TCP Syn Flood attack.
• **udp**: Enables protection against UDP Flood attack.

---

**ftp-bounce**

Enables protection against FTP Bounce attacks.

---

**ip-unaligned-timestamp**

Enables protection against IP Unaligned Timestamp attacks.

---

**ipv6-dst-options [ invalid-options | unknown-options ]**

Drops IPv6 packets containing the IPv6 destination options extension header:

- The Tunnel Encapsulation Limit (option type: 0x04) is a destination option defined in RFC 2473.
- The Home Address option (option type: 0xC9) is part of Mobile IP processing defined in RFC 3775. This option is only valid as a Destination Option.
- The NSAP Address option (option type: 0xC3) is assigned as a Destination Option by RFC 1888 and deprecated (reclassified as historic) by RFC 4048.
- **invalid-options**: Drops IPv6 packets containing invalid IPv6 destination options.
  - The following values are invalid in a Destination Options extension header option type field. Packets with these options in a Destination Options header will be dropped.
    - Value 0xC2, Jumbo Payload
    - Value 0x05, Router Alert
    - Value 0x06, Quick start
    - Value 0x07, CALIPSO
- **unknown-options**: Drops IPv6 packets containing unknown IPv6 destination options.

---

**ipv6-extension-hdr [ limit extension_limit ]**

Default: 8

Limits the number of IPv6 extension headers in an IPv6 packet. An IPv6 packet can contain zero or more extension headers.

Firewall will not fully parse packets with unknown extension headers as the extension header format is unspecified. Under such cases, the transport protocol will be considered as **unknown**. Packets with invalid length field in the extension headers and packets with next header 0x01 (ICMPv4) will be dropped. IPv6 uses ICMPv6 of type 0x3A.

*extension_limit* must be an integer from 0 through 4294967295.

---

**ipv6-frag-hdr nested-fragmentation**

Drops IPv6 packets containing nested fragmentation (reassembled packets containing a fragment header). IPv6 fragmentation is done only by the source node. An IPv6 fragment packet must have only one fragment header. Firewall will drop packets with more than one fragment header. The Reassembled packet containing a fragment header will be dropped by Firewall. As per RFC 2460, the fragment length (except for last fragment) must be a multiple of 8 octets. If not, such fragments are dropped.

---

**ipv6-hop-by-hop [ invalid-options | jumbo-payload | router-alert | unknown-options ]**

Drops IPv6 packets containing the hop-by-hop extension header.
The Hop-by-Hop Options extension header, if present, must be the first header to follow the IPv6 main header. This is indicated by a value of 0x00 in the next header field in the main header. The length must be expressed as a multiple of 8 octets (excluding the first 8 octets). If not, such packets will be dropped.

- **invalid-options**: Drops IPv6 packets containing invalid IPv6 hop-by-hop options.

  The following values are invalid in a Hop-by-Hop extension header option type field. Packets with these options in a hop-by-hop header will be dropped.
  - Value 0x04, Tunnel Encapsulation limit
  - Value 0xC9, Home Address Destination option
  - Value 0xC3, NSAP Address option

  The options are present in TLV (Type Length Value) format. If the length specified is invalid, then such packets will be dropped.

- **jumbo-payload**: Drops IPv6 packets with jumbo payload hop-by-hop options.

  The Jumbo Payload option (RFC 2675) has the option type value 0xC2 and is only valid as a Hop-by-Hop option. This option allows the creation of very large IP packets (packets larger than 65K bytes). If this option is allowed, the following validity checks will be done.
  - The IP payload length must be 0x00 when the Jumbo Payload option is present.
  - The Jumbo Payload option must be used only when the length is greater than 65,535; the two most significant bytes of the Jumbo length cannot be 0x00.
  - The Jumbo Payload option cannot be used in conjunction with a Fragmentation extension header.

  If any of the above checks fail, then the IPv6 packet will be dropped. The Option Type field must have $4n+2$ alignment.

- **router-alert**: Drops IPv6 packets with router alert hop-by-hop options.

  The Router Alert (RFC 2711) option is used to signal the routers that a closer inspection of the packet is warranted. Denial of service (DoS) attacks can occur if an attacker sends large number of packets with this option. Only one option of this type must be present, regardless of value, per Hop-by-Hop header with $2n + 0$ alignment.

- **unknown-options**: Drops IPv6 packets containing unknown IPv6 hop-by-hop options.

---

**mime-flood**
Enables protection against HTTP Multiple Internet Mail Extension (MIME) header flooding attacks.

**port-scan**
Enables protection against Port Scan attacks.

**tcp-window-containment**
Enables protection against TCP sequence number out-of-range attacks.

**source-router**
Enables protection against IPv4/IPv6 Source Route IP Option attacks.
This command can be used to filter IPv4/IPv6 packets containing Routing header of Type 0 (source routing). In this release, only type 0 filtering is supported.
**teardrop**

Enables protection against IPv4/IPv6 Teardrop attacks.

**winnuke**

Enables protection against WIN-NUKE attacks.

**Usage**

Use this command to enable Stateful Firewall protection from different types of DoS attacks. This command can be used multiple times for different DoS attacks.

**Important:** DoS attacks are detected only in the downlink direction.

**Example**

The following command enables protection from all supported DoS attacks:

```
firewall dos-protection all
```
firewall flooding

This command configures Stateful Firewall protection from Packet Flooding attacks.

Important: In release 8.0, this configuration is available in the ACS Configuration Mode. In release 8.1, for Rulebase-based Stateful Firewall configuration, this configuration is available in the ACS Rulebase Configuration Mode. In release 8.3, this configuration is available in the ACS Rulebase Configuration Mode.

Product
PSF

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Firewall-and-NAT Policy Configuration
active-charging service service_name > fw-and-nat policy policy_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-fw-and-nat-policy)#

Syntax

```
firewall flooding { protocol { icmp | tcp-syn | udp } packet limit packets | sampling-interval interval } 

default firewall flooding { protocol { icmp | tcp-syn | udp } packet limit | sampling-interval }
```

default

Configures the default setting for the specified configuration.

```
protocol { icmp | tcp-syn | udp }
```

Specifies the transport protocol:

- `icmp`: Configuration for ICMP protocol.
- `tcp-syn`: Configuration for TCP-SYN packet limit.
- `udp`: Configuration for UDP protocol.

```
packet limit packets
```

Specifies the maximum number of specified packets a subscriber can receive during a sampling interval. `packets` must be an integer from 1 through 4294967295.
Default: 1000 packets per sampling interval for all protocols.

```
sampling-interval interval
```

Specifies the flooding sampling interval, in seconds. `interval` must be an integer from 1 through 60.
Default: 1 second
The maximum sampling-interval configurable is 60 seconds.
Usage

Use this command to configure the maximum number of ICMP, TCP-SYN, / UDP packets allowed to prevent the packet flooding attacks to the host.

Example

The following command ensures a subscriber will not receive more than 1000 ICMP packets per sampling interval:

```
firewall flooding protocol icmp packet limit 1000
```

The following command ensures a subscriber will not receive more than 1000 UDP packets per sampling interval on different 5-tuples. That is, if an attacker is sending lot of UDP packets on different ports or using different spoofed IP addresses, those packets will be limited to 1000 packets per sampling interval. This way only “suspected” malicious packets are limited and not “legitimate” packets.

```
firewall flooding protocol udp packet limit 1000
```

The following command ensures a subscriber will not receive more than 1000 TCP-Syn packets per sampling interval:

```
firewall flooding protocol tcp-syn packet limit 1000
```

The following command specifies a flooding sampling interval of 1 second:

```
firewall flooding sampling-interval 1
```
**firewall icmp-checksum-error**

This command configures Stateful Firewall action on packets with ICMP/ICMPv6 Checksum errors.

**Product**
PSF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Firewall-and-NAT Policy Configuration

```bash
active-charging service service_name > fw-and-nat policy policy_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-fw-and-nat-policy)#
```

**Syntax**

```bash
firewall icmp-checksum-error { drop | permit }
```

**default firewall icmp-checksum-error**

```bash
default
```

Configures the default setting.
Default: drop

```bash
drop
```

Drops packets with ICMP/ICMPv6 Checksum errors.

```bash
permit
```

Permits packets with ICMP/ICMPv6 Checksum errors.

**Usage**

Use this command to configure Stateful Firewall action on packets with ICMP/ICMPv6 Checksum errors. This command also applies to ICMP/ICMPv6 packets with Inner IP Checksum error. For NAT-only calls, packets with ICMP/ICMPv6 errors are dropped, and other packets are allowed.

**Example**

The following command configures Stateful Firewall to drop packets with ICMP/ICMPv6 Checksum errors:

```bash
firewall icmp-checksum-error drop
```
firewall icmp-destination-unreachable-message-threshold

This command configures a threshold on the number of ICMP/ICMPv6 error messages sent by the subscriber for a particular data flow.

Important: In release 8.0, this configuration is available in the ACS Configuration Mode. In release 8.1, for Rulebase-based Stateful Firewall configuration, this configuration is available in the ACS Rulebase Configuration Mode. In release 8.3, this configuration is available in the ACS Rulebase Configuration Mode.

Product:
PSF

Privilege:
Security Administrator, Administrator

Mode:
Exec > ACS Configuration > Firewall-and-NAT Policy Configuration

active-charging service service_name > fw-and-nat policy policy_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-fw-and-nat-policy)#

Syntax:

firewall icmp-destination-unreachable-message-threshold messages then-block-server

{ default | no } firewall icmp-destination-unreachable-message-threshold

default
Conf...
The following command configures a threshold of 10 ICMP/ICMPv6 error messages:

```
firwall icmp-destination-unreachable-message-threshold 10 then-block-server
```
firewall icmp-echo-id-zero

This command configures Stateful Firewall action on echo packets with ICMP/ICMPv6 ID zero.

Product
PSF

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Firewall-and-NAT Policy Configuration
active-charging service service_name > fw-and-nat policy policy_name

Entering the above command sequence results in the following prompt:
[local]host_name(config-fw-and-nat-policy)#

Syntax

firewall icmp-echo-id-zero { drop | permit }

default firewall icmp-echo-id-zero

default
Configures the default setting.
Default: permit

drop
Drops packets with ICMP/ICMPv6 ID zero.

permit
Permits packets with ICMP/ICMPv6 ID zero.

Usage
Use this command to configure Stateful Firewall action on echo packets with ICMP/ICMPv6 ID zero.

Example
The following command configures Stateful Firewall to drop packets with ICMP/ICMPv6 ID zero:

firewall icmp-echo-id-zero drop
**firewall icmp-fsm**

This command enables/disables Stateful Firewall’s ICMP/ICMPv6 Finite State Machine (FSM).

**Product**
PSF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Firewall-and-NAT Policy Configuration

```
active-charging service service_name > fw-and-nat policy policy_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-fw-and-nat-policy)#
```

**Syntax**

```
[ default | no ] firewall icmp-fsm
```

- **default**
  Configures the default setting.
  Default: Enabled. Same as **firewall icmp-fsm**.

- **no**
  Disables Stateful Firewall ICMP/ICMPv6 FSM checks.

**Usage**

Use this command to enable/disable Stateful Firewall ICMP/ICMPv6 FSM checks. When Stateful Firewall and ICMP/ICMPv6 FSM are enabled, ICMP/ICMPv6 reply messages for which there is no saved ICMP/ICMPv6 request message are discarded. ICMP/ICMPv6 error messages (i.e., messages containing an embedded message) for which there is no saved flow for the embedded message are discarded.

**Example**

The following command disables Stateful Firewall’s ICMP/ICMPv6 FSM checks:

```
no firewall icmp-fsm
```
firewall ip-reassembly-failure

This command configures Stateful Firewall action on IPv4/IPv6 packets involved in IP Reassembly Failure scenarios.

**Product**
PSF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Firewall-and-NAT Policy Configuration

**Syntax**
```
firewall ip-reassembly-failure { drop | permit }
```

**Usage**
Use this command to configure Stateful Firewall action on IPv4/IPv6 packets involved in IP reassembly failure scenarios such as missing fragments, overlapping offset, etc. For NAT-only calls, packets involved in IP reassembly failure scenarios are dropped.

**Example**
The following command specifies to drop IPv4/IPv6 packets involved in IP reassembly failure scenarios:
```
firewall ip-reassembly-failure drop
```
**firewall malformed-packets**

This command configures Stateful Firewall action on malformed packets. In release 12.0, this command supports ICMPv6 and IPv6 packets.

**Product**
PSF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Firewall-and-NAT Policy Configuration

```bash
active-charging service service_name > fw-and-nat policy policy_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-fw-and-nat-policy)#
```

**Syntax**

```bash
firewall malformed-packets { drop | permit }
```

**default firewall malformed-packets**

```
default
Configures the default setting.
Default: permit

drop
Drops malformed packets.

permit
Permits malformed packets.
```

**Usage**

Use this command to configure Stateful Firewall action on malformed packets. For NAT-only calls, malformed packets are always permitted.

**Example**

The following command specifies Stateful Firewall to drop malformed packets:

```
firewall malformed-packets drop
```
**firewall max-ip-packet-size**

This command configures the maximum IPv4/IPv6 packet size (after IP reassembly) allowed over Stateful Firewall.

<table>
<thead>
<tr>
<th><strong>Important:</strong> In release 8.0, this configuration is available in the ACS Configuration Mode. In release 8.1, for Rulebase-based Stateful Firewall configuration, this configuration is available in the ACS Rulebase Configuration Mode. In release 8.3, this configuration is available in the ACS Rulebase Configuration Mode.</th>
</tr>
</thead>
</table>

**Product**

PSF

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > ACS Configuration > Firewall-and-NAT Policy Configuration

```
active-charging service service_name > fw-and-nat policy policy_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-fw-and-nat-policy)#
```

**Syntax**

```
firewall max-ip-packet-size packet_size protocol { icmp | non-icmp }

default firewall max-ip-packet-size protocol { icmp | non-icmp }
```

**default**

Configures the default setting.

Default: 65535 bytes (for both ICMP/ICMPv6 and non-ICMP/ICMPv6)

**packet_size**

Specifies the maximum packet size allowed by firewall. Any IPv6 packet with payload size greater than the configured value will be dropped.

*packet_size* must be an integer from 30000 through 65535.

**protocol { icmp | non-icmp }**

Specifies the transport protocol:

- **icmp**: Configuration for ICMP/ICMPv6 protocol.
- **non-icmp**: Configuration for protocols other than ICMP/ICMPv6.

**Usage**

Use this command to configure the maximum IPv4/IPv6 packet size allowed for ICMP/ICMPv6 and non-ICMP/ICMPv6 packets to prevent packet flooding attacks to the host. Packets exceeding the configured size will be dropped for “Jolt” and “Ping-Of-Death” attacks.

**Example**

The following command allows a maximum packet size of **60000** for ICMP/ICMPv6 protocol:
firewall max-ip-packet-size 60000 protocol icmp
**firewall mime-flood**

This command configures Stateful Firewall protection from MIME Flood attacks.

**Important:** In release 8.0, this configuration is available in the ACS Configuration Mode. In release 8.1, for Rulebase-based Stateful Firewall configuration, this configuration is available in the ACS Rulebase Configuration Mode. In release 8.3, this configuration is available in the ACS Rulebase Configuration Mode.

**Product**
PSF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Firewall-and-NAT Policy Configuration

```
active-charging service service_name > fw-and-nat policy policy_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-fw-and-nat-policy)#
```

**Syntax**

```
firewall mime-flood { http-headers-limit max_limit | max-http-header-field-size max_size }

default firewall mime-flood { http-headers-limit | max-http-header-field-size }
```

**default**
Configures the default setting for the specified parameter.

```
http-headers-limit max_limit
```

Specifies the maximum number of headers allowed in an HTTP packet. If the number of HTTP headers in a page received is more than the specified limit, the request will be denied.

*max_limit* must be an integer from 1 through 256.

Default: 16

```
max-http-header-field-size max_size
```

Specifies the maximum header field size allowed in the HTTP header, in bytes. If the size of HTTP header in the received page is more than the specified number of bytes, the request will be denied.

*max_size* must be an integer from 1 through 8192.

Default: 4096 bytes

**Usage**
Use this command to configure the maximum number of headers allowed in an HTTP packet, and the maximum header field size allowed in the HTTP header to prevent MIME flooding attacks.
This command is only effective if Stateful Firewall DoS protection for MIME flood attacks has been enabled using the `firewall dos-protection mime-flood` command, and the `route` command has been configured to send HTTP packets to the HTTP analyzer.

**Example**

The following command sets the maximum number of headers allowed in an HTTP packet to 100:

```
firewall mime-flood http-headers-limit 100
```

The following command sets the maximum header field size allowed in the HTTP header to 1000 bytes:

```
firewall mime-flood max-http-header-field-size 1000
```
**firewall policy**

This command enables/disables Stateful Firewall support in a Firewall-and-NAT policy.

---

### Important:
In release 8.0, this configuration is available in the ACS Configuration Mode. In release 8.1, for Rulebase-based Stateful Firewall configuration, this configuration is available in the ACS Rulebase Configuration Mode. In release 8.3, this configuration is available in the ACS Rulebase Configuration Mode.

#### Product
PSF

#### Privilege
Security Administrator, Administrator

#### Mode
Exec > ACS Configuration > Firewall-and-NAT Policy Configuration

`active-charging service service_name > fw-and-nat policy policy_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-fw-and-nat-policy)#
```

#### Syntax

In 11.0 and earlier releases:

```
firewall policy firewall-required
```

```
no firewall policy
```

In 12.0 and later releases:

```
firewall policy { ipv4-and-ipv6 | ipv4-only | ipv6-only }
```

```
{ default | no } firewall policy
```

---

**default**

Disables IPv4 and IPv6 Stateful Firewall support in the Firewall-and-NAT policy.

---

**no**

Disables IPv4 and IPv6 Stateful Firewall support in the Firewall-and-NAT policy.

---

**firewall-required**

Enables Stateful Firewall support in the Firewall-and-NAT policy.

---

### Important:
This keyword is available only in 11.0 and earlier releases.

---

**ipv4-and-ipv6**

Enables both IPv4 and IPv6 Stateful Firewall support in the Firewall-and-NAT policy.
**ipv4-only**
Enables IPv4 Stateful Firewall and disables IPv6 Stateful Firewall in the Firewall-and-NAT policy.

**ipv6-only**
Enables IPv6 Stateful Firewall and disables IPv4 Stateful Firewall support in the Firewall-and-NAT policy.

**Usage**
Use this command to enable/disable IPv4 and/or IPv6 Stateful Firewall support for all subscribers using a Firewall-and-NAT policy.

**Example**
The following command enables IPv4 and IPv6 Stateful Firewall support in a Firewall-and-NAT policy:

```bash
firewall policy ipv4-and-ipv6
```

The following command disables Stateful Firewall support in a Firewall-and-NAT policy:

```bash
no firewall policy
```
firewall tcp-checksum-error

This command configures Stateful Firewall action on packets with TCP Checksum error.

Product
PSF

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Firewall-and-NAT Policy Configuration

active-charging service service_name > fw-and-nat policy policy_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-fw-and-nat-poly)#

Syntax

firewall tcp-checksum-error { drop | permit }

default firewall tcp-checksum-error

default

Configures the default setting.
Default: drop

drop

Drops packets with TCP Checksum errors.

permit

Permits packets with TCP Checksum errors.

Usage

Use this command to configure Stateful Firewall action on packets with TCP Checksum error. For NAT-only calls, packets with TCP Checksum errors are permitted.

Example

The following command specifies Stateful Firewall to drop packets with TCP Checksum errors:

    firewall tcp-checksum-error drop
**firewall tcp-first-packet-non-syn**

This command configures Stateful Firewall action on TCP flows starting with a non-SYN packet.

**Important:** In release 9.0, this command is deprecated. This configuration is available as the `firewall tcp-fsm [first-packet-non-syn {drop | permit | send-reset}]` command.

### Product
PSF

### Privilege
Security Administrator, Administrator

### Mode
Exec > ACS Configuration > Firewall-and-NAT Policy Configuration

```
active-charging service service_name > fw-and-nat policy policy_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-fw-and-nat-policy)#
```

### Syntax
```
firewall tcp-first-packet-non-syn { drop | reset }
```

```
default firewall tcp-first-packet-non-syn
```

**default**
Configures the default setting.
Default: `drop`

**drop**
Drops the non-SYN packet.

**reset**
Sends reset.

### Usage
Use this command to configure Stateful Firewall action on TCP flows starting with a non-SYN packet.

### Example
For flows starting with a non-SYN packet, the following command specifies Stateful Firewall to drop the non-SYN packet:

```
firewall tcp-first-packet-non-syn drop
```
**firewall tcp-fsm**

This command enables/disables Stateful Firewall’s TCP Finite State Machine (FSM).

**Product**
PSF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Firewall-and-NAT Policy Configuration

**Syntax**

```
firewall tcp-fsm [ first-packet-non-syn { drop | permit | send-reset } ]
{ default | no } firewall tcp-fsm
```

- **default**
  Configures the default setting.
  Default: drop

- **no**
  Disables Stateful Firewall’s TCP FSM.

**Usage**

Use this command to enable/disable Stateful Firewall’s TCP FSM checks. When Stateful Firewall and TCP FSM are enabled, state of the TCP session is checked to decide whether to forward TCP packets.

**Example**

The following command enables TCP FSM, and configures action to take on TCP flows starting with a non-SYN packet to drop the packet:

```
firewall tcp-fsm first-packet-non-syn drop
```
### firewall tcp-idle-timeout-action

This command configures action on TCP idle timeout expiry.

**Important:** In release 9.0 and later this command is also available to NAT.

**Product**
- PSF
- NAT

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > ACS Configuration > Firewall-and-NAT Policy Configuration

```
activate-charging service service_name > fw-and-nat policy policy_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-fw-and-nat-policy)#
```

**Syntax**

```
firewall tcp-idle-timeout-action { drop | reset }
{ default | no } firewall tcp-idle-timeout-action
```

- **default**
  - Configures the default setting.
  - Default: reset

- **no**
  - Configures the TCP idle timeout expiry action to reset.

- **drop**
  - Drops the session on TCP idle timeout expiry.

- **reset**
  - Resends TCP RST on TCP idle timeout expiry. When configured to reset, the session is dropped, and the system can avoid packets arriving for the idle flow from getting dropped.

**Usage**

Use this command to configure action to take on TCP idle timeout expiry.

**Example**

The following command configures action to take on TCP idle timeout expiry to drop:

```
firewall tcp-idle-timeout-action drop
```
firewall tcp-options-error

This command configures Stateful Firewall action on packets with TCP Option errors.

Product
PSF

Privileges
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Firewall-and-NAT Policy Configuration

active-charging service service_name > fw-and-nat policy policy_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-fw-and-nat-policy)#

Syntax

firewall tcp-options-error { drop | permit }

default firewall tcp-options-error

---

default
Configures the default setting.
Default: permit

---

drop
Drops packets with TCP Option errors.

---

permit
Permits packets with TCP Option errors.

Usage
Use this command to configure Stateful Firewall action on packets with TCP Option errors.

Example

The following command configures Stateful Firewall to drop packets with TCP Option errors:

    firewall tcp-options-error drop
**firewall tcp-partial-connection-timeout**

This command configures action on idle timeout for partially open TCP connections.

**Product**
PSF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Firewall-and-NAT Policy Configuration

```
active-charging service service_name > fw-and-nat policy policy_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-fw-and-nat-policy)#
```

**Syntax**

```
firewall tcp-partial-connection-timeout timeout

{ default | no } firewall tcp-partial-connection-timeout
```

- **default**
  Configures the default setting.

- **no**
  Disables the idle timeout for partially open TCP connections.

- **timeout**
  Specifies the timeout in seconds.
  
  *timeout* must be an integer from 0 through 86400.
  Default: 30 seconds

**Usage**

Use this command to configure idle timeout for TCP connections that are yet to be established (partially open) in the case of Firewall enabled calls.

**Example**

The following command sets the idle timeout setting to 30 seconds:

```
firewall tcp-partial-connection-timeout 30
```
firewall tcp-reset-message-threshold

This command configures a threshold on the number of TCP reset messages sent by the subscriber for a particular data flow. After this threshold is reached, further downlink traffic to the subscriber on the unwanted flow is blocked.

**Product**
PSF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Firewall-and-NAT Policy Configuration

```
active-charging service service_name > fw-and-nat policy policy_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-fw-and-nat-policy)#
```

**Syntax**

```
firewall tcp-reset-message-threshold messages then-block-server

{ default | no } firewall tcp-reset-message-threshold
```

---

| { default | no } |
|----------------|
| **default**    |
| Configures the default setting. |
| Default: Disabled |

<p>| |</p>
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>no</strong></td>
</tr>
<tr>
<td>Disables the configuration.</td>
</tr>
</tbody>
</table>

**messages**

Specifies the threshold on the number of TCP reset messages sent by the subscriber for a particular data flow. **messages** must be an integer from 1 through 100.

**Usage**

Use this command to configure a threshold on the number of TCP reset messages (TCP RST+ACK) sent by the subscriber for a particular data flow. After the threshold is reached, assuming the server is not reacting properly to the reset messages further downlink traffic to the subscriber on the unwanted flow is blocked.

This configuration enables QCHAT noise suppression for TCP.

**Example**

The following command sets the threshold on the number of TCP reset messages to 10:

```
firewall tcp-reset-message-threshold 10 then-block-server
```
**firewall tcp-syn-flood-intercept**

This command configures TCP SYN intercept parameters for protection against TCP SYN flooding attacks.

**Important:** In release 8.0, this configuration is available in the ACS Configuration Mode. In release 8.1, for Rulebase-based Stateful Firewall configuration, this configuration is available in the ACS Rulebase Configuration Mode. In release 8.3, this configuration is available in the ACS Rulebase Configuration Mode.

---

**Product**

PSF

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > ACS Configuration > Firewall-and-NAT Policy Configuration

`active-charging service service_name > fw-and-nat policy policy_name`

Entering the above command sequence results in the following prompt:

`[local]host_name(config-fw-and-nat-policy)#`

**Syntax**

```plaintext
firewall tcp-syn-flood-intercept { mode { none | watch [ aggressive ] } | watch-timeout intercept_watch_timeout }

default firewall tcp-syn-flood-intercept { mode | watch-timeout }
```

**default**

Configures the default settings for SYN Flood DoS protection.

**mode { none | watch [ aggressive ] }**

Specifies the TCP SYN flood intercept mode:

- **none**: Disables the TCP SYN Flood Intercept feature.
- **watch**: Configures TCP SYN flood intercept feature in watch mode. The Stateful Firewall passively watches to see if TCP connections become established within a configurable interval. If connections are not established within the timeout period, the Stateful Firewall clears the half-open connections by sending RST to TCP client and server. The default watch-timeout for connection establishment is 30 seconds.
- **aggressive**: Configures TCP SYN flood Intercept or Watch feature for aggressive behavior. Each new connection request causes the oldest incomplete connection to be deleted. When operating in watch mode, the watch timeout is reduced by half. If the watch-timeout is 30 seconds, under aggressive conditions it becomes 15 seconds. When operating in intercept mode, the retransmit timeout is reduced by half (i.e. if the timeout is 60 seconds, it is reduced to 30 seconds). Thus the amount of time waiting for connections to be established is reduced by half (i.e. it is reduced to 150 seconds from 300 seconds under aggressive conditions).

Default: none
watch-timeout intercept_watch_timeout

Specifies the TCP intercept watch timeout, in seconds.

*intercept_watch_timeout* must be an integer from 5 through 30.
Default: 30

**Usage**

This TCP intercept functionality provides protection against TCP SYN Flooding attacks. This command enables and configures TCP intercept parameters to prevent TCP SYN flooding attacks by intercepting and validating TCP connection requests for DoS protection mechanism configured with the *dos-protection* command.

The system captures TCP SYN requests and responds with TCP SYN-ACKs. If a connection initiator completes the handshake with a TCP ACK, the TCP connection request is considered as valid by system and system forwards the initial TCP SYN to the valid target which triggers the target to send a TCP SYN-ACK. Now system intercepts with TCP SYN-ACK and sends the TCP ACK to complete the TCP handshake. Any TCP packet received before the handshake completion will be discarded.

**Example**

The following command sets the intercept watch timeout setting to 15 seconds:

```
firewall tcp-syn-flood-intercept watch-timeout 15
```
firewall tcp-syn-with-ecn-cwr

This command configures Stateful Firewall action on TCP SYN packets with either ECN or CWR flag set.

Product
PSF

Privileges
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Firewall-and-NAT Policy Configuration

active-charging service service_name > fw-and-nat policy policy_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-fw-and-nat-policy)#

Syntax

firewall tcp-syn-with-ecn-cwr { drop | permit }

default firewall tcp-syn-with-ecn-cwr

default
Confures the default setting.
Default: permit

drop
Drops TCP SYN packets with either ECN or CWR flag set.

permit
Permits TCP SYN packets with either ECN or CWR flag set.

Usage

Use this command to configure Stateful Firewall action on receiving a TCP SYN packet with either ECN or CWR flag set.

Example

The following command configures Stateful Firewall to drop TCP SYN packets with ECN / CWR flag set:

firewall tcp-syn-with-ecn-cwr drop
firewall udp-checksum-error

This command configures Stateful Firewall action on packets with UDP Checksum error.

**Product**
PSF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Firewall-and-NAT Policy Configuration

active-charging service service_name > fw-and-nat policy policy_name

Entering the above command sequence results in the following prompt:

`[local]host_name(config-fw-and-nat-policy)#`

**Syntax**

```
firewall udp-checksum-error { drop | permit }
default firewall udp-checksum-error
```

<table>
<thead>
<tr>
<th>default</th>
<th>Configures the default setting. Default: drop</th>
</tr>
</thead>
<tbody>
<tr>
<td>drop</td>
<td>Drops packets with UDP Checksum error.</td>
</tr>
<tr>
<td>permit</td>
<td>Permits packets with UDP Checksum error.</td>
</tr>
</tbody>
</table>

**Usage**
Use this command to configure Stateful Firewall action on packets with UDP Checksum error. For NAT-only calls, packets with UDP Checksum error are permitted.

**Example**
The following command specifies to drop packets with UDP Checksum error:

```
firewall udp-checksum-error drop
```
firewall validate-ip-options

This command enables / disables the Stateful Firewall validation of IP options for errors.

Product
PSF

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Firewall-and-NAT Policy Configuration

active-charging service service_name > fw-and-nat policy policy_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-fw-and-nat-policy)#

Syntax

[ default | no ] firewall validate-ip-options

default
Configures the default setting.
Default: Disabled. Same as no firewall validate-ip-options

no
Disables validation of IP options.

Usage
Use this command to enable / disable Stateful Firewall validation of IP options. When enabled, Stateful Firewall will drop packets with IP option errors.
For NAT calls, validation of IP Options is disabled.

Example
The following command enables validation of IP options:

firewall validate-ip-options
nat binding-record

This command configures the generation of NAT Binding Records.

Product
NAT

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Firewall-and-NAT Policy Configuration

`active-charging service service_name > fw-and-nat policy policy_name`

Enter the above command sequence results in the following prompt:

```
[local]host_name(config-fw-and-nat-policy)#
```

Syntax

```
nat binding-record edr-format edr_format [ port-chunk-allocation ] [ port-chunk-release ]

{ default | no } nat binding-record
```

- **default**
  - Configures the default setting.
  - Default: `port-chunk-release`

- **no**
  - Disables generating NAT Binding Records.

- **edr-format edr_format**
  - Specifies the Event Data Record (EDR) format name.
  - `edr_format` must be an alphanumeric string of 1 through 63 characters.

- **port-chunk-allocation**
  - Specifies generating NAT Binding Records when a port-chunk is allocated.

- **port-chunk-release**
  - Specifies generating NAT Binding Record when a port-chunk is released.

Usage

Use this command to configure the generation of NAT Binding Records.

Example

The following command configures an EDR format named `test123` and specifies generating NAT Binding Records when a port chunk is allocated:

```
nat binding-record edr-format test123 port-chunk-allocation
```
nat check-point-info

This command enables or disables the checkpointing of basic NAT, H323 and SIP ALG recovery. ICSR recovery can also be enabled or disabled for basic NAT and SIP flows.

Product
PSF
NAT

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Firewall-and-NAT Policy Configuration

active-charging service service_name > fw-and-nat policy policy_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-fw-and-nat-policy)#

Syntax

[ default | no ] nat check-point-info { basic [ icsr-also | limit-flows limit ] | h323-alg | sip-alg [ icsr-also ] }

- **default**
  - Configures this command with its default setting.
  - Default: Disabled

- **no**
  - Disables the basic NAT recovery and stand-alone H323 ALG and SIP ALG recovery. Also disables ICSR recovery for SIP ALG.

- **basic [ icsr-also | limit-flows limit ]**
  - Configures the basic flow checkpointing information.
  - *icsr-also*: Enables checkpointing for ICSR.
  - *limit-flows*: Limits the specified flows for basic NAT checkpointing. limit must be an integer from 1 through 100.
    - Default: 100

- **h323-alg**
  - Enables checkpointing of H323 ALG.

- **sip-alg [ icsr-also ]**
  - Enables checkpointing of SIP ALG.
    - *icsr-also*: Enables checkpointing for ICSR.
Usage

Use this command to enable or disable the checkpointing of basic NAT, standalone H323 and SIP ALG recovery. ICSR recovery can also be enabled or disabled for basic NAT and SIP flows. The maximum basic flows that can be checkpointed is also configured. By default, 100 flows can be recovered in a standalone chassis and ICSR setup.

Example

The following command enables basic NAT recovery and ICSR recovery with flows limited to 10:

```
nat check-point info basic limit-flows 10 icsr-also
```
nat icsr-flow-recovery

This command enables/disables the NAT ICSR Flow checkpointing support for subscribers in a Firewall-and-NAT policy. This command is deprecated in StarOS 14.0 and later releases, and is replaced by the `nat check-point-info` command.

**Product**
NAT

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Firewall-and-NAT Policy Configuration

```
active-charging service service_name > fw-and-nat policy policy_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-fw-and-nat-policy)#
```

**Syntax**

```
[ default | no ] nat icsr-flow-recovery
```

`default`
Configures the default setting.
Default: Disabled. Same as `no icsr-flow-recovery`.

`no`
Disables the NAT ICSR Flow checkpointing.

**Usage**
Use this command to enable/disable all NAT ICSR Flow checkpointing for subscribers using this policy.

**Example**
The following command enables NAT ICSR Flow checkpointing:

```
nat icsr-flow-recovery
```
nat policy

This command enables/disables Network Address Translation (NAT) support in a Firewall-and-NAT policy.

**Important:** In release 8.3, this configuration is available in the ACS Rulebase Configuration Mode.

**Product**
NAT

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Firewall-and-NAT Policy Configuration

```
active-charging service service_name > fw-and-nat policy policy_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-fw-and-nat-policy)#
```

**Syntax**

In 12.1 and earlier releases:

```
nat policy nat-required [ default-nat-realm nat_realm_name [ fw-and-nat-action action_name ] ]
```

```
no nat policy
```

In 12.2 and later releases:

```
nat policy [ ipv4-and-ipv6 | ipv4-only | ipv6-only ] [ default-nat-realm nat_realm_name [ fw-and-nat-action action_name ] ]
```

```
no nat policy
```

```
no
```

Disables both NAT44 and NAT64 support in the Firewall-and-NAT policy.

```
nat-required
```

Enables NAT support in the Firewall-and-NAT policy.

**Important:** This keyword is available only in 12.1 and earlier releases, and is supported in release 12.2 for backward compatibility. The `nat policy nat-required` command enables only NAT44.

```
ipv4-and-ipv6
```

Enables NAT processing for both IPv4 and IPv6 in the Firewall-and-NAT policy.

```
ipv4-only
```

Enables NAT processing for IPv4 in the Firewall-and-NAT policy.
**ipv6-only**

Enables NAT processing for IPv6 in the Firewall-and-NAT policy.

**default-nat-realm nat_realm_name**

Specifies the default NAT realm for the Firewall-and-NAT policy. 

`nat_realm_name` must be the name of an existing NAT realm, and must be an alphanumeric string of 1 through 31 characters.

**fw-and-nat-action action_name**

Specifies the Firewall-and-NAT action name.

`action_name` must be an alphanumeric string of 1 through 63 characters.

---

**Usage**

Use this command to enable/disable IPv4 and/or IPv6 NAT support for all subscribers using a Firewall-and-NAT policy.

In release 8.1, to enable NAT support for a subscriber, Stateful Firewall must also be enabled for that subscriber. See the `firewall policy` CLI command.

Once NAT is enabled for a subscriber, the NAT IP address to be used is chosen from the NAT realms specified in the rules. See the `access-rule` CLI command.

You can enable/disable NAT at any time, however the changed NAT status will not be applied to active calls. The new NAT status will only be applied to new calls.

---

**Example**

The following command enables NAT support in a Firewall-and-NAT policy:

```
nat policy nat-required
```

The following command disables NAT support in a Firewall-and-NAT policy:

```
no nat policy
```

The following command enables IPv4 and IPv6 NAT support in a Firewall-and-NAT policy:

```
nat policy ipv4-and-ipv6
```
nat private-ip-flow-timeout

This command configures the Private IP NPU flow timeout setting.

Product
NAT

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Firewall-and-NAT Policy Configuration

active-charging service service_name > fw-and-nat policy policy_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-fw-and-nat-policy)#

Syntax

nat private-ip-flow-timeout timeout

{ default | no } nat private-ip-flow-timeout

---

**default**

Configures the default setting.
Default: 180 seconds

---

**no**

Disables the Private IP NPU flow timeout configuration.
When disabled, the flow is installed at call setup and will be removed only when the subscriber disconnects.

---

**timeout**

Specifies the Private IP NPU flow timeout period in seconds.
timeout must be an integer from 180 through 86400.

---

Usage

Use this command to configure the Private IP NPU flow timeout setting.
For NAT-enabled calls, by default, the downlink private IP NPU flow will not be installed at call setup for a subscriber session. The flow will only be installed on demand. When there is no traffic on the private flow, the private IP flow will be removed after the configurable timeout period.

Example

The following command configures the Private IP NPU flow timeout setting to 36000 seconds:

    nat private-ip-flow-timeout 36000
nat suppress-aaa-update

This command suppresses sending NAT Bind Update (NBU) to the AAA server when PPP disconnect happens.

**Important:** This command is customer-specific. For more information please contact your local service representative.

**Product**
NAT

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Firewall-and-NAT Policy Configuration

```text
active-charging service service_name > fw-and-nat policy policy_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-fw-and-nat-policy)#
```

**Syntax**

```text
nat suppress-aaa-update call-termination

default nat suppress-aaa-update
```

```text
default
```

Configures the default setting.

Default: No suppression of AAA updates.

**Usage**

Use this command to suppress sending of NBU to the AAA server when PPP disconnect happens, as these NBUs would be cleared at the AAA after receiving the accounting-stop. This enables to minimize the number of messages between the chassis and AAA server. When not configured, NBU are sent to the AAA server whenever a port chunk is allocated, de-allocated, or the call is cleared (PPP disconnect).

**Example**

The following command suppresses the sending of NBU to the AAA server:

```
  nat suppress-aaa-update call-termination
```
Chapter 136
Firewall-and-NAT Access Ruledef Configuration Mode Commands

The Firewall-and-NAT Access Ruledef Configuration Mode is used to configure and manage Access rule definitions used by the Stateful Firewall (FW) and Network Address Translation (NAT) in-line services.

Mode

Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

active-charging service service_name > access-ruledef access_ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-fw-ruledef)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
## bearer 3gpp apn

This command configures an access ruledef to analyze user traffic based on APN bearer.

### Product
- PSF
- NAT

### Privilege
- Security Administrator, Administrator

### Mode
- Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

The command sequence to configure an access ruledef is as follows:

```
active-charging service service_name > access-ruledef access_ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-fw-ruledef)#
```

### Syntax

```
[ no ] bearer 3gpp apn [ case-sensitive ] operator value
```

- **no**
  - Removes previously configured bearer ruledef.

- **case-sensitive**
  - This keyword makes the rule case sensitive.
  - By default, ruledefs are not case sensitive.
  - Default: Disabled

- **operator**
  - Specifies how to logically match the APN name.
  - **operator** must be one of the following:
    - !=: Does not equal
    - !contains: Does not contain
    - !ends-with: Does not end with
    - !starts-with: Does not start with
    - =: Equals
    - contains: Contains
    - ends-with: Ends with
    - starts-with: Starts with

- **value**
  - The APN name to match in bearer flow.
  - **value** must be an alphanumeric string of 1 through 63 characters that can include punctuation characters.
Usage
Use this command to specify an access ruledef to analyze user traffic based on APN name.

Example
The following command creates an access ruledef for analyzing user traffic for an APN named `apn12`:

```
bearer 3gpp apn = apn12
```
bearer 3gpp imsi

This command configures an access ruledef to analyze user traffic based on International Mobile Station Identification (IMSI) number in bearer flow.

Product
PSF

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

active-charging service service_name > access-ruledef access_ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-fw-ruledef)#

Syntax

[ no ] bearer 3gpp imsi { operator msid | { !range | range } imsi_pool imsi_pool }

no
Removes previously configured bearer ruledef.

operator
Specifies how to logically match the MSID.
operator must be one of the following:
- !=: Does not equal
- ==: Equals

msid
Specifies the Mobile Station Identifier.

{ !range | range } imsi_pool imsi_pool
{ !range | range }: Specifies the range criteria:
- !range: Not in the range of
- range: In the range of

imsi_pool imsi_pool: Specifies the IMSI pool name. imsi_pool must be an alphanumeric string of 1 through 63 characters.

Usage
Use this command to specify an access ruledef to analyze user traffic based on IMSI number of mobile station.

Example
The following command creates an access ruledef to analyze user traffic for the IMSI number 9198838330912:

```
bearer 3gpp imsi = 9198838330912
```
### bearer username

This command configures an access ruledef to analyze user traffic based on user name of the bearer flow.

**Product**
- PSF
- NAT

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

```plaintext
active-charging service service_name > access-ruledef access_ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs-fw-ruledef)#
```

**Syntax**

```
[ no ] bearer username [ case-sensitive ] operator value
```

- **no**
  - Removes previously configured bearer ruledef.

- **case-sensitive**
  - This keyword makes the rule case sensitive.
  - By default, ruledefs are not case sensitive.
  - Default: Disabled

- **operator**
  - Specifies how to logically match the MSID.
  - `operator` must be one of the following:
    - `!=`: Does not equal
    - `!contains`: Does not contain
    - `!ends-with`: Does not end with
    - `!starts-with`: Does not start with
    - `=`: Equals
    - `contains`: Contains
    - `ends-with`: Ends with
    - `starts-with`: Starts with

- **value**
  - Specifies the user name.
  - `value` must be an alphanumeric string of 1 through 127 characters.
Usage
Use this command to specify a access ruledef to analyze user traffic based on user name of the bearer flow.

Example
The following command creates an access ruledef for analyzing user traffic for the user name user12:

\[ \text{bearer username} = \text{user12} \]
create-log-record

This command enables/disables access ruledef logging.

Product
- PSF
- NAT

Privilege
- Security Administrator, Administrator

Mode
Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

active-charging service service_name > access-ruledef access_ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-fw-ruledef)#

Syntax

[ no ] create-log-record

  no

  Disables access ruledef logging.

Usage

Use this command to enable/disable access ruledef logging.

Example

The following command enables access ruledef logging:

  create-log-record

The following command disables access ruledef logging:

  no create-log-record
end

Exits the current configuration mode and returns to the Exec mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**

Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
```
exit
```

**Usage**
Use this command to return to the parent configuration mode.
icmp any-match

This command configures an access ruledef to match any ICMPv4 traffic for the user.

Product
PSF
NAT

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

active-charging service service_name > access-ruledef access_ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-fw-ruledef)#

Syntax

[ no ] icmp any-match operator condition

no
Removes previously configured ICMPv4 any-match ruledef.

operator
Specifies how to logically match the analyzed state.
operator must be one of the following:
• !=: Does not equal
• ==: Equals

condition
Specifies the condition to be matched for the user traffic.
condition must be one of the following:
• FALSE: Specified condition is FALSE.
• TRUE: Specified condition is TRUE.

Usage
Use this command to specify an access ruledef to match any ICMPv4 traffic of the user.

Example
The following command creates an access ruledef to match any non-ICMPv4 traffic of the user:

icmp any-match = FALSE
**icmp code**

This command configures an access ruledef to analyze user traffic based on ICMPv4 code.

**Product**

PSF
NAT

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

```plaintext
active-charging service service_name > access-ruledef access_ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-fw-ruledef)#
```

**Syntax**

```
[ no ] icmp code operator code
```

- **no**
  - Removes previously configured ICMPv4 code ruledef.

- **operator**
  - Specifies how to logically match the ICMPv4 code.
    - `!=`: Does not equal
    - `<=`: Less than or equals
    - `=`: Equals
    - `>=`: Greater than or equals

- **code**
  - Specifies the ICMPv4 code.
    - `code` must be an integer from 0 through 255.

**Usage**

Use this command to define an access ruledef to analyze user traffic based on the ICMPv4 code.

**Example**

The following command creates an access ruledef for analyzing user traffic using the ICMPv4 code as 23:

```
icmp code = 23
```
icmp type

This command configures an access ruledef to analyze user traffic based on ICMPv4 type.

Product

PSF
NAT

Privilege

Security Administrator, Administrator

Mode

Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

active-charging service service_name > access-ruledef access_ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-fw-ruledef)#

Syntax

[ no ] icmp type operator type

no
Removes previously configured ICMPv4 type ruledef.

operator
Specifies how to logically match the ICMPv4 type.
operator must be one of the following:
• !=: Does not equal
• <=: Less than or equals
• =: Equals
• >=: Greater than or equals

type
Specifies the ICMPv4 type.
type must be an integer from 0 through 255.
For example, 0 for ECHO Reply, 3 for Dest. Unreachable, and 5 for Redirect.

Usage

Use this command to define an access ruledef to analyze user traffic based on the ICMPv4 type.

Example

The following command creates an access ruledef for analyzing user traffic using an ICMPv4 type as 123:

icmp type = 123
**icmpv6 any-match**

This command configures an access ruledef to match any ICMPv6 traffic for the user.

**Product**
PSF  
NAT

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

active-charging service service_name > access-ruledef access_ruledef_name

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acsfw-ruledef)#
```

**Syntax**

```
[ no ] icmpv6 any-match operator condition
```

- **no**
  Removes previously configured ICMPv6 any-match ruledef.

- **operator**
  Specifies how to logically match the analyzed state.
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `==`: Equals

- **condition**
  Specifies the condition to be matched for the user traffic.
  `condition` must be one of the following:
  - **FALSE**: Specified condition is FALSE.
  - **TRUE**: Specified condition is TRUE.

**Usage**
Use this command to specify an access ruledef to match any ICMPv6 traffic of the user.

**Example**
The following command creates an access ruledef to match any non-ICMPv6 traffic of the user:

```
icmpv6 any-match = FALSE```
**icmpv6 code**

This command configures an access ruledef to analyze user traffic based on ICMPv6 code.

**Product**
PSF
NAT

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

`active-charging service service_name > access-ruledef access_ruledef_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-fw-ruledef)#
```

**Syntax**

```
[ no ] icmpv6 code operator code
```

- **no**
  Removes previously configured ICMPv6 code ruledef.

- **operator**
  Specifies how to logically match the ICMPv6 code.
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `<=`: Less than or equals
  - `==`: Equals
  - `>=`: Greater than or equals

- **code**
  Specifies the ICMPv6 code.
  `code` must be an integer from 0 through 255.

**Usage**
Use this command to define an access ruledef to analyze user traffic based on the ICMPv6 code.

**Example**
The following command creates an access ruledef for analyzing user traffic using the ICMPv6 code as 23:

```
icmpv6 code = 23
```
icmpv6 type

This command configures an access ruledef to analyze user traffic based on ICMPv6 type.

Product
PSF
NAT

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

active-charging service service_name > access-ruledef access_ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-fw-ruledef)#

Syntax

[ no ] icmpv6 type operator type

no
Removes previously configured ICMPv6 type ruledef.

operator
Specifies how to logically match the ICMPv6 type.
operator must be one of the following:
- !=: Does not equal
- <=: Less than or equals
- ==: Equals
- >=: Greater than or equals

type
Specifies the ICMPv6 type.
type must be an integer from 0 through 255.
For example, 0 for ECHO Reply, 3 for Dest. Unreachable, and 5 for Redirect.

Usage
Use this command to define an access ruledef to analyze user traffic based on the ICMPv6 type.

Example
The following command creates an access ruledef for analyzing user traffic using an ICMPv6 type as 123:

icmpv6 type = 123
**ip any-match**

This command configures an access ruledef to match any IP traffic for the user.

**Product**
PSF
NAT

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

```
active-charging service service_name > access-ruledef access_ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-fw-ruledef)#
```

**Syntax**

```
[ no ] ip any-match operator condition
```

- **no**
  - Removes previously configured IP any-match ruledef.

- **operator**
  - Specifies how to logically match the analyzed state.
  - `operator` must be one of the following:
    - `!=`: Does not equal
    - `==`: Equals

- **condition**
  - Specifies the condition to be matched for the user traffic.
  - `condition` must be one of the following:
    - `FALSE`: Specified condition is FALSE.
    - `TRUE`: Specified condition is TRUE.

**Usage**

Use this command to specify an access ruledef to match any IP traffic of the user.

**Example**

The following command creates an access ruledef to match any non-IP traffic of the user:

```
ip any-match = FALSE
```
**ip downlink**

This command configures an access ruledef to analyze user traffic based on IP packet flow in downlink direction (to subscriber).

**Product**
- PSF
- NAT

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

```
active-charging service service_name > access-ruledef access_ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-fw-ruledef) #
```

**Syntax**

```
[ no ] ip downlink operator condition
```

- **no**
  Removes previously configured IP ruledef.

- **operator**
  Specifies how to logically match the packet flow direction.
  **operator** must be one of the following:
  - !=: Does not equal
  - ==: Equals

- **condition**
  Specifies the condition to match.
  **condition** must be one of the following:
  - TRUE: Analyzed
  - FALSE: Not analyzed

**Usage**

Use this command to define an access ruledef to analyze user traffic based on the IP packet flow direction as downlink.

**Example**

The following command creates access ruledef for analyzing user traffic using an IP packet direction to downlink (to subscriber):

```
ip downlink = TRUE
```
**ip dst-address**

This command configures an access ruledef to analyze user traffic based on IP destination address.

**Product**
- PSF
- NAT

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

active-charging service service_name > access-ruledef access_ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-fw-ruledef)#

**Syntax**

```
[ no ] ip dst-address { operator { ipv4/ipv6_address | ipv4/ipv6_address/mask } | { !range | range } host-pool host_pool }
```

- **no**
  Removes previously configured IP destination address ruledef.

- **operator { ipv4/ipv6_address | ipv4/ipv6_address/mask }**
  - **operator** specifies how to logically match the IP destination address.
  - **operator** must be one of the following:
    - !=: Does not equal
    - <=: Less than or equals
    - =: Equals
    - >=: Greater than or equals

- **ipv4/ipv6_address**: Specifies the IP address of destination node for outgoing traffic.
  - **ipv4/ipv6_address** must be the IP address entered using IPv4 dotted-decimal notation or IPv6 colon-separated-hexadecimal notation.

- **ipv4/ipv6_address/mask**: Specifies the IP address of destination node for outgoing traffic.
  - **ipv4/ipv6_address/mask** must be the IP address entered using IPv4 dotted-decimal notation or IPv6 colon-separated-hexadecimal notation. The mask bit is a numeric value which is the number of bits in the subnet mask.

- **{ !range | range } host-pool host_pool**
  - **!range | range**: Specifies the range criteria:
    - !range: Not in the range of
    - range: In the range of

- **host-pool host_pool**: Specifies the host pool name. **host_pool** must be an alphanumeric string of 1 through 63 characters.
**Usage**

Use this command to specify an access ruledef to analyze user traffic based on the IP destination address.

**Example**

The following command creates IP ruledef for analyzing user traffic using an IP destination address of 10.1.1.1:

```
ip dst-address = 10.1.1.1
```
**ip protocol**

This command configures an access ruledef to analyze user traffic based on the protocol being transported by IP packets.

**Product**
PSF
NAT

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

```
active-charging service service_name > access-ruledef access_ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-fw-ruledef)#
```

**Syntax**

```
[ no ] ip protocol { { operator { protocol | protocol_assignment } } | { operator protocol_assignment } }
```

- **no**
  Removes previously configured IP protocol address ruledef.

- **operator { protocol | protocol_assignment }**
  **operator:** Specifies how to logically match the IP protocol.
  **operator** must be one of the following:
  - !=: Does not equal
  - ==: Equals

- **protocol:** Specifies the protocol by name.
  **protocol** must be one of the following:
  - ah
  - esp
  - gre
  - icmp
  - tcp
  - udp

- **protocol_assignment:** Specifies the protocol by assignment number. **protocol_assignment** must be an integer from 0 through 255 (for example, 1 for ICMP, 6 for TCP, and 17 for UDP).

```
operator protocol_assignment
```

**operator:** Specifies how to logically match the IP protocol.

**operator** must be one of the following:
- <=: Less than or equals
- >=: Greater than or equals

**protocol_assignment**: Specifies the protocol by assignment number. **protocol_assignment** must be an integer from 0 through 255 (for example, 1 for ICMP, 6 for TCP, and 17 for UDP).

**Usage**

Use this command to specify an access ruledef to analyze user traffic based on the IP protocol.

**Example**

The following command creates IP ruledef for analyzing user traffic using a protocol assignment of 1:

```plaintext
ip protocol = 1
```
**ip server-ip-address**

This command configures an access ruledef to analyze user traffic based on IP server address.

**Product**
PSF
NAT

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

```sh
cisco> active-charging service service_name > access-ruledef access_ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-fw-ruledef)#
```

**Syntax**

```
[ no ] ip server-ip-address { operator { ipv4/ipv6_address | ipv4/ipv6_address/mask } | { !range | range } host-pool host_pool_name }
```

- **no**
  Removes previously configured IP server address.

- **operator**
  Specifies how to logically match the IP server address.
  * operator must be one of the following:
    - !=: Does not equal
    - <=: Less than or equals
    - ==: Equals
    - >=: Greater than or equals

- **ipv4/ipv6_address**: Specifies the server IP address. For uplink packets (subscriber to network), this field matches the destination IP address in the IP header. For downlink packets (network to subscriber), this field matches the source IP address in the IP header. `ipv4/ipv6_address` must be an IP address in IPv4-dotted decimal notation or IPv6 colon-separated hexadecimal notation.

- **ipv4/ipv6_address/mask**: Specifies the server IP address with subnet mask bit. For uplink packets (subscriber to network), this field matches the destination IP address in the IP header. For downlink packets (network to subscriber), this field matches the source IP address in the IP header. `ipv4/ipv6_address/mask` must be an IP address in IPv4 dotted-decimal notation or IPv6 colon-separated hexadecimal notation with subnet mask bit. The mask bit is a numeric value which is the number of bits in the subnet mask.

- **{ !range | range } host-pool host_pool_name**

  - **{ !range | range }**: Specifies the range criteria.
    - !range: Not in the range of
    - range: In the range of
**Usage**

Use this command to specify an access ruledef to analyze user traffic based on IPv4 or IPv6 server address. For uplink packets, this field matches the destination IP address in the IP header. For downlink packets, this field matches the source IP address in the IP header.

**Example**

The following command creates an IP ruledef for analyzing user traffic using IPv4 server address `10.1.1.1`:

```
ip server-ip-address = 10.1.1.1
```
**ip server-ipv6-network-prefix**

This command configures an access ruledef to analyze user traffic based on IPv6 server prefix.

**Product**
PSF
NAT

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

```
active-charging service service_name > access-ruledef access_ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-fw-ruledef)#
```

**Syntax**

```
[ no ] ip server-ipv6-network-prefix operator ipv6_prefix/prefix_length
```

- **no**
  - Removes previously configured IPv6 server prefix.

- **operator ipv6_prefix/prefix_length**
  - **operator**: Specifies how to logically match the IPv6 server prefix.
    - !=: Does not equal
    - ==: Equals
  - **ipv6_prefix/prefix_length**: Specifies the server’s IPv6 address with subnet mask bit.
    - The **prefix_length** is the number of bits to match. The configurable prefix length values are 32, 40, 48, 56, 64 and 96.

**Usage**

Use this command to specify an access ruledef to analyze user traffic based on IPv6 server prefix. When a first packet for a flow is received, it is matched against a set of rules configured in the Firewall-and-NAT policy. If the incoming IPv6 packet matches a ruledef and configured prefix, then it indicates that NAT64 needs to be applied on the packet. If the packet did not match the prefix configured, then NAT64 will not be applied on the packet. If there is no rule matching the packet or if there is no rule configured, then the incoming IPv6 packet is matched against the well-known prefix. If the well-known prefix matches, then NAT64 is applied on the packet.

**Example**

The following command creates an IP ruledef to analyze user traffic using the IPv6 server prefix `abcd:dcba` with 32 bits of the server IPv6 address:

```
ip server-ipv6-network-prefix = abcd:dcba::/32
```
ip src-address

This command configures an access ruledef to analyze user traffic based on IP source address.

Product
PSF
NAT

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

active-charging service service_name > access-ruledef access_ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-fw-ruledef)#

Syntax

[ no ] ip src-address { operator { ipv4/ipv6_address | ipv4/ipv6_address/mask } | { !range | range } host-pool host_pool }

no
Removes previously configured IP destination address ruledef.

operator { ipv4/ipv6_address | ipv4/ipv6_address/mask }
operator: Specifies how to logically match the IP source address.
operator must be one of the following:
• !=: Does not equal
• <=: Less than or equals
• ==: Equals
• >=: Greater than or equals
ipv4/ipv6_address: Specifies the IP address using IPv4 dotted-decimal notation or IPv6 colon-separated-hexadecimal notation.
ipv4/ipv6_address/mask: Specifies the IP address using IPv4 dotted-decimal notation or IPv6 colon-separated-hexadecimal notation with subnet mask bit. The mask bit is a numeric value which is the number of bits in the subnet mask.

{ !range | range } host-pool host_pool

!range | range: Specifies the range criteria:
• !range: Not in the range of
• range: In the range of
host-pool host_pool: Specifies the host pool name. host_pool must be an alphanumeric string of 1 through 63 characters.
Usage
Use this command to specify an access ruledef to analyze user traffic based on the IP source address.

Example
The following command creates IP ruledef for analyzing user traffic using an IP source address of 10.1.1.1:

```
ip src-address = 10.1.1.1
```
**ip uplink**

This command configures an access ruledef to analyze user traffic based on IP packet flow in the uplink direction (from subscriber).

**Product**  
PSF

**Privilege**  
Security Administrator, Administrator

**Mode**  
Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

```
active-charging service service_name > access-ruledef access_ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-acs-fw-ruledef)#
```

**Syntax**

```
[ no ] ip uplink operator condition
```

- **no**  
  Removes previously configured IP uplink match ruledef.

- **operator**  
  Specifies how to logically match the IP packet flow direction.  
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `==`: Equals

- **condition**  
  Specifies the condition to match.  
  `condition` must be one of the following:
  - `TRUE`: Not analyzed
  - `FALSE`: Analyzed

**Usage**

Use this command to define an access ruledef to analyze user traffic based on the IP packet flow direction as uplink.

**Example**

The following command creates access ruledef for analyzing user traffic using an IP packet direction to uplink (from subscriber):

```
ip uplink = TRUE
```
ip version

This command defines rule expressions to match version number in IP header.

Product
PSF
NAT

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

active-charging service service_name > access-ruledef access_ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-fw-ruledef)#

Syntax

[ no ] ip version = { ipv4 | ipv6 }

- no
  Deletes the specified rule expression.

- ipv4
  Specifies the rule expression for IP version 4.

- ipv6
  Specifies the rule expression for IP version 6.

Usage
Use this command to define rule expressions to match IPv4/IPv6 version number in IP header.

Example

The following command defines a rule expression to match user traffic for the IP version ipv6:

  ip version = ipv6
tcp any-match

This command configures an access ruledef to match any TCP traffic for the user.

Product
PSF
NAT

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

active-charging service service_name > access-ruledef access_ruledef_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acsc-fw-ruledef)#

Syntax

[ no ] tcp any-match operator condition

no
Removes previously configured TCP any-match ruledef.

operator
Specifies how to logically match the analyzed state.
operator must be one of the following:
- !=: Does not equal
- ==: Equals

condition
Specifies the condition to be matched for the user traffic.
condition must be one of the following:
- FALSE: Specified condition is FALSE.
- TRUE: Specified condition is TRUE.

Usage
Use this command to specify an access ruledef to match any TCP traffic of the user.

Example
The following command creates an access ruledef to match any non-TCP traffic of the user:

tcp any-match = FALSE
**tcp dst-port**

This command configures an access ruledef to analyze user traffic based on destination TCP port.

**Product**
PSF
NAT

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

active-charging service service_name > access-ruledef access_ruledef_name

Entering the above command sequence results in the following prompt:

[local] host_name(config-acs-fw-ruledef) #

**Syntax**

```plaintext
[ no ] tcp dst-port { operator port_number | { !range | range } { start_range to end_range | port-map port_map } }
```

- **no**
  Removes the previously configured destination TCP port ruledef.

- **operator**
  Specifies how to logically match the port number.
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `<=`: Less than or equals
  - `=`: Equals
  - `>=`: Greater than or equals

- **port_number**
  Specifies the port number to match.
  `port_number` must be an integer from 1 through 65535.

- **range | !range**
  Specifies the range criteria:
  - `!range`: Not in the range
  - `range`: In the range

- **start_range to end_range**
  Specifies the starting and ending port numbers for the range of destination TCP ports.
  `start_range` must be an integer from 1 through 65535.
  `end_range` must be an integer from 1 through 65535 that is greater than `start_range`. 
**port-map port_map**

Specifies name of the port-map for the port range.

*port_map* must be an alphanumeric string of 1 through 63 characters.

**Usage**

Use this command to specify an access ruledef to analyze user traffic based on destination TCP port.

**Example**

The following command creates an access ruledef for analyzing user traffic matching destination port for TCP as 10:

```
tcp dst-port = 10
```
**tcp either-port**

This command configures an access ruledef to analyze user traffic based on either (destination or source) TCP ports.

**Product**
PSF
NAT

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration
active-charging service service_name > access-ruledef access_ruledef_name

Entering the above command sequence results in the following prompt:

[local] host_name(config-acs-fw-ruledef) #

**Syntax**

```
[ no ] tcp either-port { operator port_number | { !range | range } { start_range to end_range | port-map port_map } }
```

- **no**
  Removes previously configured TCP either-port (destination or source) ruledef.

- **operator**
  Specifies how to logically match the port number.
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `<=`: Less than or equals
  - `=`: Equals
  - `>=`: Greater than or equals

- **port_number**
  Specifies the port number to match.
  `port_number` must be an integer from 1 through 65535.

- **range | !range**
  Specifies the range criteria:
  - `!range`: Not in the range
  - `range`: In the range

- **start_range to end_range**
  Specifies the starting and ending port numbers for the port range.
  `start_range` must be an integer from 1 through 65535.
  `end_range` must be an integer from 1 through 65535 that is greater than `start_range`. 
**tcp either-port**

```sql
port-map port_map
```

Specifies name of the port-map for the port range.

`port_map` must be an alphanumeric string of 1 through 63 characters.

**Usage**

Use this command to specify an access ruledef to analyze user traffic based on either TCP port.

**Example**

The following command creates an access ruledef for analyzing user traffic matching destination or source port for TCP as 10:

```text
tcp either-port = 10
```
**tcp src-port**

This command configures an access ruledef to analyze user traffic based on source TCP port.

**Product**
PSF
NAT

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

`active-charging service service_name > access-ruledef access_ruledef_name`

Entering the above command sequence results in the following prompt:

```bash
[local]host_name(config-acs-fw-ruledef)#
```

**Syntax**

```bash
[ no ] tcp src-port { operator port_number | { !range | range } { start_range to end_range | port-map port_map } }
```

- **no**
  Removes previously configured source TCP port ruledef.

- **operator**
  Specifies how to logically match the port number.
  `operator` must be one of the following:
  - !==: Does not equal
  - <=: Less than or equals
  - ==: Equals
  - >=: Greater than or equals

- **port_number**
  Specifies the port number to match.
  `port_number` must be an integer from 1 to 65535.

- **range | !range**
  Specifies the range criteria:
  - !=range: Not in the range
  - range: In the range

- **start_range to end_range**
  Specifies the starting and ending port numbers for the port range.
  `start_range` must be an integer from 1 to 65535.
  `end_range` must be an integer from 1 to 65535 that is greater than `start_range`.
**port-map** *port_map*

Specifies name of the port-map for the port range.

*port_map* must be an alphanumeric string of 1 through 63 characters.

---

**Usage**

Use this command to specify an access ruledef to analyze user traffic based on source TCP port.

**Example**

The following command creates an access ruledef for analyzing user traffic matching source port for TCP as 10:

```
tcp src-port = 10
```
**udp any-match**

This command configures an access ruledef to match any UDP traffic for the user.

**Product**

PSF
NAT

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

```plaintext
active-charging service service_name > access-ruledef access_ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-fw-ruledef)#
```

**Syntax**

```
[ no ] udp any-match operator condition
```

- **no**
  
  Removes previously configured UDP any-match ruledef.

- **operator**
  
  Specifies how to logically match the analyzed state.
  
  * operator must be one of the following:
    - `!=`: does not equal
    - `=`: equals

- **condition**
  
  Specifies the condition to be matched for the user traffic.
  
  * condition must be one of the following:
    - `FALSE`: Specified condition is FALSE.
    - `TRUE`: Specified condition is TRUE.

**Usage**

Use this command to specify an access ruledef to match any UDP traffic of the user.

**Example**

The following command creates an access ruledef to match any UDP traffic of the user:

```
udp any-match = TRUE
```
**udp dst-port**

This command configures an access ruledef to analyze user traffic based on destination UDP port.

**Product**
- PSF
- NAT

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

```
active-charging service service_name > access-ruledef access_ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-fw-ruledef)#
```

**Syntax**

```
[ no ] udp dst-port { operator port_number | !range | range } { start_range to end_range | port-map port_map }
```

**no**
Removes previously configured destination UDP ports ruledef.

**operator**
Specifies how to logically match the port number.

`operator` must be one of the following:

- `!=`: Does not equal
- `<=`: Less than or equals
- `==`: Equals
- `>=`: Greater than or equals

**port_number**
 Specifies the port number to match.
`port_number` must be an integer from 1 through 65535.

**!range | range**
Specifies the range criteria.

- `!range`: Not in the range
- `range`: In the range

**start_range to end_range**
Specifies the starting and ending port numbers for the port range.
`start_range` must be an integer from 1 through 65535.
`end_range` must be an integer from 1 through 65535 that is greater than `start_range`. 
Firewall-and-NAT Access Ruledef Configuration Mode Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>port-map</strong> <code>port_map</code></td>
<td>Specifies name of the port-map for the port range. <code>port_map</code> must be an alphanumeric string of 1 through 63 characters.</td>
</tr>
</tbody>
</table>

**Usage**

Use this command to specify an access ruledef to analyze user traffic based on destination UDP port.

**Example**

The following command creates an access ruledef for analyzing user traffic matching destination port for UDP as 10:

```
udp dst-port = 10
```
udp either-port

This command configures an access ruledef to analyze user traffic based on either (destination or source) UDP port.

**Product**
PSF
NAT

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

```
active-charging service service_name > access-ruledef access_ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-fw-ruledef)#
```

**Syntax**

```
[ no ] udp either-port { operator port_number | { !range | range } { start_range to end_range | port-map port_map } }
```

- **no**
  Removes previously configured either-port (destination or source) UDP ruledef.

- **operator**
  Specifies how to logically match the port number.
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `<=`: Less than or equals
  - `==`: Equals
  - `>=`: Greater than or equals

- **port_number**
  Specifies the port number to match.
  `port_number` must be an integer from 1 through 65535.

- **!range | range**
  Specifies the range criteria.
  - `!range`: Not in the range
  - `range`: In the range

- **start_range to end_range**
  Specifies the starting and ending port numbers for the port range.
  `start_range` must be an integer from 1 through 65535.
  `end_range` must be an integer from 1 through 65535 that is greater than `start_range`.

-Cisco ASR 5x00 Command Line Interface Reference

4906
**port-map** *port_map*

Specifies name of the port-map for the port range.  
*port_map* must be an alphanumeric string of 1 through 63 characters.

**Usage**

Use this command to specify an access ruledef to analyze user traffic based on either UDP port.

**Example**

The following command creates an access ruledef for analyzing user traffic matching destination or source port for UDP as 10:

```
udp either-port = 10
```
**udp src-port**

This command configures an access ruledef to analyze user traffic based on source UDP port.

**Product**

PSF

NAT

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > ACS Configuration > Firewall-and-NAT Access Ruledef Configuration

`active-charging service service_name > access-ruledef access_ruledef_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-fw-ruledef)#
```

**Syntax**

```
[ no ] udp src-port { operator port_number | { !range | range } { start_range to end_range | port-map port_map } }
```

**no**

Removes previously configured source UDP port ruledef.

**operator**

Specifies how to logically match the port number.

`operator` must be one of the following:

- `!=`: Does not equal
- `<=`: Less than or equals
- `=`: Equals
- `>=`: Greater than or equals

**port_number**

Specifies the port number to match.

`port_number` must be an integer from 1 through 65535.

**!range | range**

Specifies the range criteria.

- `!range`: Not in the range
- `range`: In the range

**start_range to end_range**

Specifies the starting and ending port numbers for the port range.

`start_range` must be an integer from 1 through 65535.

`end_range` must be an integer from 1 through 65535 that is greater than `start_range`. 
**port-map** *port_map*

Specifies name of the port-map for the port range.

*port_map* must be an alphanumeric string of 1 through 63 characters.

---

**Usage**

Use this command to specify an access ruledef to analyze user traffic based on source UDP port.

**Example**

The following command creates an access ruledef for analyzing user traffic matching source port for UDP as 10:

```
udp src-port = 10
```
Chapter 137
FNG Service Configuration Mode Commands

The FNG Service Configuration Mode is used to configure the properties required for the Femto Network Gateway (FNG) to interface with the Femto Access Points (FAPs) in the network.

Mode

Exec > Global Configuration > Context Configuration > FNG Service Configuration

\texttt{configure > context context\_name > fng-service service\_name}

Entering the above command sequence results in the following prompt:

\texttt{[context\_name]\_host\_name(config-fng-service)#}

\\begin{itemize}
\item[] \textbf{Important:} The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
\end{itemize}
aaa aggregation

Sets the system attributes for A12 aggregation for the FNG service.

Product
FNG

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > FNG Service Configuration

configure > context context_name > fng-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-fng-service)#

Syntax

aaa aggregation { interface type a12| destination address ipv4_address | a12-group { context name [ aaa-group name ] | aaa-group name [ context name ] } }

no aaa aggregation interface type a12

no a12 destination address ipv4_address

no aaa aggregation a12-group { context name [ aaa-group name ] | aaa-group name [ context name ] }

aaa aggregation interface type a12

Enables A12 aggregation functionality for the FNG service.

aaa aggregation interface a12 destination address ipv4_address

Adds a destination address for an AN-AAA server for A12 aggregation. A maximum of ten destination addresses can be configured.

aaa aggregation a12-group { context name [ aaa-group name ] | aaa-group name [ context name ] }

Defines the AAA context and AAA group to be used for A12 aggregation.
If the context name and AAA group are not specified, the FNG defaults to the FNG service context and the default AAA group in that context. If the AAA group is specified but the context is not specified, the FNG uses the FNG service context and the AAA group in that context. If the AAA group is not specified and the context is specified, the FNG uses the default AAA group in that context.

no aaa aggregation interface type a12

Disables A12 aggregation functionality for the FNG service.

no aaa aggregation a12-destination address ipv4_address

Deletes the specified destination address for an AN-AAA server.
no aaa aggregation a12-group { context name [ aaa-group name ] | aaa-group [ context name ] }

Deletes the specified AAA context and AAA group to be used for A12 aggregation.

**Usage**

Sets the system attributes for AAA aggregation in the FNG service.

**Example**

The following command enables the A12 functionality for the FNG service:

```
aggregation interface type a12
```
aaa authentication

Specifies the AAA group to use for FAP authentication.

**Product**
FNG

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > FNG Service Configuration

```
configure > context context_name > fng-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-fng-service)#
```

**Syntax**

```
aaa authentication { context-name name aaa-group name | context-name name aaa-group name }
```

```
no aaa authentication
```

**Usage**

Use this command to specify that during IPSec session establishment using IKEv2 setup, the FNG will use Radius AAA for FAP authentication.

**Example**

Use the following to configure device authentication for an AAA group named `aaa-10` in the FNG context named `fng1`:

```
aaa authentication context-name fng1 aaa-group aaa-10
```
bind

Binds the FNG service IP address to a crypto template and specifies the maximum number of sessions the FNG service supports.

Product
FNG

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > FNG Service Configuration
configure > context context_name > fng-service service_name

Entering the above command sequence results in the following prompt:
[context_name]host_name(config-fng-service)#

Syntax

bind address ipv4_address { crypto-template string }[ max-sessions number ]

no bind

no bind
Removes a previously configured binding.

address ipv4_address
Specifies the IPv4 address of the FNG service.

crypto-template string
Specifies the name of the crypto template to be bound to the FNG service. 
string is any value from 0 - 127 alpha and/or numeric characters.

max-sessions number
Specifies the maximum number of sessions to be supported by the FNG service as an integer from 0 through 1000000. Default: 1000000
If the max-sessions value is changed on an existing system, the new value takes effect immediately if it is higher than the current value. If the new value is lower than the current value, existing sessions remain established, but no new sessions are permitted until usage falls below the newly-configured value.

Usage

Binds the IP address used as the connection point for establishing the IKEv2 sessions to a crypto template. It can also define the maximum number of sessions the FNG can support.

Example

The following command binds an FNG service with an IP address of 10.2.3.4 to the crypto template named T1 and sets the maximum number of sessions to 500000:

bind address 10.2.3.4 crypto-template T1 max-sessions 500000
default

Sets or restores the default condition for the selected parameter.

Product
FNG

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > FNG Service Configuration

configure > context context_name > fng-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-fng-service)#

Syntax

default { { aaa attribute 3gpp2-service-option } | duplicate-session-detection | ip source-violation { drop-limit | period } | setup-timeout | subscriber name }

aaa attribute 3gpp2-service-option
Sets or restores the default value of 4095.

duplicate-session-detection
Sets or restores the default option for duplicate session detection to be fapid-based.

ip source-violation { drop-limit | period }
Sets or restores the IP source violation detection defaults, as follows:
drop-limit: Sets or restores the maximum number of IP source violations within the detection period before dropping the call to the default value of 10.
period: Sets or restores the detection period for IP source violations to the default value of 120 seconds.

setup-timeout
Sets or restores the maximum time allowed for session setup to the default value of 60 seconds.

subscriber name
Sets or restores the name of the default subscriber.
name is a string of 1-127 characters.

username mac-address-stripping
The default behavior is to disable stripping the MAC address from the username.

Usage
Configures the default settings for a given parameter.

Example
Use the following command to set the maximum time allowed for session setup to the default value of 60 seconds:

```
default setup-timeout
```
duplicate-session-detection

Configures the FNG to detect duplicate call sessions based on Femtocell Access Point (FAP) ID and to clear old call information.

This feature is disabled by default.

Product
FNG

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > FNG Service Configuration
configure > context context_name > fng-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-fng-service)#

Syntax

duplicate-session-detection { fapid-based }

no duplicate-session-detection

default duplicate-session-detection

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fapid-based</td>
<td>Sets the FNG to detect duplicate call sessions based on the FAP ID.</td>
</tr>
<tr>
<td>no duplicate-session-detection</td>
<td>Disables duplicate session detection.</td>
</tr>
<tr>
<td>default duplicate-session-detection</td>
<td>Sets or restores the default option for duplicate session detection to be fapid-based.</td>
</tr>
</tbody>
</table>

Usage

By default, duplicate session detection is disabled. Use this command to enable this feature. It applies only to calls established after the feature has been enabled.

The following command enables duplicate session detection based on FAP ID:

duplicate-session-detection fapid-based
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Use this command to return to the parent configuration mode.
ip source-violation

Sets the parameters for IP source validation. Source validation is useful if packet spoofing is suspected or for verifying packet routing and labeling within the network.

Source validation requires the source address of received packets to match the IP address assigned to the subscriber (either statically or dynamically) during the session.

Product
FNG

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > FNG Service Configuration

configure > context context_name > fng-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-fng-service)#

Syntax

ip source-violation { clear-on-valid-packet | drop-limit num | period secs }

no ip source-violation clear-on-valid-packet

clear-on-valid-packet

Configures the service to reset the drop-limit counters upon receipt of a properly addressed packet. Default: disabled

drop-limit num

Sets the maximum number of allowed IP source violations within the detection period before dropping a call as an integer from 1 through 1000000. Default: 10

period secs

Sets the detection period (in seconds) for IP source violations as an integer from 1 through 1000000. Default: 120

Usage

This function allows the operator to configure the network to prevent problems such as when a user gets handed back and forth between two gateways a number of times during a handoff scenario.

When a subscriber packet is received with a source IP address violation, the system increments the IP source violation drop-limit counter and starts the timer for the IP source violation period. Every subsequent packet received with a bad source address during the IP source violation period causes the drop-limit counter to increment.

For example, if the drop-limit is set to 10, after 10 source violations, the call is dropped. The detection period timer continues to count throughout this process.

Example
The following command sets the drop limit to 15 and leaves the other values at their default values:

```
ip source-violation drop-limit 15
```
setup-timeout

Specifies the maximum time allowed to set up a session in seconds.

Product
FNG

Privilege
Security-Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > FNG Service Configuration

configure > context context_name > fng-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-fng-service)#

Syntax

setup-timeout integer

default setup-timeout

setup-timeout integer

Sets the session setup timer (in seconds) as an integer from 2 through 300. Default: 60

default

Sets or restores the default session setup timer value to 60 seconds.

Usage

The FNG clears both the user session and tunnels if a call does not initiate successfully before the session setup timer expires.

Example

The following command sets the session setup timeout value to the default value of 60 seconds:

default setup-timeout
The FTP Configuration Mode is used to manage the FTP server options for the current context.

Mode

Exec > Global Configuration > Context Configuration > FTP Configuration

configure > context context_name > server ftpd

Entering the above command sequence results in the following prompt:

[local] host_name(config-ftp)#

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
## exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Use this command to return to the parent configuration mode.
max servers

Configures the maximum number of FTP servers that can be started within any 60 second interval. If this limit is reached, the system waits two minutes before trying to start any more servers.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > FTP Configuration

configure > context context_name > server ftpd

Entering the above command sequence results in the following prompt:

[local]host_name(config-ftp)#

Syntax

max servers count

```plaintext
count

Default: 40
Specifies the maximum number of servers that can be spawned in any 60-second interval. count must be an integer from 1 through 100.
```

Usage

Set the number of servers to tune the system response as a heavily loaded system may need more servers to support the incoming requests.
The converse would be true as well in that a system can benefit by reducing the number of servers such that FTP services do not cause excessive system impact to other services.

Example

```
max servers 50
```
timeout

Configures the client idle timeout before an FTP session is automatically closed.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > FTP Configuration

**Syntax**
```
timeout seconds
```

- `seconds`
  - Default: 900
  - Specifies the number of seconds of inactivity before an FTP session is automatically closed. `seconds` must be an integer from 10 through 86400.

**Usage**
Adjust the session timeout to fine tune the system. FTP session resources can be released sooner to support additional requests by adjusting the timeout to a smaller value.

**Example**
```
timeout 300
```
Chapter 139
GGSN Service Configuration Mode Commands

The Gateway GPRS Support Node (GGSN) Configuration Mode is used to create and manage GGSN services within
the current context.

Mode

Exec > Global Configuration > Context Configuration > GGSN Service Configuration

configure > context context_name > ggsn-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ggsn-service) #

**Important**: The commands or keywords/variables that are available are dependent on platform type, product
version, and installed license(s).
accounting

Configures the name of the context configured on the system that processes accounting for PDP contexts handled by this GGSN service.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > GGSN Service Configuration

command configure > context context_name > ggsn-service service_name

Entering the above command sequence results in the following prompt:

\[context_name\] host_name(config-ggsn-service)#

**Syntax**

```
accounting context context_name

no accounting context
```

**Usage**

By default, the system attempts to use the same context as the one in which the GGSN service is configured for accounting purposes. This command can be used to either change the system’s default behavior, or allow GPRS Tunneling Protocol Prime (GTPP) accounting to a charging gateway (CG).

By default when GTPP accounting is used, accounting records will be sent to the accounting servers configured in whichever context the GGSN service is configured. This command may be used to override that default.

**Example**

The following command configures the GGSN service’s accounting context to be plmn1:

```
accounting context plmn1
```
associate gtpu-service

This command associates a previously configured GTP-U service to bind the GGSN service with a peer. A GTP-U service must be configured in Context Configuration mode before using this configuration.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > GGSN Service Configuration

```
configure > context context_name > ggsn-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ggsn-service)#
```

**Syntax**

```
associate gtpu-service svc_name

noassociate gtpu-service
```

---

**no**

Removes the associated GTP-U service from this GGSN service configuration.

**svc_name**

Identifies the name of the GTP-U service preconfigured in Context Configuration mode to associate with a GGSN service. `svc_name` is an alphanumeric string from 1 through 63 characters.

**Usage**

Use this command to configure GTP-U data plan between GGSN service and peer node. The service defined for GTP-U can be configured in Context configuration mode.

**Example**

Following command associates GTP-U service named `gtpu-hnb1` with specific GGSN service.

```
associate gtpu-service gtpu-hnb1
```
associate peer-map

This command associates a previously configured GGSN peer-map in LTE Policy Configuration mode with GGSN service. A peer-map must be configured before using this configuration.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > GGSN Service Configuration

```bash
configure > context context_name > ggsn-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ggsn-service)#
```

**Syntax**

```bash
associate peer-map peer_map_name

no associate peer-map
```

### no

Removes the associated Peer-Map from this GGSN service configuration.

### peer_map_name

Identifies the name of the Peer Map preconfigured in LTE-Policy Configuration mode to associate with a GGSN service. `peer_map_name` is an alphanumeric string from 1 through 63 characters.

**Usage**

Use this command to associate Peer Map with GGSN service. The peer-profile associated with peer map can be configured in GGSN Peer-Profile configuration mode.

**Important:** When there is no association of peer-map in any of the service, then “default” peer profile of the corresponding service-interface type shall be applied except for GTP-C parameters. Also GTP-C parameters configuration shall be applied from GG service level configuration for GGSN. A maximum of 1024 peer map rules can be configured on one system.

**Example**

Following command associates Peer Map named `ggsn_peer_map1` with specific GGSN service.

```bash
associate ggsn_peer_map1
```
associate pgw-service

This command enables a previously configured P-GW service to which handover will be done by the GGSN service. The P-GW service must be configured in Context Configuration mode before using this configuration.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > GGSN Service Configuration

```bash
configure > context context_name > ggsn-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ggsn-service)#
```

**Syntax**

```bash
associate pgw-service svc_name

no associate pgw-service
```

- **no**
  - Removes the associated P-GW service from this GGSN service configuration.

- **svc_name**
  - Identifies the name of the P-GW service preconfigured in Context Configuration mode to which handover will be done.
  - The `svc_name` must be an alphanumeric string from 1 through 63 characters.

**Usage**

Use this command to allow enabling/disabling bearer handover from GGSN to a P-GW service. The service defined for P-GW can be configured in Context configuration mode. The P-GW’s eGTP service should have the same bind address as GGSN service and P-GW and GGSN should share same GTP-U, otherwise handover will fail.

**Example**

Following command enables P-GW service named `pgw-test` handover with specific GGSN service.

```bash
associate pgw-service pgw-test
```
authorize-with-hss

This command enables or disables subscriber session authorization via a Home Subscriber Server (HSS) over an S6b Diameter interface. This feature is required to support the interworking of GGSN with P-GW and HA.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > GGSN Service Configuration

`configure > context context_name > ggsn-service service_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ggsn-service)#
```

**Syntax**

```
authorize-with-hss [ report-ipv6-addr ]
[ default | no ] authorize-with-hss
```

- `<no>`
  Disables the default authorization of subscriber over S6b interface. Resets the command to the default setting of “authorize locally” from an internal APN authorization configuration.

- `<report-ipv6-addr>`
  Enables the IPv6 address reporting through Authorization-Authentication-Request (AAR) towards the S6b interface.

**Usage**

Use this command to enable/disable the authorization support for subscriber over S6b interface, which is used between GGSN and the 3GPP AAA to exchange the information related to charging, P-CSCF discovery, etc. By use of this feature allows the GGSN service to interact with HSS over S6b interface through Diameter configuration which is already configured on the system.

**Important:** Diameter configuration must be available before enabling this command. For more information of Diameter interface configuration, refer Diameter Endpoint Configuration Mode Commands chapter.

**Important:** This command is a license-enabled feature.

**Example**

The following command enables the subscriber authorization via an HSS over an S6b Diameter interface to provide session interoperability between GGSN and PGW and HA in this GGSN service:

```
authorize-with-hss
```
bind

Binds the GGSN service to a logical IP interface serving as the Gn interface. Specifies the maximum number of subscribers that can access this service over the interface.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > GGSN Service Configuration

configure > context context_name > ggsn-service service_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ggsn-service)#
```

**Syntax**

```
bind address ip_address
no bind address ip_address
```

---

**bind**

Binds the GGSN service to a logical IP interface serving as the Gn interface. Specifies the maximum number of subscribers that can access this service over the interface.

```
bind address 192.168.3.1
```

---

**Usage**

Used to associate or tie the GGSN service to a specific logical IP address. The logical IP address or interface takes on the characteristics of a Gn interface. Only one interface can be bound to a service. The interface should be configured prior to issuing this command.

**Example**

The following command would bind the logical IP interface with the address of 192.168.3.1 to the GGSN service:

```
bind address 192.168.3.1
```

The following command disables a binding that was previously configured:

```
no bind address
```
cc behavior

Configures the 3GPP behavior bits associated with the GGSN’s charging characteristics (CC).

Product
GGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > GGSN Service Configuration

configure > context context_name > ggsn-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ggsn-service)#

Syntax

cc behavior | no-records nr_value

{ default | no } cc behavior

no-records nr_value

Default: 0 (disabled)

Specifies the behavior bit upon which the GGSN ceases sending accounting records to a server.

nr_value can be configured to an integer from 1 through 12 corresponding to the 12 behavior bits – B1 through B12.

Usage

3GPP standards after 3GPP R98 included 12 behavior bits as part of GGSN charging characteristics. Like the charging characteristics profile index, the behavior bits are sent by the SGSN to the GGSN in the Create PDP Context request message.

This command configures the behavior bits for each of the conditions described.

Example

The following command configures a behavior bit of 10 for no-records:

    cc behavior no-records 10
cc profile

Configures the charging characteristic (CC) profile index properties.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > GGSN Service Configuration

```bash
configure > context context_name > ggsn-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ggsn-service)#
```

**Syntax**

```bash
cc profile index [ buckets number | interval time [ downlink down_octets uplink up_octets | total total_octets ] | prepaid { prohibited | use-rulebase-configuration } ] | sgsns num_changes | tariff time1 mins hours [ time2 mins hours [ time3 mins hours [ time4 mins hours [ time5 mins hours [ time6 mins hours ] ] ] ] ] ] | volume { downlink vol_down_octets uplink vol_up_octets | total total_octets } ]
```

```bash
no cc profile index { buckets | interval | prepaid | sgsns | tariff | volume }
```

```bash
default cc profile index
```

```bash
no
```

Removes a previously configured profile index.

```bash
default
```

Returns the specified cc profile to the original default system settings.

```bash
index
```

Configures a profile index for the parameter to be specified. `index` can be configured to an integer from 0 through 15.

**Important:** 3GPP standards suggest that profile index values of 1, 2, 4, and 8 be used for hot billing, flat rate billing, prepaid billing and normal billing, respectively. A single charging characteristics profile can contain multiple behavior settings.

```bash
buckets number
```

Default: 4

Specifies the number of statistics container changes due to QoS changes or tariff time that can occur before an accounting record should be closed.

`number` can be configured to an integer from 1 through 4.
interval time [downlink down_octets uplink up_octets | total total_octets ]

Specifies the normal time duration that must elapse before closing an accounting record provided that any or all of the following conditions occur:

- Downlink traffic volume is reached within the time interval
- Uplink traffic volume is reached within the time interval
- Total traffic volume (up and downlink) is reached within the time interval

time is measured in seconds and can be configured to an integer from 60 through 40000000.
down_octets is the downlink traffic volume measured in octets and can be configured to an integer from 0 through 1000000.
up_octets is the uplink traffic volume measured in octets and can be configured to an integer from 0 through 1000000.
total_octets is the total traffic volume measured in octets and can be configured to an integer from 0 through 1000000.

prepaid { prohibited | use-rulebase-configuration }

This command enables or disables prepaid for the specified profile index.
Default: N/A
prohibited: Disable prepaid for the specified profile index.
use-rulebase-configuration: Use the prepaid configuration in the rulebase.

sgsns num_changes

Default: 4
Specifies the number of SGSN changes (such as, inter-SGSN switchovers) resulting in a new RAI (Routing Area Identity) that can occur before closing an accounting record.
num_changes can be configured to an integer from 1 through 15.

tariff time1 mins hours time2 mins hours time3 mins hours time4 mins hours time5
mins hours time6 mins hours

Specifies time-of-day time values to close the current statistics container (but not necessarily the accounting record). Six different tariff times may be specified. If less than six times are required, the same time can be specified multiple times.

Important: The system assumes that the billing system uses the day/date to determine if the statistics container represents an actual tariff period.

For each of the different tariff times, the following parameters must be configured:

- mins: The minutes of the hour, an integer value from 0 to 59.
- hours: The hour of the day, an integer value from 0 to 23.

volume {downlink vol_down_octets uplink vol_up_octets | total total_octets } 

Specifies the downlink, uplink, and total volumes that must be met before closing an accounting record.
vol_down_octets is measured in octets and can be configured to an integer from 100000 to 4000000000.
vol_up_octets is measured in octets and can be configured to an integer from 100000 to 4000000000.
total_octets is the total traffic volume (up and downlink) measured in octets and can be configured to an integer from 100000 to 4000000000.
Usage
Charging characteristics consist of a profile index and behavior settings. This command configures profile indexes for the GGSN’s charging characteristics. The GGSN supports up to 16 profile indexes. This command works in conjunction with the `cc-sgsn` command located in the APN Configuration Mode that dictates which CCs should be used for subscriber PDP contexts.

Example
The following command configures a profile index of 10 for tariff times of 7:00 AM and 7:30 PM:

```
cc profile 10 tariff time1 0 7 time2 30 19 time3 0 7 time4 30 19
```
default

Sets/restores the default value assigned for the specified parameter.

Product
GGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > GGSN Service Configuration

configure > context context_name > ggsn-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ggsn-service)#

Syntax

[ default ] { cc { behavior | profile index } | echo-interval | gtpu echo-interval | gtpu reorder { context | sequence-numbers | timeout } | guard-interval | ip { local-port gtpc-v1 | qos-dscp } | max-retransmissions | plmn { unlisted-sgsn } | setup-timeout | timeout

cc { behavior | profile index }

Restores the GGSN’s charging characteristics parameters to the following default settings:

• behavior: Restores all behavior parameters to their default values of 0 (disabled).
• profile: For the specified index, the following defaults are applied:
  • buckets: 4
  • interval: Disabled
  • volume: Disabled
  • sgsns: 4
  • tariff-time: Disabled

echo-interval

Restores the GTP echo-interval parameter to its default setting of 60.

gtpu echo-interval

Restores the GTPU echo-interval parameter to its default setting of 60.

gtpu reorder { context | sequence-numbers | timeout }

Restores the gtpu reordering parameters to the following default settings:

• gtpu reorder context: Disabled
• gtpu reorder sequence-numbers: Disabled
• gtpu reorder timeout: 100 milliseconds
gtpu udp-checksum insert
Restores the GGSN gtpu udp-checksum parameter to its default setting of enabled.

guard-interval
Restores the GGSN guard-interval parameter to its default setting of 100.

ip {local-port gtpc-v1 | qos-dscp }
Restores the GGSN ip parameters to the following default setting:
- local-port gtpc-v1: 2123
- qos-dscp: conversational ef streaming af11 interactive af21 background be

max-retransmissions
Restores the GGSN max-retransmissions parameter to its default setting of 4.

plmn { unlisted-sgsn }
Restores the GGSN plmn unlisted-ggsn parameter to its default setting of reject.

setup-timeout
Restores the GGSN setup-timeout parameter to its default setting of 60.

timeout
Restores the GGSN timeout parameter to its default setting of 5.

Usage
After the system has been modified from its default values, this command is used to set/restore specific parameters to their default values.

Example
The following command restores the GGSN service’s guard interval parameter to its default setting:

    default guard-interval
dns-client

This command defines the context name where a DNS client is configured. It associates an existing DNS client configuration with the GGSN to perform a DNS query for P-CSCF, if a P-CSCF query request in an AAA message is received from the Diameter node.

Product
GGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > GGSN Service Configuration

configure > context context_name > ggsn-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ggsn-service)#

Syntax

<table>
<thead>
<tr>
<th>dns-client context dns_ctxt_name</th>
</tr>
</thead>
<tbody>
<tr>
<td>{ no</td>
</tr>
</tbody>
</table>

- **no**
  - Removes the association of DNS context which was configured to perform DSN query in this GGSN service.

- **default**
  - Sets the default context for the DNS client.

  - **dns_ctxt_name**
    - Specifies the name of the context in which a DNS client configuration is present. Typically this should be the same context in which this GGSN service is configured.
    - **dns_ctxt_name** is a context name and must be alphanumeric string of 1 through 79 characters.

Usage

Use this command to associate a DNS client configuration to perform DNS query used for the resolution of P-CSCF query received in AAA message from Diameter peer, on the basis of DNS client parameters configured in a context.

A DNS client configuration must be present in the same context as GGSN service before enabling this command to perform DNS query for P-CSCF.

**Important:** This command is a license-enabled feature.

Example

The following command associates a DNS client configuration to perform DNS query for P-CSCF with this GGSN service which is configured in same context as GGSN service:
default dns-client context
**echo-interval**

Configures the rate at which GPRS Tunneling Protocol (GTP) v1-C Echo packets are sent from the GGSN service to the SGSN.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > GGSN Service Configuration  
configure > context context_name > ggsn-service service_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ggsn-service)#
```

**Syntax**

```
echo-interval seconds [ dynamic [ smooth-factor multiplier ] ]
{ default | no } echo-interval
```

- **default**
  Configures the default value (60 seconds) for echo interval.

- **no**
  Disables the sending of GTPv1-C Echo packets.

- **seconds**
  Default: 60
  Specifies the frequency at which the GGSN service sends GTPv1-C Echo packets to the SGSN(s) it is configured to communicate with.
  *seconds* is measured in seconds and can be configured to an integer from 60 through 3600.

- **dynamic [ smooth-factor multiplier ]**
  Enables the dynamic echo timer for the GTP-U service.
  **smooth-factor multiplier**: Introduces a multiplier into the dynamic echo timer as an integer from 1 through 5. Default: 2

**Usage**

Use this command to adjust the rate at which the GGSN sends these packets. GTPv1-C Echo packets are used to detect whether SGSNs that the GGSN service is communicating with, has become unresponsive or has rebooted.

The system initiates this protocol for each of the following scenarios:

- Upon system boot
• Upon the configuration of a new SGSN on the system using the `sgsn address` command as described in this chapter
• Upon the execution of the path failure detection policy as described in `path-failure` command of this chapter

The echo-interval command is used in conjunction with the `max-retransmissions` and `retransmission-timeout` commands as described in this chapter. In addition to receiving an echo response for this echo protocol, if GGSN receives a Node Alive Request message or a Echo Request message from a presumed dead SGSN, it will immediately assume the SGSN is active again.

If the GGSN discovers that an SGSN has become unresponsive, it will terminate all PDP contexts that had been established with the SGSN.

**Example**

The following command configures the GGSN service to send GTP Echo packets every 120 seconds:

```
   echo-interval 120
```
**echo-retransmission-timeout**

Configures the timeout for GTPv1 echo message retransmissions for this service.

**Product**
GGSN

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > GGSN Service Configuration

```plaintext
configure > context context_name > ggsn-service service_name
```

Entering the above command sequence results in the following prompt:

```plaintext
[context_name]host_name(config-ggsn-service)#
```

**Syntax**

```plaintext
echo-retransmission-timeout seconds
default echo-retransmission-timeout
```

**default echo-retransmission-timeout**

```plaintext
default
```

Returns the command to its default setting of 3.

```plaintext
seconds
```

Default: 5

Configures the echo retransmission timeout, in seconds, for the GTPv1 service as an integer ranging from 1 to 20.

**Usage**

Use this command to configure the amount of time, in seconds, before the GTPv1 service transmits another echo request message. The value set in this command is used, as is, for the default echo. If dynamic echo is enabled (echo-interval dynamic) the value set in this command serves as the dynamic minimum (if the RTT multiplied by the smooth factor is less than the value set in this command, the service uses this value).

**Example**

The following command sets the retransmission timeout for echo messages to 2 seconds:

```plaintext
echo-retransmission-timeout 2
```
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**
Use this command to return to the Exec mode.
**exit**

Exits the current mode and returns to the parent configuration mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

`exit`

**Usage**

Use this command to return to the parent configuration mode.
 fqdn

This command defines Fully Qualified Domain Name (FQDN) which would be used for authorization over S6b interface between GGSN and 3GPP AAA/HSS.

Product
GGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > GGSN Service Configuration
configure > context context_name > ggsn-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ggsn-service)#

Syntax

fqdn host host_name realm realm_id

{ no | default } fqdn

no

Removes the configured FQDN host name and realm ID from the GGSN service.

default

Sets the system to default mode for this command and configures the host and realm ID value to NULL.

host host_name

Specifies the name of the host to be used for authorization over an S6b interface to a 3GPP AAA server/HSS from the GGSN service.
host_name is a unique node name for authorization over the S6b interface from this GGSN service.
host_name must be an alphanumeric string of 1 through 127 characters. Punctuation marks are allowed.

realm realm_id

 Specifies the realm as an FQDN to be used for authorization over S6b interface with 3GPP AAA server/HSS from GGSN service. The realm may typically be a company or service name.
realm_id is a unique identifier configured for the authorization over S6b interface from this GGSN service, expressed as an alphanumeric string of 1 through 127 characters. Punctuation marks are allowed.

host_name

Usage

Use this command to define host and realm as the FQDN for a 3GPP AAA server/HSS that would be used for authorization over an S6b interface with the GGSN. The realm specified as an FQDN may typically be a company or service name.
By default the FQDN host and realm will be NULL.
Important: This command is a license-enabled feature.

Example

The following configures the hss1 as host name and xyz.com as realm to support authorization over an S6b from this GGSN service:

```
fqdn host hss1 realm xyz.com
```
gtpc map-mbr-ambr

This command maps the Maximum Bit Rate AVP received in Update PDP Context QoS message from SGSN to Aggregate Maximum Bit Rate attribute value (AMBR), if AMBR is not received in Update PDP Context QoS message from SGSN. This command is applicable for Gn-Gp GGSN mode only and not applicable to standalone GGSN. By default this command is disabled.

Product
GGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > GGSN Service Configuration

configure > context context_name > ggsn-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ggsn-service)#

Syntax

[ default | no ] gtpc map-mbr-ambr

default
Sets the default mode to map the Maximum Bit Rate AVP received in Update PDP Context QoS message from SGSN to Aggregate Maximum Bit Rate attribute value (AMBR), if AMBR is not received in Update PDP Context QoS message from SGSN.

no
Removes the configured mapping of the MBR AVP received in Update PDP Context message from SGSN to AMBR attribute value.

Usage
Use this command to map the Maximum Bit Rate AVP received in Update PDP Context QoS message from SGSN to Aggregate Maximum Bit Rate attribute value (AMBR), if AMBR is not received in Update PDP Context QoS message from SGSN.

Important: To use this command event trigger for QoS-Change for session must be provisioned on PCRF.

Example

The following command configures the GGSN service to map the MBR received in Update PDP Context QoS message from SGSN to Aggregate Maximum Bit Rate attribute value (AMBR):

  gtpc map-mbr-ambr
gtpc nsapi-in-create-pdp-response

This command excludes or includes the optional information element (IE) Network Service Access Point Identifier (NSAPI) within “Create PDP Context Response” messages in GTP-C.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > GGSN Service Configuration
configure > context context_name > ggsn-service service_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ggsn-service)#
```

**Syntax**

```
[ default | no ] gtpc nsapi-in-create-pdp-response
```

- **default**
  Sets the default mode for GTP-C messages not to include the NSAPI IE in “Create PDP Context Response” messages.

- **no**
  Removes the preconfigured mode for GTP-C messages; the GTP-C message will not include the NSAPI IE in “Create PDP Context Response” messages. By default it is disabled.

**Usage**
Use this command to exclude or include the NSAPI IE in “Create PDP Context Response” GTP-C messages received from the SGSN.

**Example**
The following command configures the GGSN service to include the optional NSAPI IE in “Create PDP Context Response” messages:

```
gtpc nsapi-in-create-pdp-response
```
operator-del-cause

This CLI will enable or disable the Cause-IE feature for Delete PDP Context Request in GGSN.

Important: This command is license dependent. For more information please contact your Cisco account representative.

Product
GGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > GGSN Service Configuration
configure > context context_name > ggsn-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ggsn-service)#

Syntax

gtpc operator-del-cause

default gtpc operator-del-cause

no gtpc operator-del-cause

operator-del-cause

Enables or Disables Operator Cause-IE Behavior Feature for Delete PDP Context Request sent to delete the last PDP Context of the PDN connection. This CLI is disabled by default.

default

Sets the default mode for Operator Cause-IE Behavior Feature. By default, it is disabled.

no

Disables Operator Cause-IE Behavior Feature.

Usage
This CLI enables or disables the Cause-IE feature for Delete PDP Context Request in GGSN. The Cause-IE configuration for Delete PDP Context Request is given in the APN configuration and is also available in clear subscribers CLI. When this new CLI is enabled, the feature will be applied to GGSN based on the APN configuration or the clear subscribers CLI. This new CLI will be disabled by default.

Example
The following command enables the Cause-IE feature.

gtpc operator-del-cause
**gtpc private-extension**

This command includes customer-specific private extensions in GTP-C messages.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > GGSN Service Configuration

```bash
configure > context context_name > ggsn-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ggsn-service)#
```

**Syntax**

```bash
gtpc private-extension { { { focs | odb } access-list acl_name in disconnect-on-violation } | ggsn-preservation-mode | loss-of-radio-coverage | none }
```

```bash
default gtpc private-extension
```

```bash
no gtpc private-extension [ focs | ggsn-preservation-mode | loss-of-radio-coverage ]
```

- **default**
  Sets the default mode for GTP-C messages. By default it is disabled.

- **no**
  Disables the configured private extensions for GTP-C messages.

- **{focs | odb} access-list acl_name in disconnect-on-violation**
  Configures the Free-Of-Charge-Service (FOCS) and Operator Determined Barring (ODB) extensions for all packet-oriented services as defined by operators.

  - **focs**: Enables or disables Free of Charge Services for the subscriber who has no credit, and also takes the access-list `acl_name` to be applied for FOCS.
  - **odb**: Enables or disables “all packet oriented service barred” for the subscriber, and also takes the access-list `acl_name` to be applied for ODB.

  `acl_name` is the name of a configured access control list (ACL) for this service.

- **ggsn-preservation-mode**
  Enables the processing of customer-specific private extension in Update PDP Context requests. This extension indicates whether the subscriber is active or idle, and whether RAN resources have been released. It also indicates the desired “type” of preservation mode behavior.

  When `ggsn-preservation-mode` is configured, different types of accounting records are generated based on the “type” of mode. To enable the generation of different accounting records, the trigger for preservation...
mode must be configured for RADIUS or GTPP for that accounting protocol. If that trigger is not configured, there will be no change in the generation of accounting records.

**Important:** This is a customer-specific keyword and needs customer-specific license to use this feature.

---

**loss-of-radio-coverage**

Enables the protection against overcharging a subscriber due to loss of radio coverage (LORC) in a GGSN service. It also enables the system to understand the private extension for LORC) in GTP-C Update PDP Context messages from the SGSN.

**Important:** This is a license enabled keyword and need feature-specific license to use it.

---

**none**

Removes the private extensions from record which are from GTP-C messages received from the SGSN.

---

**Usage**

Use this command to configure the processing of private extensions within GTP-C messages received from the SGSN. It also configures the customer specific features, such as preservation mode for GGSN service. Overcharging protection (LORC) is a solution which provides the ability to accurately bill customers. This implementation is based on Cisco-specific private extension to GTP messages and/or any co-relation of G-CDRs and S-CDRs. It also does not modify any RANAP messages.

**Important:** This is a license enabled command that requires installation of feature-specific licenses to use this command.

---

**Example**

The following command configures the GGSN service to record the private extension for protecting the subscribers from overcharging during loss of radio coverage:

```
gtpc private-extension loss-of-radio-coverage
```
gtpc ran-procedure-ready-delay

This command configures the GGSN to enable the RAN Procedure Ready feature for the particular GGSN service and specify the timeout period for the RAN procedure timer in the GGSN. This timer starts on arrival of every secondary Create PDP Context request.

Product
GGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > GGSN Service Configuration

configure > context context_name > ggsn-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ggsn-service)#

Syntax

```
gtpc ran-procedure-ready-delay { timeout dur } { default | no } gtpc ran-procedure-ready-delay
```

**default**
Sets the default mode of RAN Procedure Ready feature for this GGSN service. By default it is disabled.

**no**
Disables the RAN Procedure Ready feature for this GGSN service. By default it is disabled.

**timeout dur**
Default: 10
Specifies the timeout duration (in seconds) for the RAN procedure timer. This timer starts on the arrival of every secondary “Create PDP Context Request” message. This is an optional keyword. If no timeout period is specified, the default value is 10 seconds. `dur` must be an integer from 1 through 40.

Usage

Use this command to enable the RAN Procedure Ready feature for this GGSN service and specify the timeout period for the RAN procedure timer. This timer starts on the arrival of every secondary “Create PDP Context Request” message. The GGSN waits until the Radio Access Bearer setup is completed and “Update PDP Context Request” is sent by the SGSN. If any downlink data is received before arrival of the “Update PDP Context Request” or before timer expiry, the downlink packets will be queued or buffered. If the buffer becomes full (total buffer limit is of 1024 packets), all newly arriving packets are dropped.

The RAN Procedure Ready feature supports the following scenarios when RAB setup timer starts at the GGSN:
• If the GGSN receives the “Update PDP Context Request” before timer expiry, the GGSN stops the timer, sends all the queued/buffered packets in ‘first-in first-out’ manner and disables buffering of subsequent downlink data.

• If the GGSN receives the “Update PDP Context Request” before the timer expires, it processes the “Update PDP Context Request” as usual, but does not disable the buffering of downlink data. It then waits for another “Update PDP Context Request” to come with the RAN Procedure Ready set, or waits for timer to expire.

• If the GGSN does not receive the “Update PDP Context Request” with RAN Procedure Ready set before timer expiry, the timer is fired and the GGSN starts sending all queued packets and disables buffering of subsequent downlink data (assuming that the corresponding SGSN does not support this feature).

• If the timer has expired and the GGSN receives an “Update PDP Context Request” for a secondary PDP context with or without RAN Procedure Ready bit set, the UPC will be processed normally without buffering the packets.

**Important:** This feature does not affect the Enhanced Charging Service or deep packet inspection (DPI) since the buffering of downlink data is done before sending it to an ACSMgr.

**Important:** During an SGSN handoff scenario all packets are processed normally and the downlink packets are buffered until the timer expires.

**Example**

The following command configures the GGSN service to enable the RAN Procedure Ready feature and specify the timeout period as 20 seconds for the RAN Procedure timer in GGSN:

```
gtpc ran-procedure-ready-delay timeout 20
```
**gtpc support-earp**

Enables Evolved ARP (e-ARP) support for GGSN service on Gn-Gp interface.

**Product**
GGSN

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > GGSN Service Configuration

**Syntax**

```
[ default | no ] gtpc support-earp
```

- **no**
  Ignores E-ARP IE received in CPC/UPC Messages.

- **default**
  Sets the E-ARP support behavior to default, or disables the support.

**Usage**

NRUPC initiated by GGSN/PGW is not responded to by the SGSNs of some vendors where behavior of SGSN is not compliant to standards. To accommodate SGSN non-compliance, the GGSN/PGW software has been enhanced with CLI-controlled behavior to suppress sending of the GGSN/PGW-initiated UPC only if SGSN requested values are less than PCRF authorized bit rates and if the values of the “No QoS Negotiation” and “Upgrade QoS Supported” flags received in the SGSN-initiated Update Request does not allow change/upgrade in QoS values in Update Response. By default, this behavior is disabled and it should be enabled if interoperability issues are seen with the SGSN.

When SGSN informs GGSN that, for a transaction either for Create PDP context Request or Update PDP Context Request, if(SGSN) does not support QoS-Upgrade and/or QoS-Negotiation, and if GGSN has to modify(either upgrade or degrade), QoS, then GGSN sends SGSN a response with unchanged QoS. Followed by the response, GGSN initiates a NRUPC with modified QoS. This is NRUPC for QoS-Change. To honor common flags suppress NRUPC cli's are introduced.

This command suppress NRUPC (for qos-change) sent from GGSN to SGSN under following condition:

- When SGSN sends Create PDP Context Request with UQS=0. If Upgrade QoS Supported bit of the Common Flags IE is set to 0 or the Common Flags IE is absent then the SGSN does not support QoS upgrade in Response message functionality.
- When SGSN sends Update PDP Context Request with NQN flag = 1.
- When SGSN sends Update PDP Context Request QoS Update Support flag = 0

This suppression feature works with a limited functionality as follows:

- It works only on MBR and def-eps-qos.
- It holds if MBR in CPC/ UPC Request < AMBR authorized by (PCRF/MME).
- AMBR is not related to common flags hence no suppression on modification of AMBR.
• It doesn’t hold if MBR in CPC/ UPC Request > AMBR authorized by (PCRF/MME). NRUPC will be generated to equalize the value of MBR to AMBR.

This command enables Evolved ARP support for GGSN service on Gn-Gp interface. Changing E-ARP support for GGSN service can impact existing bearers. By default E-ARP support is disabled.

⚠️ **Caution:** Changing the E-ARP support status from ‘disable’ (default) to ‘enable’ will have less or no impact on existing calls whereas changing the E-ARP support status from ‘enable’ to ‘disable’ will have more impact on existing calls.

**Example**

The following example disables the e-ARP support:

```
default gtpc support-earp
```
gtpc suppress-nrupc

This command helps enabling as well as disabling the NRUPC suppression.

Product
GGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > GGSN Service Configuration

cfgurre > context context_name > ggsn-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ggsn-service)#

Syntax

[ no ] gtpc suppress-nrupc { cpc | upc } { qos-change }

no
Disables the NRUPC suppression.

Usage
This command is used to enable or disable the NRUPC suppression caused by QoS change.

Example
The following example disables the NRUPC suppression using “upc” as GTP procedure:

no gtpc suppress-nrupc upc qos-change
gtpu echo-interval

This command is obsolete and now available for configuration in GTP-U service configuration mode.
guard-interval

Configures the time period after which a redundant PDP context request received from an SGSN is treated as a new request rather than a re-send of a previous request.

**Product**

GGSN

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > GGSN Service Configuration

configure > context context_name > ggsn-service service_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ggsn-service)#
```

**Syntax**

```
guard-interval guard_time

{ default | no } guard-interval
```

**Usage**

The guard interval is used to protect against replay attacks. Without a guard interval configured, information from a valid PDP context request could be used to gain un-authorized network access.

If the GGSN service receives a PDP context request in which the International Mobile Subscriber Identity (IMSI), the Network Service Access Point Identifier (NSAPI), the end user IP address, and the GTP sequence number are identical to those received in a previous request, the GGSN treats the new request as a re-send of the original. Therefore, information from a valid PDP context request could be collected and re-sent at a later time by an un-authorized user to gain network access.

Configuring a guard interval limits the amount of time that the information contained within a PDP context request remains valid.

**Example**

The following command configures the GGSN service with a guard interval of 60 seconds:
guard-interval 60
ip local-port

Configures the local User Datagram Protocol (UDP) port for the Gn interfaces’ GTP-C socket for GTPv1.

Product
GGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > GGSN Service Configuration
configure > context context_name > ggsn-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ggsn-service)#

Syntax

ip local-port gtpc-v1 port#
default ip local-port gtpc-v1

default

Configures the default value for the local UDP port for GTP Version 1 control messaging for this GGSN service.

gtpc-v1 port#

Default: 2123
Specifies the UDP port number for GTPv1 GTPC sockets.
port# can be configured to an integer from 1 through 65535.

Usage

By default, the GGSN service attempts to use GTPv1 when communicating with SGSNs. This parameter configures the UDP port over which the GTP control (GTP-C) sockets are sent. If an SGSN only supports GTPv0, the GGSN service automatically switches to GTPv0 when communicating with this SGSN. In the scenario, the GGSN service communicates with the SGSN on UDP port 3386 and does not have a GTP-C socket.

Important: The UDP port setting on the SGSN must match the local-port setting for the GGSN service on the system in order for the two devices to communicate.

Example

The following command configures the GGSN service to use UDP port 2500 for exchanging GTPC sockets with SGSNs when using GTPv1:

   ip local port 2500
ip qos-dscp

Configures the quality of service (QOS) differentiated service code point (DSCP) used when sending data packets over the Gn interface.

Product
GGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > GGSN Service Configuration

configure > context context_name > ggsn-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ggsn-service)#

Syntax

```plaintext
ip qos-dscp { qci { 1 { dscp } | 2 { dscp } | 3 { dscp } | 4 { dscp } | 5 { dscp |
allocation-retention-priority } | 6 { dscp | allocation-retention-priority } | 7 { dscp |
allocation-retention-priority } | 8 { dscp | allocation-retention-priority } | 9 { dscp
}} | gtpc } +

no ip qos-dscp { qci { 1 | 2 | 3 | 4 | 5 { allocation-retention-priority | dscp } | 6 { allocation-retention-priority | dscp } | 7 { allocation-retention-priority | dscp } | 8 { allocation-retention-priority | dscp } | 9 | gtpc } +
```

allocation-retention-priority

Specifies the DSCP for interactive class if the allocation priority is present in the QOS profile.

allocation-retention-priority can be the integer 1, 2, or 3.

DSCP values use the following matrix to map based on traffic handling priority and Alloc/Retention priority if the allocation priority is present in the QOS profile.

The following table shows the DSCP value matrix for allocation-retention-priority.

Table 26. Default DSCP Value Matrix

<table>
<thead>
<tr>
<th>Allocation Priority</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic Handling Priority</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>ef</td>
<td>ef</td>
<td>ef</td>
</tr>
<tr>
<td>2</td>
<td>ef</td>
<td>ef</td>
<td>ef</td>
</tr>
<tr>
<td>3</td>
<td>af21</td>
<td>af21</td>
<td>af21</td>
</tr>
<tr>
<td></td>
<td>af21</td>
<td>af21</td>
<td>af21</td>
</tr>
</tbody>
</table>
**qci**

Configures the QoS Class Identifier (QCI) attribute of QOS. Here the qci_val is the QCI for which the negotiate limit is being set; it ranges from 1 to 9.

**dscp**

Default QCI:
- 1: ef
- 2: ef
- 3: af11
- 4: af11
- 5: ef
- 6: ef
- 7: af21
- 8: af21
- 9: be

Specifies the DSCP for the specified traffic pattern. dscp can be configured to any one of the following:

<table>
<thead>
<tr>
<th>af11: Assured Forwarding 11 per-hop-behavior (PHB)</th>
<th>af32: Assured Forwarding 32 PHB</th>
</tr>
</thead>
<tbody>
<tr>
<td>af12: Assured Forwarding 12 PHB</td>
<td>af33: Assured Forwarding 33 PHB</td>
</tr>
<tr>
<td>af13: Assured Forwarding 13 PHB</td>
<td>af41: Assured Forwarding 41 PHB</td>
</tr>
<tr>
<td>af21: Assured Forwarding 21 PHB</td>
<td>af42: Assured Forwarding 42 PHB</td>
</tr>
<tr>
<td>af22: Assured Forwarding 22 PHB</td>
<td>af43: Assured Forwarding 43 PHB</td>
</tr>
<tr>
<td>af23: Assured Forwarding 23 PHB</td>
<td>be: Best effort forwarding PHB</td>
</tr>
<tr>
<td>af31: Assured Forwarding 31 PHB</td>
<td>ef: Expedited forwarding PHB</td>
</tr>
</tbody>
</table>

+ More than one of the above keywords can be entered within a single command.

**Usage**

DSCP levels can be assigned to specific traffic patterns in order to ensure that data packets are delivered according to the precedence with which they are tagged. The diffserv markings are applied to the outer IP header of every GTP data packet. The diffserv marking of the inner IP header is not modified.

The traffic patterns are defined by QCI (1 to 9). Data packets falling under the category of each of the traffic patterns are tagged with a DSCP that further indicate their precedence as shown in the following tables:
Table 27. Class structure for assured forwarding (af) levels

<table>
<thead>
<tr>
<th>Drop Precedence</th>
<th>Class 1</th>
<th>Class 2</th>
<th>Class 3</th>
<th>Class 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>af11</td>
<td>af21</td>
<td>af31</td>
<td>af41</td>
</tr>
<tr>
<td>Medium</td>
<td>af12</td>
<td>af22</td>
<td>af32</td>
<td>af41</td>
</tr>
<tr>
<td>High</td>
<td>af13</td>
<td>af23</td>
<td>af33</td>
<td>af43</td>
</tr>
</tbody>
</table>

Table 28. DSCP Precedence

<table>
<thead>
<tr>
<th>Precedence (low to high)</th>
<th>DSCP</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Best Effort (be)</td>
</tr>
<tr>
<td>1</td>
<td>Class 1</td>
</tr>
<tr>
<td>2</td>
<td>Class 2</td>
</tr>
<tr>
<td>3</td>
<td>Class 3</td>
</tr>
<tr>
<td>4</td>
<td>Class 4</td>
</tr>
<tr>
<td>5</td>
<td>Express Forwarding (ef)</td>
</tr>
</tbody>
</table>

The DSCP level can be configured for multiple traffic patterns within a single instance of this command. The `no ip qos` command can be issued to remove a QOS setting and return it to it’s default setting.

**Example**

The following command configures the DSCP level for QCI to be Expedited Forwarding, `ef`:

```
   ip qos-dscp qci 1 ef
```
max-contexts

Configures the maximum Primary, Secondary per Primary, and PPP context limits for the GGSN service.

Product
GGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > GGSN Service Configuration
configure > context context_name > ggsn-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ggsn-service)#

Syntax

max-contexts { max-primary max_pri_number | max-sec-per-primary max_sec_number | ppp-pdp-contexts context_number }

default max-contexts

default

Configures the default value for maximum contexts for the GGSN service.

max-primary max_pri_number

Configures maximum primary PDP context allowed for this service. This includes PPP contexts also.
max_pri_number can be configured to an integer from 0 through 4000000.

max-sec-per-primary max_sec_number

Default: 10
Indicates the maximum number of times that GTP control packets are retransmitted.
max_sec_number can be configured to an integer from 0 through 10.

ppp-pdp-contexts context_number

Configures maximum PPP pdp context allowed for this service.
context_number can be configured to an integer from 0 through 4000000.

Usage

This command is used to limit the number of primary contexts including PPP contexts, number of secondary contexts per primary context, and PPP contexts per GGSN service.

Example

The following command configures the limits for primary, secondary contexts per primary, as well as the PPP contexts for a GGSN service:

max-contexts max-primary 4000000 max-sec-per-primary 10 ppp-pdp-contexts 250000
max-retransmissions

Configures the maximum number of times that GTP control packets are retransmitted to an SGSN before it marks it unreachable.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > GGSN Service Configuration

```bash
configure > context context_name > ggsn-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ggsn-service)#
```

**Syntax**

```bash
max-retransmissions max_number
```

```bash
default max-retransmissions
```

**default**

Configures the default value for maximum retries for GTP control packets for the GGSN service.

```bash
max_number
```

Default: 4

Indicates the maximum number of times that GTP control packets are retransmitted.

*max_number* can be configured to an integer from 0 through 15.

**Usage**

This command is used in conjunction with the *timeout* command to control the retransmission of GTP control packets when no response is received from an SGSN. It is equivalent to the N3-REQUESTS parameter discussed in 3GPP TS 29.060.

If no response is received from the SGSN prior to the expiration of the timeout value, the GTP control packets are re-sent by the GGSN. This process occurs as many times as allowed by the configuration of this command.

If the max-retransmissions value is exceeded, the GGSN records a “Path Failure” for that SGSN and releases all PDP contexts associated with it.

**Example**

The following command configures the maximum number of retransmissions to 8:

```bash
max-retransmissions 8
```
mbms policy

This command enables/disables the Multimedia Broadcast Multicast Services (MBMS) user service support for multicast and/or broadcast mode. It also specifies the policy for MBMS user service mode.

Product
GGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > GGSN Service Configuration

configure > context context_name > ggsn-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ggsn-service)#

Syntax

mbms policy { multicst broadcast | none }

{ no | default } mbms policy

no

Removes or disables the configured MBMS support for multicast and/or broadcast mode in this GGSN service.

default

Restores the default mode of MBMS support in this GGSN service.

multicst broadcast

Enables the MBMS support and configures the policy for multicast and broadcast of user service.

Usage
Use this command to enable/disable the MBMS user service support for Multicast and/or Broadcast mode. It also specifies the policy for MBMS user service mode.

Example
The following command enables MBMS support in this GGSN service:

mbms policy multicast broadcast
newcall

This command enables or disables the new call related behavior of this GGSN service when duplicate sessions with the same IP address request are received. This feature is required to support interworking with P-GW and HA.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > GGSN Service Configuration

```plaintext
configure > context context_name > ggsn-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ggsn-service)#
```

**Syntax**

```plaintext
newcall duplicate-subscriber-requested-address { accept | reject }

default newcall duplicate-subscriber-requested-address
```

---

**default**

Restores the default mode for new call session with the same address request received in this GGSN service. It rejects calls with duplicate address requests.

**accept**

Sets the system to “accept” another session using the same IP address for a new call. The new session will be created and the old session will be torn down.  
Default: Disabled

**reject**

Rejects new calls with duplicate address requests. This is the default behavior.  
Default: Enabled

**Usage**

Use this command to enable or disable new call connections when the UE is not able to gracefully disconnect from the Enterprise PDN before attempting to reconnect via another access method. When enabled this command tears down the old session in order to accept the new connection with the same IP address assignment.  
This feature also allows the GGSN to accept a request for a static subscriber address, even if the address is already used by another session. If this feature is not enabled, a new request with the same IP address for another session will be rejected.

---

**Important:** This command is a license-enabled feature.
Example

The following command allows the GGSN to accept the duplicate call session request with the same IP address:

```
newcall duplicate-subscriber-requested-address accept
```
path-failure

Determines the GTP path-failure behavior on echo/non-echo messages.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > GGSN Service Configuration

```
configure > context context_name > ggsn-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ggsn-service)#
```

**Syntax**

```
path-failure detection-policy gtp { echo [ non-echo ] | non-echo [ echo ] }
```

**Usage**

Under current circumstances, a GGSN shuts down the GTP tunnel if the associated SGSN does not respond to multiple retries of an echo or non-echo message from the GGSN. In this way, a single call failure could be responsible for the loss of all active calls in the tunnel. This is also an issue when echo is disabled, or when there is very little traffic on the SGSN and the GGSN is configured with large echo intervals. This behavior adversely impacts the user experience because the customer has to reconnect every time this happens with their SGSN.

**Example**

The following example detects path failures when the SGSN fails to respond to multiple echo message retries:

```
path-failure detection-policy gtp echo
```
The following example turns off path-failure detection. On timeout of gtp(c) message retries, the particular context will be purged:

```
no path-failure detection-policy
```
**plmn id**

Configures the GGSN’s public land mobile network (PLMN) identifiers. Up to five PLMN IDs can be configured for each GGSN service.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > GGSN Service Configuration

`configure > context context_name > ggsn-service service_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ggsn-service)#
```

**Syntax**

```
plmn id mcc mcc_value mnc mnc_value [ primary ]

no plmn id mcc mcc_value [ mnc mnc_value ]
```

**no**

Removes a previously configured PLMN identifier for the GGSN service.

**mcc mcc_value**

Specifies the mobile country code (MCC) portion of the PLMN’s identifier. `mcc_number` is the PLMN MCC identifier and can be configured to an integer between 100 and 999.

**mnc mnc_value**

Specifies the mobile network code (MNC) portion of the PLMN’s identifier. This option is optional. `mnc_number` is the PLMN MNC identifier and can be configured to any 2- or 3-digit integer from 00 through 999.

**primary**

When multiple PLMN IDs are configured, the `primary` keyword can be used to designate one of the PLMN IDs to be used for the AAA attribute (3GPP-GGSN-MCC-MNC).

**Usage**

The PLMN identifier is used by the GGSN service to determine whether or not a mobile station is visiting, roaming, or home. Multiple GGSN services can be configured with the same PLMN identifier. Up to five PLMN IDs can be configured for each GGSN Service.

**Example**

The following command configures the PLMN identifier with an MCC of 462 and MNC of 2:

```
plmn id mcc 462 mnc 02
```
**plmn unlisted-sgsn**

Configures the GGSN’s policy for handling communications from SGSNs with which it is not configured to communicate.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > GGSN Service Configuration

```
configure > context context_name > ggsn-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ggsn-service)#
```

**Syntax**

```
default plmn unlisted-sgsn
```

```
```

**default**
Resets configured parameters to their default settings.

**foreign**
Default: Disabled
Specifies that the GGSN service accepts messages from SGSNs that are not configured within the service using the **sgsn address** command.
This keyword also dictates that unlisted SGSNs are treated as if they belong to a foreign PLMN. Therefore, PDP contexts originating from them are treated as visiting or roaming.

**mcc mcc_value**
Specifies the mobile country code (MCC) portion of the PLMN’s identifier.
**mcc_value** is the PLMN MCC identifier and can be configured to an integer from 100 through 999.

**mnc mnc_value**
Specifies the mobile network code (MNC) portion of the PLMN’s identifier.
**mnc_value** is the PLMN MNC identifier and can be configured to a 2- or 3-digit integer from 00 through 999.

**disable-gtpc-echo**
Default: Send GTPC Echo messages to unlisted SGSNs.
When this keyword is specified, GTPC echo messages are not sent to unlisted SGSNs.

reject-foreign-subscriber
Default: Disabled
Specifies that incoming calls from foreign subscribers are rejected.

home
Default: Disabled
Specifies that the GGSN service accepts messages from SGSNs that are not configured within the service using the `sgsn address` command. This keyword also dictates that unlisted SGSNs are treated as if they belong to the GGSN service’s home PLMN.

rat-type { GAN | GERAN | HSPA | UTRAN | WLAN }
This keyword configures the type of radio access technology.
GERAN: Specifies the GSM EDGE Radio Access Network type of RAT.
HSPA: Specifies the High Speed Packet Access type of RAT.
UTRAN: Specifies the UMTS Terrestrial Radio Access Network type of RAT.
WLAN: Specifies the Wireless Local Access Network type of RAT.

reject
Default: Enabled
Specifies that the GGSN service rejects messages from SGSNs that are not configured within the service using the `sgsn address` command. When the GGSN service rejects the message(s), it returns a cause code of No Resources 199 (C7H, No resources available).

Usage
This command works in conjunction with the `sgsn` command that configures the GGSN service to communicate with specific SGSNs. Any messages received from SGSNs not configured in that list are subject to the rules dictated by the `unlisted-sgsn` policy.

Example
The following command configures the GGSN service to accept messages from unlisted SGSNs and treat the SGSN as if it is on the GGSN’s home network:

```plaintext
plmn unlisted-sgsn accept home
```
**policy**

Specifies the reject code to be used in the “Create PDP Context” response message when a RADIUS server timeouts.

**Product**

GGSN

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > GGSN Service Configuration

```
configure > context context_name > ggsn-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ggsn-service)#
```

**Syntax**

```
policy { accounting-server-timeout use-reject-code { system-failure | no-resources } | authentication-server-timeout use-reject-code { system-failure | user-authentication-failure } }

default policy { authentication-server-timeout | accounting-server-timeout }
```

---

**default**

Restores the specified parameter to its default setting.

| accounting-server-timeout use-reject-code { system-failure | no-resources } |
|-----------------------------------|
| **Default:** no-resources         |
| Specifies the reject code used by the GGSN if communication with an accounting server times out. The possible reject codes are: |
| • system-failure (204 (CCH))       |
| • no-resources (199 (C7H))         |

| authentication-server-timeout use-reject-code { system-failure | user-authentication-failure } |
|-----------------------------------|
| **Default:** user-authentication-failure |
| Specifies the reject code used by the GGSN if communication with an authentication server times out. The possible reject codes are: |
| • system-failure (204 (CCH))       |
| • user-authentication-failure (209 (D1H)) |

**Usage**

This command is used to configure the cause code used by the GGSN if communication with either a RADIUS authentication or accounting server times out.

When this parameter is used in conjunction with Radius accounting servers, the response is only set if a flag is configured in the APN Delay GTP Response, only after getting a response to the Accounting Start.
Example

The following command configures the GGSN response to a RADIUS authentication server timeout to be `system-failure`:

```
policy authentication-server-timeout use-reject-code system-failure
```
retransmission-timeout

Configures the timeout period in between retransmissions of GTP control packets. This timeout configuration is not applicable on Echo Request retransmission.

**Important:** In 17.3 and later releases, this command has been deprecated.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > GGSN Service Configuration

```
configure > context context_name > ggsn-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name] host_name(config-ggsn-service)#
```

**Syntax**

```
retransmission-timeout retransmit_time
```

**default retransmission-timeout**

```
default
```

Configures the default time interval that must pass without an SGSN response before the GGSN service retransmits GTP control packets.

```
retransmit_time
```

Default: 5

Specifies the amount of time that must pass without an SGSN response before the GGSN service retransmits GTP control packets. `retransmit_time` is measured in seconds and can be configured to an integer from 1 through 20.

**Usage**

This command is used in conjunction with the `max-retransmissions` command to control the retransmission of GTP control packets when no response is received from an SGSN.

If no response is received from the SGSN prior to the expiration of the timeout value, the GTP control packets are re-sent by the GGSN. This process occurs as many times as allowed by the configuration of the `max-retransmissions` command.

If the `max-retransmissions` value is exceeded within the retransmission-timeout period, the GGSN records a “Path Failure” for that SGSN and releases all PDP contexts associated with it.

**Important:** This retransmission timeout configuration in not applicable for Echo Requests message retransmission. Echo are sent/retransmitted every echo interval, which can be configured separately.
Example

The following command configures a timeout value of 20 seconds:

```
retransmission-timeout 20
```
**setup-timeout**

Configures the maximum amount of time the GGSN service allows for the setting up of PDP contexts.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > GGSN Service Configuration

```config
configure > context context_name > ggsn-service service_name
```

Entering the above command sequence results in the following prompt:

```
<context_name>host_name(config-ggsn-service)#
```

**Syntax**

```
setup-timeout setup_time
```

```
default setup-timeout
```

**Usage**

Use this command to limit the amount of time allowed for setting up PDP contexts. If the PDP context is not setup within the configured time frame, the GGSN service rejects the PDP context with a cause code of 199 (C7H, No resources available).

**Example**

The following command allows a maximum of 120 seconds for the setting up of PDP contexts:

```
setup-timeout 120
```
sgsn address

Configures the SGSNs that this GGSN service is allowed to communicate with.

Product
GGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > GGSN Service Configuration

configure > context context_name > ggsn-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ggsn-service)#

Syntax

sgsn address { { ip_address [ subnetmask netmask ] } | ip_address/netmask } [ plmn-foreign [ reject-foreign-subscriber ] | mcc mcc_code mnc mnc_code [ reject-foreign-subscriber ] ] [ rat-type { GAN | GERAN | HSPA | UTRAN | WLAN } ] [ description description ] [ disable-gtpc-echo ]

no sgsn { address ip_address [ subnetmask netmask ] }

no

Removes a specific SGSN from the list or all configured SGSNs.

address

Configures the IP address of the SGSN.

ip_address must be expressed in IPv4 dotted-decimal notation.

subnetmask

Configures the subnet mask of the SGSN.

netmask must be expressed in IPv4 dotted-decimal notation.

disable-gtpc-echo

Default: Send GTPC Echo messages to unlisted SGSNs.

When this keyword is specified, GTPC echo messages are not sent to unlisted SGSNs.

plmn-foreign

Indicates whether or not the SGSN belongs to a foreign public land mobile network (PLMN).

reject-foreign-subscriber

Default: Disabled

Specifies that incoming calls from foreign subscribers are rejected.
mcc  mcc_code

Specifies the mobile country code (MCC) portion of the PLMN’s identifier.
mcc_code is the PLMN MCC identifier and configured as an integer from 100 through 999.

mnc  mnc_code

Specifies the mobile network code (MNC) portion of the PLMN’s identifier.
mnc_code is the PLMN MNC identifier and configured as a 2- or 3-digit integer from 00 through 999.

rat-type {GAN | GERAN | HSPA | UTRAN | WLAN }

This keyword configures the type of radio access technology.
GERAN: Specifies the GSM EDGE Radio Access Network type of RAT.
HSPA: Specifies the High Speed Packet Access type of RAT.
UTRAN: Specifies the UMTS Terrestrial Radio Access Network type of RAT.
WLAN: Specifies the Wireless Local Access Network type of RAT.

description  description

Add description field to the SGSN entry in GGSN service.
description is an alphanumeric string of 1 through 63 characters.

Usage

Use this command to configure a list of SGSNs that the GGSN service is to communicate with. This command can be entered multiple times to configure multiple SGSNs.

Important: The GGSN only communicates with the SGSNs configured using this command unless a plmn-policy is enabled to allow communication with unconfigured SGSNs. PLMN policies are configured using the plmn unlisted-sgsn command.

Example

The following command configures the GGSN to communicate with an SGSN on a foreign PLMN with an IP address of 192.168.1.100 and subnet mask of 255.255.255.0:
sgn address 192.168.1.100 subnetmask 255.255.255.0 plmn-foreign
sgsn define-multiple-address-group

This command defines an SGSN Multiple Address Group and enters SGSN Multiple Address Group Configuration mode. Whenever there is a change in the control address in a GTPC UPC message, it is treated as an inter-SGSN handoff because an SGSN is usually identified uniquely by a single IP-address. This command supports a multiple address group feature which allows you to specify a set of addresses that specify a single SGSN. When a UPC handoff is received from any address in the group, it is treated as an intra-SGSN handoff.

Product
GGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > GGSN Service Configuration

configure > context context_name > ggsn-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ggsn-service)#

Syntax

sgsn define-multiple-address-group grp_name [ -noconfirm ]

no sgsn define-multiple-address-group grp_name

no

Removes a specific SGSN Multiple Address Group from the list GGSN service configuration.

grp_name

Specifies the name of an SGSN multiple address group to create or configure. grp_name is an alphanumeric string from 1 through 63 characters.

-noconfirm

Specifies that the command must execute without any additional prompt and confirmation from the user.

Usage

Use this command to create or configure an SGSN Multiple Address Group that the GGSN service is to communicate with. This command can be entered multiple times to configure multiple SGSN Multiple Address Groups.

Example

The following command creates an SGSN Multiple Address Group named sgsngrp1 and enters SGSN Multiple Address Group Configuration mode:

sgsn define-multiple-address-group sgsngrp1
sgsn multiple-address-group

Configures the SGSN multiple address groups that this GGSN service is allowed to communicate with.

Product
GGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > GGSN Service Configuration

configure > context context_name > ggsn-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ggsn-service)#

Syntax

sgsn multiple-address-group grp_name [ disable-gtpc-echo ] [ mcc mcc_code mnc mnc_code [ reject-foreign-subscriber ] ] [ plmn-foreign [ reject-foreign-subscriber ] [ rat-type { GAN | GERAN | HSPA | UTRAN | WLAN } ] [ description description ]

no sgsn multiple-address-group grp_name

no

Removes a specific SGSN multiple address group from the list of configured SGSN multiple address groups.

grp_name
Specifies the name of a configured SGSN multiple address group to use.

disable-gtpc-echo
Default: Send GTPC Echo messages to unlisted SGSNs.
When this keyword is specified, GTPC echo messages are not sent to unlisted SGSNs.

plmn-foreign
Indicates whether or not the SGSN multiple address group belongs to a foreign public land mobile network (PLMN).

reject-foreign-subscriber
Default: Disabled
Specifies that incoming calls from foreign subscribers are rejected.

mcc mcc_code
Specifies the mobile country code (MCC) portion of the PLMN’s identifier.
mcc_code is the PLMN MCC identifier and can be configured to an integer from 100 through 999.
mnc mnc_code

Specifies the mobile network code (MNC) portion of the PLMN’s identifier.

*mnc_code* is the PLMN MNC identifier configured as a 2- or 3-digit integer from 00 through 999.

rat-type { GAN | GERAN | HSPA | UTRAN | WLAN }

This keyword configures the type of radio access technology.

GERAN: Specifies the GSM EDGE Radio Access Network type of RAT.
HSPA: Specifies the High Speed Packet Access type of RAT.
UTRAN: Specifies the UMTS Terrestrial Radio Access Network type of RAT.
WLAN: Specifies the Wireless Local Access Network type of RAT.

description description

Add a description field to the SGSN multiple address group entry in the GGSN service configuration.

*description* must be an alphabetic string of 1 through 63 characters.

**Usage**

Use this command to configure a list of SGSN multiple address groups with which the GGSN service is to communicate. This command can be entered multiple times to configure multiple SGSN multiple address groups.

**Important:** The GGSN only communicates with the SGSN multiple address groups configured using this command unless a plmn-policy is enabled to allow communication with unconfigured SGSNs. PLMN policies are configured using the `plmn unlisted-sgsn` command.

**Example**

The following command configures the GGSN to communicate with an SGSN with multiple address that is defined by an SGSN multiple address group named *sgsngrp1* that is on a foreign PLMN:

```
sgsn multiple-address-group sgsngrp1 plmn-foreign
```
sgsn mcc-mnc

This command configures sgsn mcc-mnc for this GGSN service.

Product
GGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > GGSN Service Configuration

```
configure > context context_name > ggsn-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ggsn-service)#
```

Syntax

```
sgsn mcc-mnc { prefer-rai | prefer-uli }
```

```
default sgsn mcc-mnc
```

```
default
    Configures the default option for sgsn mcc-mnc. Default is ‘prefer-uli’.
```

```
prefer-rai
    Configures sgsn mcc-mnc using rai.
```

```
prefer-uli
    Configures sgsn mcc-mnc using uli.
```

Usage

Use this command to configure the sgsn mcc-mnc.

Example

The following command configures the sgsn mcc-mnc to ‘prefer-rai’:

```
sgsn mcc-mnc prefer-rai
```
**trace-collection-entity**

This command configures the trace collection entity IP address. Trace collection entity is the destination node to which trace files are transferred and stored.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > GGSN Service Configuration

```
configure > context context_name > ggsn-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ggsn-service)#
```

**Syntax**

```
trace-collection-entity IPv4_addr
no trace-collection-entity
```

- **no**

  Removes the configured IPv4 address for trace collection in this GGSN service.

- **IPv4_addr**

  Specifies the IP address in IPv4 dotted-decimal notation.

**Usage**

Use this command to configure the trace collection entity IP address. This configuration is required because during signaling session trace activation, CPC REQ and UPC REQ do not provide the IP address for the trace collection entity.

**Example**

The following command configures the trace collection entity IP address with this GGSN service:

```
trace-collection-entity 192.36.56.56
```
Chapter 140
Global Configuration Mode Commands (A-K)

This section includes the commands `aaa accounting-overload-protection` through `imei-profile`. The Global Configuration Mode is used to configure basic system-wide parameters.

Mode

Exec > Global Configuration

`configure`

Entering the above command sequence results in the following prompt:

```
[local] host_name(config) #
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
aaa accounting-overload-protection

This command configures Overload Protection Policy for accounting requests.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration

Syntax
aaa accounting-overload-protection prioritize-gtp

{ default | no } aaa accounting-overload-protection

default
Configures the default setting.
Default: no priority assigned

no
Disables the Overload Protection configuration.

prioritize-gtp
Gives higher priority to GTPP requests among the other outstanding requests. So while purging the lower priority requests will be selected first.

Usage
Use this command to configure Overload Protection Policy for accounting requests.

Example
The following command prioritizes GTPP requests among the other outstanding requests:

    aaa accounting-overload-protection prioritize-gtp
aaa default-domain

Configure global accounting and authentication default domain for subscriber and context-level administrative user sessions.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration

`configure`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```bash
aaa default-domain { administrator | subscriber } domain_name
no aaa default-domain { administrator | subscriber }
```

- **no**

Removes all or only the specified configured domain.

- **administrator | subscriber**

`administrator`: Configures the default domain for context-level administrative users.

`subscriber`: Configures the default domain for subscribers.

- **domain_name**

Sets the default context.

domain_name must be an alphanumeric string of 1 through 79 characters.

**Usage**

This command configures the default domain which is used when accounting and authentication services are required for context-level administrative user and subscriber sessions whose user name does not include a domain.

**Example**

The following commands configure the default domains for context-level administrative users and subscribers, respectively:

```bash
aaa default-domain administrator sampleAdministratorDomain
aaa default-domain subscriber sampleSubscriberDomain
```
aaa domain-matching ignore-case

This command disables case sensitivity when performing domain matching. When this command is enabled, the system disregard case when matching domains.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local] host_name(config)#

Syntax

[ no ] aaa domain-matching ignore-case

default aaa domain-matching

  default
  Configures ignore-case as the domain matching method.

  no
  Specifies that the system consider case when domain matching.

Usage
Use this command to configure the system to ignore case when matching domains.

Example
The following command configures the system to ignore case when matching domains:

  aaa domain-matching ignore-case
aaa domain-matching imsi-prefix

Enables domain lookup for session based on the International Mobile Subscriber Identity (IMSI) prefix length. Default: Disabled

**Important:** This command is only available in 8.3 and later releases.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

**Syntax**

aaa domain-matching imsi-prefix prefix-length prefix_length

no aaa domain-matching imsi-prefix

default aaa domain-matching

  no

  Specifies the system must not consider imsi-prefix domain matching method.

  prefix-length

  Specifies the IMSI length to be matched with the domain.
  *prefix_length* must be an integer from 1 through 15.

**Usage**

Use this command to configure the IMSI-prefix method of domain matching. This command enables domain lookup for the session based on the IMSI prefix length. If there is a domain configured with the matching IMSI prefix, the associated configuration is used.

This feature does not support partial matches.

**Example**

The following command configures the IMSI prefix method for domain matching setting the prefix length to 10.

```
  aaa domain-matching imsi-prefix prefix-length 10
```
aaa large-configuration

This command enables or disables the system to accept a large number of RADIUS configurations to be defined and stored.

**Important:** For this command to take affect, after entering the command the configuration must be saved and reloaded.

When aaa large-configuration is disabled, the following restrictions are in place:

- Only one (1) NAS IP address can be defined per context with the radius attribute command.
- The RADIUS attribute `nas-ip-address` can only be configured if the RADIUS group is `default`.
- Only 320 RADIUS servers can be configured system-wide.
- Only 64 RADIUS groups can be configured system-wide.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

```
[local] host_name(config) #
```

**Syntax**

```
[ no ] aaa large-configuration
```

- **no**
  Disables AAA large configuration support.

**Usage**

When aaa large-configuration is enabled, the system provides the ability to configure multiple NAS IP addresses in a single context to used with different radius groups. As well, the command allows support for up to 1,600 RADIUS server configurations and for a PDSN a maximum of 400 or for a GGSN a maximum of 800 RADIUS server group configurations system-wide.

**Example**

To enable the definition of a large number of RADIUS configurations, enter the following commands in the following order:

In APN Configuration mode, enter:

```
default aaa group
```

In Global Configuration mode, enter:
aaa large-configuration

In Exec mode, use the `save configuration` command and then the `reload` command.
The `aaa last-resort` command is used to configure global accounting and authentication last resort domain for subscriber and context-level administrative user sessions.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration
configure
Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
aaa last-resort context { administrator | subscriber context_name }
no aaa last-resort context { administrator | subscriber }
```

- **no**
  - Removes all or only the specified previously configured authentication last resort domain name.

- **administrator | subscriber**
  - **administrator**: Configures the last resort domain for context-level administrative.
  - **subscriber**: Configures the last resort domain for the subscribers.

- **context_name**
  - Specifies the context which is to be set as the last resort. `context_name` must be an alphanumeric string of 1 to 79 characters.

**Usage**

Set the last resort context which is used when there is no applicable default domain (context) and there is no domain provided with the subscriber’s or context-level administrative user’s name for use in the AAA functions.

**Example**

The following commands configure the last resort domains for context-level administrative user and subscribers, respectively:

```
aaa last-resort administrator sampleAdministratorDomain
aaa last-resort subscriber sampleSubscriberDomain
```

The following command removes the previously configured domain called `sampleAdministratorDomain`:
no aaa last-resort administrator sampleAdministratorDomain
aaa tacacs+

This command enables or disables system-wide TACACS+ AAA (authentication, authorization and accounting) services for administrative users. This command is valid only if TACACS+ servers and related services have been configured in TACACS Configuration Mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration

```plaintext
configure
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config)#
```

**Syntax**

```
[ no ] aaa tacacs+
```

**Usage**

Enables or disables the use of TACACS+ AAA services for administrative users.

**Example**

```
aaa tacacs+

no aaa tacacs+
```
aaa username-format

Configure global accounting and authentication user name formats for AAA (authentication, authorization and accounting) functions. Up to six formats may be configured.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

[ no ] aaa username-format { domain | username } separator
default aaa username-format

no
Removes the specified user name format from the configuration.

domain | username
Default: username @
domain: indicates the left side of the string from the separator character is a domain name and the right side is the user name.
username: indicates the left side of the string from the separator character is a user name and the right side is the domain name.

Important: The user name string is always searched from right to left for the first occurrence of the separator character.

separator
Specifies the character to use to delimit the domain from the user name for global AAA functions. Permitted characters include: @, %, -, \, #, or /. To specify a back slash (\) as the separator, you must enter a double back slash (\\) on the command line.

Usage
Define the formats for user name delimiting if certain domains or groups of users are to be authenticated based upon their user name versus domain name.

Example

aaa username-format domain @
aaa username-format username %

no aaa username-format username %
**active-charging service**

This command allows you to create/configure/delete the Active Charging Service (ACS)/Enhanced Charging Service (ECS).

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
active-charging service acs_service_name [ -noconfirm ]

no active-charging service acs_service_name
```

---

**Syntax**

```
active-charging service acs_service_name [ -noconfirm ]

no active-charging service acs_service_name
```

---

**no**

Deletes the specified Active Charging Service.

**acs_service_name**

Specifies name of the Active Charging Service.

*acs_service_name* must be the name of an Active Charging Service, and must be an alphanumeric string of 1 through 15 characters.

If the named Active Charging Service does not exist, it is created, and the CLI mode changes to the ACS Configuration Mode wherein the service can be configured. If the named Active Charging Service already exists, the CLI mode changes to the ACS Configuration Mode.

**-noconfirm**

Specifies that the command must execute without any additional prompt and confirmation from the user.

**Usage**

Use this command to create/configure/delete an Active Charging Service in the system. Note that, in this release, only one Active Charging Service can be created in the system.

Use this command after enabling ACS using the `require active-charging` command. This command allows administrative users to configure the ACS functionality.

On entering this command, the CLI prompt changes to:

```
[context_name]hostname(config-acs)#
```

**Example**

The following command creates an ACS service named test:

```
active-charging service test
```
alarm

Enables or disables alarming options for the SPIO card or the SSC internal alarms and the central-office external alarms. To verify the state of the alarms, refer to the `show alarm` command.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration
`configure`
Entering the above command sequence results in the following prompt:

```
[local] host_name(config) #
```

**Syntax**

```
alarm { audible | central-office }

no alarm { audible | central-office }
```

`no`
Disables the option specified.

`audible | central-office`

`audible`: indicates the internal audible alarm on the SPIO cards or SSCs are to be enabled.
`central-office`: indicates the central office alarms are to be enabled.

**Usage**
Disable CO and audible alarms when an existing device provides such capability.

**Example**
The following commands enable the SPIO card or SSC internal alarms and disable the central office alarms, respectively.

```
alarm audible

no alarm central-office
```
apn-profile

Creates an instance of an Access Point Name (APN) profile.

Product
MME
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

[ no ] apn-profile apn_profile_name

no
Deletes the APN profile instance from the configuration.

apn_profile_name
Specifies the name of the APN profile. Enter an alphanumeric string of 1 through 64 characters.

Usage
Use this command to create an instance of an APN profile and to enter the APN profile configuration mode. An APN profile is a template which groups a set of APN-specific commands that may be applicable to one or more APNs. See the APN Profile Configuration Mode Commands chapter for information regarding the definition of the rules contained within the profile and the use of the profile.

Important: An APN profile is a key element of the Operator Policy feature and is only valid when associated with at least one operator policy.

To see what APN profiles have already been created, return to the Exec mode and enter the show apn-profile all command.

Example

The following command creates a configuration instance of an APN profile:

apn-profile apnprof27
**apn-remap-table**

Creates an instance of an Access Point Name (APN) remap table.

**Product**
MME
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
[ no ] apn-remap-table apn_remap_table_name
```

- **no**
  Deletes the APN remap table instance from the configuration.

- **apn_remap_table_name**
  Specifies the name of the APN remap table. Enter an alphanumeric string of 1 through 65 characters.

**Usage**

Use this command to create an instance of an APN remap table and to enter the APN remap table configuration mode. An APN remap table includes entries that define how an incoming APN, or the lack on one, will be handled. See the *APN Remap Table Configuration Mode Commands* chapter for information regarding the definition of the entries contained within the table and the use of the table.

**Important:** An APN remap table is a key element of the Operator Policy feature and is only valid when associated with at least one operator policy.

To see what APN remap tables have already been created, return to the Exec mode and enter the `show apn-remap-table all` command.

**Example**

The following command creates a configuration instance of an APN remap table:

```
apn-remap-table pnremap-USorigins-table1
```
**arp**

Configures a system-wide time interval for performing Address Resolution Protocol (ARP) refresh.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

**configure**

Entering the above command sequence results in the following prompt:

`[local]host_name(config)#`

**Syntax**

```
arp base-reachable-time time
default arp base-reachable-time
```

---

**default**

Restores the parameter to its default setting.

**time**

Default: 30

Specifies the ARP refresh interval (in seconds) as an integer from 30 through 86400.

---

**Usage**

Use this command to configure a system-wide ARP refresh interval. Once a neighbor is found, the entry is considered valid for at least a random value between the `time/2` and the `time*1.5`.

**Example**

The following command configures an ARP refresh interval of 1 hour:

```
arp base-reachable-time 3600
```
autoconfirm

This command disables or enables confirmation for certain commands. This command affects all future CLI sessions.

**Important:** To change the behavior for the current CLI session only, use the `autoconfirm` command in the Exec Mode.

**Product**
All

**Privilege**
Security Administrator, Administrator, Operator

**Mode**
Exec > Global Configuration

`configure`
Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
autoconfirm

no autoconfirm
```

**Usage**
When autoconfirm is enabled, certain commands ask you to answer yes or no to confirm that you want to execute the command. When autoconfirm is disabled the confirmation questions never appear. Disabling autoconfirm disables command confirmation for all future CLI sessions.

By default `autoconfirm` is enabled.

**Example**

The following command enables command confirmation for all future CLI sessions;

```
autoconfirm
```

The following command disables command confirmation for all future CLI sessions;

```
no autoconfirm
```
autoless

This command is obsolete. It is included in the CLI for backward compatibility with older configuration files. When executed, this command issues a warning and performs no function.
banner

Configures the CLI banner which is displayed upon the start of a CLI session.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
banner { charging-service | lawful-intercept | motd | pre-login } string
no banner { charging-service | lawful-intercept | motd | pre-login }
```

- **no**
  Removes the banner message by setting it to be a string of zero length.

- **charging-service**
  Specifies the Active Charging Service banner message. The banner is displayed upon initialization of an SSH CLI session with ACS-admin privileges (whenever anyone with the CLI privilege bit for ACS logs on).

- **lawful-intercept**
  Refer to the *Lawful Intercept Configuration Guide* for a description of this parameter.

- **motd**
  Configures the CLI banner message of the day which is displayed upon the initialization of any CLI session.

- **pre-login**
  Configures the CLI banner displayed before a CLI user logs in.

**Important:** This banner is displayed only for serial port and telnet log ins. It is not supported in ssh and, therefore, will not be displayed before ssh log ins.

- **string**
  Specifies the banner or message to be displayed at session initialization. `string` may be an alphanumeric string of 0 through 2048 characters. The string must be enclosed in double quotation marks if the banner or message is to include spaces.
## Usage

Set the message of the day banner when an important system wide message is needed. For example, in preparation for removing a chassis from service, set the banner 1 or more days in advance to notify administrative users of the pending maintenance.

## Example

```
banner motd "Have a nice day."

banner motd No_News_Today

no banner motd
```
boot delay

Configures the delay period, in seconds, before attempting to boot the system from a software image file residing on an external network server.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
boot delay time

no boot delay
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Deletes the setting for the boot delay. The boot process executes immediately.</td>
</tr>
<tr>
<td>time</td>
<td>Specifies the amount of time (in seconds) to delay prior to requesting the software image from the external network server as an integer from 1 through 300.</td>
</tr>
</tbody>
</table>

**Usage**

Useful when booting from the network when connection delays may cause timeouts. Such as when the Spanning Tree Protocol is used on network equipment.

**Important:** The settings for this command are stored immediately in the boot.sys file. No changes are made to the system configuration file.

**Example**

The following sets the boot delay to 10 seconds:

```
boot delay 10
```
boot interface

Configures Ethernet network interfaces for obtaining a system software image during the system boot process.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

Releases prior to 12.2:

```
boot interface { spio-eth1 | spio-eth2 } [ medium { auto | speed
medium_speed duplex medium_duplex } [ media medium_media ] ]
```

```
no boot interface
```

Releases after 12.2:

```
boot interface { local-eth1 | local-eth2 } [ medium { auto | speed
medium_speed duplex medium_duplex } [ media medium_media ] ]
```

```
no
```

Removes the boot interface configuration from the boot.sys file. Only files from the local file system can be loaded.

spio-eth1 | spio-eth2

Specifies the network interface to be configured where spio-eth1 is the primary interface on the SPIO (slot 24 interface 1 or slot 25 interface 1) and spio-eth2 is the secondary interface on the SPIO (slot 24 interface 2 or slot 25 interface 2). The interfaces are either RJ-45 ifor speeds of 10, 100, or 1000 megabits per second (Mbps), or SFP for the optical Gigabit (1000 Mbps).

local-eth1 | local-eth2

Specifies the network interface to be configured where local-eth1 is the primary ethernet interface and local-eth2 is the secondary ethernet interface.

For the ASR 5000, the primary is interface 1 on the SPIO and the secondary is interface 2 on the SPIO. The interfaces are either RJ-45 ifor speeds of 10, 100, or 1000 megabits per second (Mbps), or SFP for optical Gigabit (1000 Mbps).

For the ASR 5500, the primary is port 1 (1000Base-T) on the MIO and the secondary interface is port 2 (1000Base-T) on the MIO.
```
medium { auto | speed medium_speed duplex medium_duplex }
```

Default: auto

- **auto**: configures the interface to auto-negotiate the interface speed, and duplex.
- **speed medium_speed duplex medium_duplex**: specifies the speed to use at all times where `medium_speed` must be one of:
  - 10
  - 100
  - 1000

The keyword **duplex** is used to set the communication mode of the interface where `medium_duplex` must be one of:
- full
- half

```
media medium_media
```

Default: rj45

- Optionally sets the physical interface where `medium_media` must be either rj45 or sfp.

---

### Usage

Modify the boot interface settings to ensure the system is able to obtain a software image from an external network server.

**Important**: The settings for this command are stored immediately in the boot.sys file. No changes are made to the system configuration file.

### Example

The following configures the primary interface to auto-negotiate the speed.

```bash
boot interface spio-eth1 medium auto
boot interface local-eth1 medium auto
```

The following command configures the secondary interface to a fixed gigabit speed at full duplex using RJ45 connectors for the physical interface.

```bash
boot interface spio-eth2 medium speed 1000 duplex full media rj45
boot interface local-eth2 medium speed 1000 duplex full media rj45
```

The following restores the defaults for the boot interface.

```bash
no boot interface
```
boot nameserver

Configures the IP address of the DNS (Domain Name Service) server to use when looking up hostnames in URLs for network booting.

**Product**: All

**Privilege**: Security Administrator, Administrator

**Mode**: Exec > Global Configuration configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
boot nameserver ip_address

no boot nameserver
```

- **no**
  
  Removes the network boot nameserver information from the boot.sys file.

- **ip_address**
  
  IPv4 dotted-decimal address of the DNS server the system uses to lookup hostnames in URLs for a software image from the network during the system boot process.

**Usage**

Use this command to identify the DNS server to use to lookup hostnames in a software image URL.

**Important**: The settings for this command are stored immediately in the boot.sys file. No changes are made to the system configuration file.

**Example**

The following configures the system to communicate with a DNS nameserver with the IP address of 10.2.3.4:

```
boot nameserver 10.2.3.4
```
**boot networkconfig**

Configures the networking parameters for the Switch Processor I/O card network interfaces to use when obtaining a software image from an external network server during the system boot process.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
boot networkconfig { dhcp | { dhcp-static-fallback | static } ip address spio24
  ip_address [ spio25 ip_address ] netmask ip_mask [ gateway gw_address ] } }
```

no boot networkconfig

no

Removes the network configuration information from the boot.sys file.

```
dhcp
```

Indicates that a Dynamic Host Control Protocol (DHCP) server is used for communicating with the external network server.

```
dhcp-static-fallback | static
```

- **dhcp-static-fallback**: provides static IP address fallback network option when a DHCP server is unavailable.
- **static**: specifies a fixed network IP address for the external network server that hosts the software image.

```
spio24 ip_address [ spio25 ip_address ] netmask ip_mask [ gateway gw_address ]
```

```
spio24 ip_address [ spio25 ip_address ]: the IP address to use for the SPIO in slot 24 and optionally the SPIO in slot 25 for network booting. ip_address must be specified using IPv4 dotted-decimal notation.
netmask ip_mask: the network mask to use in conjunction with the IP address(es) specified for network booting. ip_mask must be specified using IPv4 dotted-decimal notation.
gateway gw_address: the IP address of a network gateway to use in conjunction with the IP address(es) specified for network booting. gw_address must be entered using IPv4 dotted-decimal notation.

**Important:** If gw_address is not specified, the network server must be on the same LAN as the system. Since both SPIOS must be in the same network, the netmask and gateway settings are shared.
Global Configuration Mode Commands (A-K)

boot networkconfig

Usage
Configure the network parameters for the ports on the SPIO cards to use to communicate with an external network server that hosts software images.

**Important:** The settings for this command are stored immediately in the boot.sys file. No changes are made to the system configuration file.

**Important:** When configuring static addresses both SPIOs must have different IP addresses. Neither address can be the same as the local context IP address.

Example
The following configures the system to communicate with the external network server via DHCP with a fallback to IP address 192.168.100.10, respectively.

```
boot networkconfig dhcp-static-fallback ip address spio24 192.168.100.10 netmask 255.255.255.0
```

The following command configures the system to communicate with an external network server using the fixed (static) IP address 192.168.100.10 with a network mask of 255.255.255.0.

```
boot networkconfig static ip address spio24 192.168.100.10 netmask 255.255.255.0
```

The following restores the system default for the network boot configuration options.

```
no boot networkconfig
```
boot system priority

Specifies the priority of a boot stack entry to use when the system first initializes or restarts. Up to 10 boot system priorities (entries in the boot.sys file located in the /flash device in the SPC, SMC or MIO) can be configured.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

boot system priority number image  image_url  config  config_path

no boot system priority number

---

no

Remove a boot stack entry at the priority specified from the boot stack when it is no longer used.

priority number

Specifies the priority for the file group (consisting of an image (.bin) and its corresponding configuration (.cfg) file) specified in the boot stack. The value must be in the range from 1 through 100 where a priority of 1 is the highest. Up to 10 boot system priorities (boot stack entries) can be configured.

**Important:** When performing a software upgrade it is important that the new file group have the highest priority (lowest value) configured.

**Important:** To ensure that higher priority numbers remain open, use an “N-1” priority numbering methodology, where “N” is the first priority in the current boot stack.

image image_url

Specifies the location of an image file to use for system startup. The URL may refer to a local or a remote file. The URL must be formatted according to the following format:

For the ASR 5000:

- `[ file: ]{ /flash | /pcmcia1 | /hd }[/directory]/filename
- `[ http: | tftp: ]://host[:port][ /directory ]/filename

For the ASR 5500:

- `[ file: ]{ /flash | /usb1 | /hd }[/directory ]/filename
Global Configuration Mode Commands (A-K)

- `boot system priority`  
  
  ![Important:](Important:
  Use of the SMC hard drive is not supported in this release.

- ![Important:](Important:
  Do not use the following characters when entering a string for the field names below: “/” (forward slash), “:” (colon) or “@” (at sign).

  
  directory is the directory name.
  
  filename is the actual file of interest.
  
  host is the IP address or host name of the server.
  
  port# is the logical port number that the communication protocol is to use.

- ![Important:](Important:
  A file intended for use on an ASR 5000 uses the convention xxxxx.asr5000.bin, where xxxxx is the software build number.

- ![Important:](Important:
  A file intended for use on an ASR 5500 uses the convention xxxxx.asr5500.bin, where xxxxx is the software build number.

- ![Important:](Important:
  When using the TFTP, it is advisable to use a server that supports large blocks, per RFC 2348. This can be implemented by using the “block size option” to ensure that the TFTP service does not restrict the file size of the transfer to 32MB.

- `config config_path`
  
  Specifies the location of a configuration file to use for system startup. This must be formatted according to the following format:
  
  For the ASR 5000:
  
  ```
  *{ file: }{ /flash | /pcmcia1 | /hd }{ /path }/filename
  ```
  
  For the ASR 5500:
  
  ```
  *{ file: }{ /flash | /usb1 | /hd }{ /path }/filename
  ```

- ![Important:](Important:
  Use of the SMC hard drive is not supported in this release.

  Where path is the directory structure to the file of interest, and filename is the name of the configuration file. This file typically has a .cfg extension.

Usage

This command is useful in prioritizing boot stack entries in the boot.sys file, typically located on the /flash device of the Active SPC, SMC, or MIO, for automatic recovery in case of a failure of a primary boot file group.
**Important**: The configuration file must reside on the SPC’s, SMC’s, or MIO’s local filesystem, stored on one of its local devices (/flash, or /pcmcia1, or /hd-raid/pcmcia1, or /pcmcia2, or /usb1, or /hd-raid). Attempts to load the configuration file from an external network server will result in a failure to load that image and configuration file group, causing the system to load the image and configuration file group with the next highest priority in the boot stack.

**Important**: Configuration changes do not take effect until the system is reloaded.

**Important**: The settings for this command are stored immediately in the boot.sys file. No changes are made to the system configuration file.

**Example**

The following commands set up two locations to obtain a boot file group from.

```
boot system priority 1 image tftp: //remoteABC/pub/2012jan.bin config /flash/pub/data/2012feb.cfg
boot system priority 2 image /flash /pub/data/2002jun.bin config /pcmcia1/pub/data/2012feb.cfg
```

The following removes the current priority 1 boot entry from the boot.sys file.

```
no boot system priority 1
```
bulkstats

Enables the collection of bulk statistics and/or enters the bulk statistic configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration

configure
Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

bulkstats { collection | historical | mode }

no bulkstats collection

---

collection
Enables the statistics collection process. Collects a periodic snapshot of activity and performance data.

historical collection
Enables the collection of historical bulk statistics.
If enabled, StarOS keeps track of activities that require the storing of more data, such as “the highest value that’s been seen over the last 24 hours”.

mode
Enters the bulk statistics configuration mode. The resulting command-line prompt will look similar to:

[<context-name>]asr5000(config-bulkstats)#

no
Disables the collection of bulk statistics.

Usage

The Bulk Statistics Configuration mode consists of commands for configuring bulk statistic properties, such as the periodicity of collection. Detailed command descriptions appear in the Bulk Statistics Configuration Mode Commands chapter.
The collected bulk statistics are sent to a collection server (called a receiver). Bulk statistics are statistics that are collected in a group or schema, for example, system statistics, port statistics, RADIUS statistics.
Once the receiver, schema, and collection properties are configured, this bulkstats command enables or disables the collection of the data.
To collect a sample that will provide an average, for example, an average of CPU counters, the “historical” features must be enabled with the bulkstats historical collection command.
Since bulk statistics are collected at regular, user-defined intervals, the `bulkstats force` command in the Exec Mode can be used to manually initiate the immediate collection of statistics.

**Example**

```plaintext
bulkstats collection
bulkstats mode
no bulkstats collection
```
ca-certificate

Configures and selects an X.509 CA certificate to enable a security gateway or SCM to perform certificate-based peer (client) authentication. The system supports a maximum of 16 certificates and 16 CA root certificates. A maximum of four CA root certificates can be bound to a crypto or ssl template.

Product
All IPSec-related products

Privilege
Administrator, Security Administrator, Operator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

ca-certificate name name { der url url | pem { data pemdata | url url [ cert-enc ] [ cert-hash-url url url ] } }

no ca-certificate name name

no

Disables ca-certificate.

name name

Names the CA certificate. name must be an alphanumeric string of 1 through 128 characters.

der url

Specifies that the der format is to be used.
url is the url of the file containing certificate in der format. url must be an existing URL expressed in one of the following formats:

- [file://]{/flash | /pcmcia | /hd-raid}[/directory]/<filename
- tftp://<host>[:<port>]///<directory>]/<filename
- ftp://[<username>[:<password>][:<password>][:<password>]@]<host>[:<port>]///<directory>]/<filename
- sftp://[<username>[:<password>][:<password>][:<password>]@]<host>[:<port>]///<directory>]/<filename
- http://[<username>[:<password>][:<password>][:<password>]@]<host>[:<port>]///<directory>]/<filename

pem

Specifies that the Privacy-enhanced Electronic Mail (PEM) format is to be used.

data pemdata

CA certificate data in PEM format. pemdata must be an alphanumeric string of 1 through 4095 characters.
url url

URL of the file containing CA certificate in PEM. url must be an existing URL expressed in one of the following formats:
- \[[file:\]/\{flash | /pcmcia | /hd-raid\}/\{directory\}/\{filename\}\]
- \[tftp://\{host\}/\{port\}/\{directory\}/\{filename\}\]
- \[ftp://\{username\}:\{password\}@\{host\}/\{port\}/\{directory\}/\{filename\}\]
- \[sftp://\{username\}:\{password\}@\{host\}/\{port\}/\{directory\}/\{filename\}\]
- \[http://\{username\}:\{password\}@\{host\}/\{port\}/\{directory\}/\{filename\}\]

When read via a file, note that show configuration will not contain the URL reference, but will instead output the data via data pemdata, such that the configuration file is self-contained.

[ cert-enc ] [ cert-hash-url url url

cert-enc: Certificate encoding type other than default encoding type.

no

Removes the named CA certificate.

Usage

Use this command to configure and select an X.509 CA certificate to enable a security gateway or SCM to perform certificate-based peer (client) authentication.

Example

Use the following command to remove a certificate named fap1:

    no ca-certificate data fap1
**ca-crl**

Configures the name and URL path of a Certificate Authority-Certificate Revocation List (CA-CRL).

**Product**
All IPSec-related products

**Privilege**
Operator

**Mode**
Exec > Global Configuration

```configure```
Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
ca-crl name name { der | pem } { url url }
no ca-crl name name
```

**no**
Removes the named CA-CRL.

**name**
Provides a name of the CA-CRL. `name` must be an alphanumeric string of 1 through 128 characters.

**der**
Specifies that Distinguished Encoding Rules (DER) format is to be used for the source format.

**pem**
Specifies that Privacy-enhanced Electronic Mail (PEM) format is to be used for the source format.

**url url**
Specifies the URL where the CA-CRL is to be fetched. `url` must be an existing URL expressed as an alphanumeric string of 1 through 1023 characters in one of the following formats:

- `[file://]{/flash | /pcmcia1 | /hd-raid}/directory/filename`
- `tftp://<host>[:<port>]/{directory}/filename`
- `ftp://[<username>[:<password>@]<host>[:<port>]/{directory}/filename`
- `sftp://[<username>[:<password>@]<host>[:<port>]/{directory}/filename`
- `http://[<username>[:<password>@]<host>[:<port>]/{directory}/filename`
- `ldap://<host>[:<port>]/{dn}/[?<attributes>][?<scope>][?<filter>][?<extensions>]`
Usage

Use this command to name and fetch a CA-CRL from a specified location. Without additional information from the CA, an issued certificate remains valid to any verifier until it expires. To revoke certificates, the CA publishes a CRL periodically to provide an updated list of certificates revoked, but not yet expired. Like a certificate, a CRL is a digital document signed by the CA. In addition to a list of serial numbers of revoked certificates, the CRL includes attributes such as issuer name (same as the issuer name in the certificate), signature (signed by the issuer using the same key that signs certificates), last update (the time this CRL was issued), and next update (the time next CRL will be available).

Example

The following command fetches a CA-CRL named list1.pem from a host.com/CRLs location and names the list CRL5:

```
ca-crl name CRL5 pem url http://host.com/CRLs/list1.pem
```
call-control-profile

Creates an instance of a call-control profile.

Product
MME
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

[ no ] call-control-profile cc_profile_name

---

no

Deletes the Call-Control Profile instance from the configuration.

---

cc_profile_name

Specifies the name of the call-control profile. Enter an alphanumeric string of 1 through 64 characters.

Usage

Use this command to create an instance of a call-control profile and to enter the call-control profile configuration mode. A call-control profile is a template which groups a set of call-handling instructions that may be applicable to one or more incoming calls. See the Call-Control Profile Configuration Mode Commands chapter for information regarding the definition of the rules contained within the profile and the use of the profile.

**Important:** A call-control profile is a key element of the Operator Policy feature and is only valid when associated with at least one operator policy.

To see what call-control profiles have already been created, return to the Exec mode and enter the show call-control-profile all command.

Example

The following command creates a configuration instance of an call-control profile:

```plaintext
call-control-profile ccprof1
```
card

Enters the Card Configuration mode for the specified card. (ASR 5x00 only)

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

**Syntax**
```
card slot_number
```

Specifies the slot number of the card for which the card configuration mode is to be entered. *slot_number* must be an integer from 1 through 48 (on the ASR 5000) or 1 through 20 (on the ASR 5500).

**Usage**
Enter the configuration mode for a specific card when changes are required.

**Example**
```
card 8
```
**card-standby-priority**

Configures the redundancy priorities for packet processing cards by specifying the slot number search order for a standby card when needed.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

`configure`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
card-standby-priority slot_num [ slot_num ] [ slot_num ] ... 
```

`slot_num`

Specifies the slot of the card for the order of the standby cards. `slot_num` must be in the range from 1 through 16 excluding slots 8 and 9 (on the ASR 5000) or 1 through 10 excluding slots 5 and 6 (on the ASR 5500). `slot_num` may be repeated as many times as necessary to indicate the complete search order.

**Usage**
Set the standby order of the redundant cards when multiple standby cards are available. Questionable hardware should be placed lower in the priority list.

**Important:** This command replaces the `paci-standby-priority` command.

**Important:** This command is not supported on all platforms.

**Example**

The following command configures the redundancy priority to use the standby cards in slots 16, 14, and 12 in that order:

```
card-standby-priority 16 14 12 
```

The following command configures the redundancy priority to use the standby cards in slots 10, 9, and 7 in that order:

```
card-standby-priority 10 9 7 
```
**cdr-multi-mode**

This command enables multiple instances of CDRMOD, one per packet processing card.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

`configure`
Entering the above command sequence results in the following prompt:

```
[local] host_name(config) #
```

**Syntax**

```
[ default ] cdr-multi-mode
```

<table>
<thead>
<tr>
<th><strong>default</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Configures this command with its default setting.</td>
</tr>
<tr>
<td>Default: Single-CDRMOD mode</td>
</tr>
</tbody>
</table>

**Usage**

Use this command to enable the multi-CDRMOD mode, wherein there will be one instance of CDRMOD per packet processing card. All the SessMgr instances that are running on a packet processing card will send the records to the CDRMOD instance running on that card.

By default, CDRMOD runs in single mode, wherein there will be only one instance of CDRMOD running for the entire chassis. All the SessMgr instances that are running on a packet processing card will send the records to the CDRMOD instance.

**Important:** For changes to this command to take effect, save the configuration and reboot the system.

**Important:** In multi-CDRMOD mode, you should enable hard-disk usage.
**certificate**

Configures and selects an X.509 Trusted Author certificate.

**Product**
All IPSec-related products

**Privilege**
Administrator, Security Administrator, Operator

**Mode**
Exec > Global Configuration

```configure```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```certificate name name { der url url | pem { data pemdata | url url } private-key pem { [ encrypted ] data pemdata | url url [cert-enc] [cert-hash-url url url] } } no certificate name name no```

**name name**
Names the certificate. `name` must be from 1 to 128 alphanumeric characters.

**der url**
Specifies that the der format is to be used.

`url` is the url of the file containing certificate in der format. `url` must be an existing URL expressed in one of the following formats:

- `[file:///flash | /pmmc1 | /hd-raid] [/directory] </filename`
- `tftp://<host>[:<port>]/<directory>/</filename`
- `ftp://[<username>[:<password>]@]<host>[:<port>]/<directory>/</filename`
- `sftp://[<username>[:<password>]@]<host>[:<port>]/<directory>/</filename`
- `http://[<username>[:<password>]@]<host>[:<port>]/<directory>/</filename`

**pem**
Specifies that the Privacy-enhanced Electronic Mail (PEM) format is to be used.

**data pemdata**
Certificate/private key data in PEM format. `pemdata` must be an alphanumeric string of 1 through 4095 (if private key is not implemented) or 1 through 8191 (if private key is implemented) characters.
url url

URL of the file containing certificate/private key in PEM. url must be an existing URL expressed in one of the following formats:
- `[file://]{/flash | /pcmcia | /hd-raid}[/directory]/<filename
- `tftp://<host>[::<port>]/<directory>/<filename
- `ftp://[<username>[:<password>]<host>[::<port>]/<directory>/<filename
- `sftp://[<username>[:<password>]<host>[::<port>]/<directory>/<filename
- `http://[<username>[:<password>]<host>[::<port>]/<directory>/<filename

When read via a file, `show configuration` will not contain the URL reference, but instead outputs the data via `data pemdata`, such that the configuration file is self-contained.

[ cert-enc ] [ cert-hash-url url url]

cert-enc: Certificate encoding type other than default encoding type.

private-key

Private key data.

encrypted

Encrypted private key data.

no

Removes the named certificate.

Usage

Use this command to Configures and selects an X.509 Trusted Author certificate.

Example

Use the following command to remove a certificate named box1:

    no certificate data box1
cli

Configures global Command Line Interface (CLI) parameters.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

cli { access { monitor-protocol | monitor-subscriber | show-configuration } { administrator | operator } } | configuration-monitor | hidden | login-failure-delay number | max-sessions number | operator clear-subscriber-one-only | test-commands [encrypted] password password | trap config-mode }

no cli { configuration-monitor | hidden | login-failure-delay number | max-sessions | operator clear-subscriber-one-only | trap config-mode }

default cli { access { monitor-protocol | monitor-subscriber | show-configuration } | configuration-monitor | login-failure-delay | max-sessions | operator clear-subscriber-one-only | trap config-mode }

no

Removes the specified option.

default

Resets the keywords to their default values.

access { monitor-protocol | monitor-subscriber | show-configuration } { operator | administrator }

Sets access privileges on the monitor protocol and monitor subscriber commands:

monitor-protocol: Selects privileges for the monitor protocol command.
monitor-subscriber: Selects privileges for the monitor subscriber command.
show-configuration: Selects privileges for the show-configuration command. However the default access level for this command is the user with operator privileges.
operator: Sets the privileges for the selected command to allow use by users with operator privileges.
administrator: Restricts use of the selected command to administrators only.

configuration-monitor

When this keyword is enabled, the system executes a show configuration checksum command every 15-minutes. The resulting checksum is compared with the previous checksum.
When a configuration change is detected, a log message and SNMP notification are generated. The SNMP notification only indicates that a change has occurred without identifying what change had been made. The 15-minute interval is fixed and cannot be configured. By default configuration monitoring is disabled.

`hidden`

Enables access to the hidden `cli test-commands` command. The `no cli hidden` command disables access to the `cli test-commands` command. This is the default mode. Refer to the description of the `test-commands` keyword below for additional information.

`login-failure-delay number`

Specifies the time to wait before a login failure is returned and another login may be attempted. Default is five seconds.

`max-sessions number`

Sets the number of allowed simultaneous CLI sessions on the system. If this value is set to a number below the current number of open CLI sessions, the open sessions will continue until closed. `number` must be an integer from 2 through 100.

⚠️ **Caution:** Use caution when setting this command. Limiting simultaneous CLI sessions prevents authorized users from accessing the system if the maximum number allowed has been reached. The system already limits CLI sessions based on available resources. Additional limitation could have adverse effects.

`operator clear-subscriber-one-only`

RestRICTs Operator to clearing only one subscriber session at a time.

`test-commands [encrypted] password password_string`

Enables access to the cli test-commands mode. The commands and keywords made available under this mode are for internal testing and debugging.

⚠️ **Caution:** CLI test-commands are intended for diagnostic use only. Access to these commands is not required during normal system operation. These command are intended for use only by Cisco TAC personnel. Some of these commands can slow system performance, drop subscribers, and/or render the system inoperable.

ℹ️ **Important:** An SNMP trap is generated when a user enables `cli test-commands (starTestModeEntered)`. Refer to the `SNMP MIB Reference` for additional information.

`encrypted`: Specifies that the system will save the password in an encrypted format in the configuration file. The system displays the encrypted keyword in the configuration file as a flag indicating that the variable following the `password` keyword is the encrypted version of the plain text password. Only the encrypted password is saved as part of the configuration file.

`password password_string`: Prompts for the password required to access `cli test-commands`. This password must have been previously configured by a Security Administrator via the `tech-support test-commands password` command. The password is an alphanumeric string of 1 through 64 characters (plain text password) or 1 through 524 characters (encrypted password).

If the `password` keyword is not entered, the user is prompted (no-echo) to enter the password. If `tech-support test-commands password` has not been enabled, you will be unable to execute `cli test-commands`. 

---

Cisco ASR 5x00 Command Line Interface Reference
Once this test mode is entered under Global Configuration mode, `cli test-commands` become part of the current configuration. Therefore, any generated configuration will contain the `cli test-commands` command as the first configuration command.

⚠️ **Caution:** Use of CLI test-commands may cause significant service interruption. Contact Cisco TAC before executing any commands while in this mode.

The `no cli test-commands` command disables access to the CLI test-commands mode.

```
trap config-mode
```

Enables sending an SNMP trap (`starCLIConfigMode`) when a CLI user enters the configuration mode.

**Usage**

This command sets access parameters and enables several operational parameters for the system’s command line interface.

**Example**

The following command sets the number of allowed simultaneous CLI sessions to 5.

```
cli max-sessions 5
```

The following command sets the command `monitor protocol` to administrator-only

```
cli access monitor-protocol administrator
```
cli-encrypt-algorithm

Specifies the type of encryption algorithm to be used for passwords and secrets.

Product
All

Privilege
Security Administrator

Mode
Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

cli-encrypt-algorithm { A | B }

default cli-encrypt-algorithm

default

Resets the encryption algorithm to “A”.

{ A | B }

Specifies the type of encryption algorithm:

• A – MD5-based cipher (default)
• B – AES-CBC-128 for encryption and HMAC-SHA1 for authentication

Usage

Specify MD5-based cipher (“A”) or AES-CBC-128 for encryption and HMAC-SHA1 for authentication (“B”) when encrypting passwords and secrets.

Example

cli-encrypt-algorithm B
clock

Configures system clock timezone and what local time zone to use.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

clock timezone tz [ local ]

no clock timezone

no

Resets the system timezone to the system default UTC.

tz

Specifies the system time zone to use as one of:
•america-buenos-aires (GMT-3:00; Buenos Aires)
•america-caracas (GMT-4:00) Caracas
•america-guatemala (GMT-6:00; Guatemala, Guatemala)
•america-la_paz (GMT-4:00; La Paz)
•america-lima (GMT-5:00; Lima, Peru)
•america-puerto-rico (GMT-4:00; Puerto Rico)
•america-sao-paulo (GMT -3:00; Brazil)
•america-tijuana (GMT-8:00; Tijuana)
•asia-almaty (GMT+6.00; Almaty, Kazakhstan)
•asia-baghdad (GMT+3:00; Baghdad, Russia Zone 2, Kuwait, Nairobi, Riyadh, Moscow, Tehran)
•asia-bangkok (GMT+7:00; Bangkok)
•asia-calcutta (GMT+5:30; Calcutta, Mumbai, New Delhi)
•asia-dhaka (GMT+6:00; Dhaka)
•asia-hong-kong (GMT+8:00; Hong_Kong)
•asia-irkutsk (GMT+9:30; Irkutsk)
•asia-kabul (GMT+4:30; Kabul)
• asia-karachi (GMT+5:00; Karachi)
• asia-katmandu (GMT+5:45; Kathmandu)
• asia-magadan (GMT+11:00; Magadan)
• asia-muscat (GMT+4:00; Abu Dhabi, UAE, Muscat, Tblisi, Volgograd, Kabul)
• asia-rangoon (GMT+6:30; Rangoon)
• asia-seoul (GMT+9:00) Seoul
• asia-tehran (GMT+3:30; Tehran)
• asia-tokyo (GMT+9:00; Tokyo, Russia Zone 8)
• atlantic-azores (GMT-2:00; Azores)
• atlantic-cape-verde (GMT-1:00; Cape Verde Islands)
• australia-perth (GMT+8:00) Perth
• australia-darwin (GMT+9:30) Northern Territory - Alice Springs, Darwin, Uluru
• australia-adelaide (GMT+9:30) Southern Territory - Adelaide
• australia-melbourne (GMT+10:00) Victoria - Ballarat, Melbourne
• australia-sydney (GMT+10:00) New South Wales - Newcastle, Sydney, Wollongong
• australia-hobart (GMT+10:00) Tasmania - Hobart, Launceston
• australia-brisbane (GMT+10:00) Queensland - Brisbane, Cairns, Toowoomba, Townsville
• australia-lordhowe (GMT+10:30) Lord Howe Island
• canada-newfoundland (GMT-3:30; Newfoundland)
• canada-saskatchewan (GMT-6:00; Saskatchewan)
• europe-central (GMT+1:00; Paris, Berlin, Amsterdam, Brussels, Vienna, Madrid, Rome, Bern, Stockholm, Oslo)
• europe-dublin (GMT+0:00) Dublin, Ireland
• europe-eastern (GMT+2:00; Russia Zone 1, Athens, Helsinki, Istanbul, Jerusalem, Harare)
• newzealand-auckland (GMT +12:00; Auckland, Wellington)
• newzealand-chatham (GMT +12:45; Chatham)
• nuku (GMT-13:00; Nuku' alofa)
• pacific-fiji (GMT+12:00; Wellington, Fiji, Marshall Islands)
• pacific-guam (GMT+10:00; Brisbane, Cairns, Sydney, Guam)
• pacific-kwajalein (GMT-12:00; Kwajalein)
• pacific-norfolk - (GMT+11:30) Norfolk Island
• pacific-samoa (GMT-11:00; Samoa)
• us-alaska (GMT-9:00; Alaska)
• us-arizona (GMT-7:00; Arizona)
• us-central (GMT-6:00; Chicago, Mexico City, Saint Louis)
• us-eastern (GMT-5:00; Bogota, Lima, New York City)
• us-hawaii (GMT-10:00; Hawaii)
Global Configuration Mode Commands (A-K)

Clock

- `us-indiana` (GMT-6:00; Indiana)
- `us-mountain` (GMT-7:00; Cheyenne, Denver, Las Vegas)
- `us-pacific` (GMT-8:00) San Francisco, LA, Seattle
- `utc` (GMT; Universal Time Coordinated: London, Dublin, Edinburgh, Lisbon, Reykjavik, Casablanca)

`local`

Indicates the timezone specified by `tz` is to be considered the local time zone for local time display and conversion.

Usage

Clock and timezone management is necessary for proper accounting records. The chassis may be set to display a different local time than that of the system clock which allows accounting records to use the system time but to display the proper local time for users.

Example

```plaintext
  clock timezone utc
  clock timezone us-indiana local
  no clock timezone
```
**cmp auto-fetch**

Use this command to add a fetch configuration for each certificate for which automatic update is required. This is a Certificate Management Protocol v2 command.

**Product**

All products supporting IPSec CMPv2 features

**Important:** This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

**Privilege**

Security Administrator

**Mode**

Exec > Global Configuration

`configure`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
cmp auto-fetch current-name cert_name ca-root ca_name time days
no auto-fetch current-name cert_name
```

**Usage**

Use this command to specify when a current certificate should be automatically fetched.

**Example**

The following command automatically fetches the current certificate 10 days before it is to expire:

```
cmp fetch current-name aqw12345 ca-root ca001 time 10
```
cmp cert-store location

Use this command to add a file location on /flash disk where the certificates and private keys will be stored. This is a Certificate Management Protocol v2 command.

Product
All products supporting IPSec CMPv2 features

Important: This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

Privilege
Security Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

cmp cert-store location pathname [key reuse]
default cmp cert-store
no cmp cert-store

location pathname

Removes the certificate storage location configuration.

Specifies the storage location of the certificates and key files in the following formats:

• [file://]/{ /flash | /usb1 | /hd-raid }[/<directory>]/<filename>
• tftp://<host>[:<port>]/[/<directory>]/<filename>
• ftp://[<username>[:<password>]<@<host>[:<port>]/[/<directory>]/<filename>
• sftp://[<username>[:<password>]<@<host>[:<port>]/[/<directory>]/<filename>
• http://[<username>[:<password>]<@<host>[:<port>]/[/<directory>]/<filename>

Usage
Use this command to specify where certificates and key files should be stored.

Example
The following command stores certificates and key files in a location different from the default location:

cmp cert-store location file://certificates
cmp cert-trap time

Defines when an SNMP MIB certificate expiry trap should be sent as the number of hours before expiration.

**Product**
All products supporting IPSec CMPv2 features

---

**Important:** This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

**Privilege**
Security Administrator

**Mode**
Exec > Global Configuration

**configure**
Entering the above command sequence results in the following prompt:

[local] host_name(config) #

**Syntax**

```
cmp cert-trap time hours

no cmp cert-trap time
```

```
no

Removes the certificate expiry MIB trap notification.

time hours

Specifies the number of hours before certificate expiry when a MIB trap should be sent. `hours` is an integer from 1 through 1024.
```

**Usage**
Use this command to set when an SNMP MIB certificate expiry trap should be sent.

**Example**
The following command specifies that an SNMP MIB certificate expiry trap should be sent 48 hours prior to expiration:

```
cmp cert-trap time 48
```
commandguard

When enabled this command causes the `configure` and `autoconfirm` CLI commands to prompt for confirmation (Y/N). When `commandguard` is disabled, these commands will not prompt for confirmation. If `autoconfirm` is enabled, `commandguard` has no affect.

**Product**
All products

**Privilege**
Security Administrator, Administrator, Operator

**Mode**
Exec > Global Configuration

`configure`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
[ no ] commandguard
```

**Usage**

Use this command to prevent users from accidentally entering Configuration mode via the CLI or file replay (most commonly caused by a cut and paste error in the configuration file). By default this command is disabled. The status of `commandguard` is output in `show configuration` commands.

**Example**

The following command enables confirmation prompting for `configure` and `autoconfirm` CLI commands:

```
commandguard
```
congestion-control

This command enables and disables the congestion control functionality on the system.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

```
configure
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
[ default | no ] congestion-control
```

- **default**
  Sets the congestion control to its default value.

- **no**
  Disables the congestion control functionality from the system. It is actually the default behavior.

**Usage**

Congestion control on the system is used to monitor the system for conditions that could potentially degrade performance when the system is under heavy load. Typically, these conditions are temporary (i.e. high CPU or memory utilization) and are quickly resolved. However, continuous or large numbers of these conditions within a specific time interval may impact the system’s ability to service subscriber sessions. The purpose of congestion control is to aid in the identification of such conditions and invoke policies for addressing the situation.

Congestion control operation is based on the configuration of the following:

- **Call disconnections on overload**: With this functionality, the system enables and disables the policy for disconnecting passive calls (chassis-wide) during an overload situation. It also configures and fine-tunes the overload-disconnect congestion control policy for an entire chassis.

- **Congestion condition thresholds**: Thresholds dictate the conditions for which congestion control is to be enabled and establish limits for defining the state of the system (congested or clear). These thresholds function in a similar fashion to the operation thresholds that can be configured for the system (as described in later in this chapter). The primary difference is that when these thresholds are reached, not only is an SNMP trap generated (starCongestion), but a service congestion policy is invoked as well.

  A threshold tolerance is configured to dictate the percentage under the configured threshold that must be reached in order for the condition to be considered “cleared”. An SNMP trap (starCongestionClear) is then triggered.
- **Service congestion policies**: Congestion policies are configurable for each service (e.g., PDSN, GGSN, P-GW, SGSN, etc.). These policies dictate how services respond should the system detect that a congestion condition threshold has been crossed.

Since the congestion control functionality on the system is disabled by default, this command should be executed once congestion-control thresholds and policies have been configured. (Refer to the other congestion-control related commands for more information.)

**Example**

The following command enables the congestion control functionality on the system.

```
congestion-control
```
**congestion-control overload-disconnect**

This command enables and disables the policy for disconnecting passive calls (chassis-wide) during an overload situation. It also configures and fine-tunes the overload-disconnect congestion control policy for an entire chassis.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration
`configure`

Entering the above command sequence results in the following prompt:

```
[local] host_name(config) #
```

**Syntax**

```
congestion-control overload-disconnect [ iterations-per-stage integer | percent percentage_value | threshold { license-utilization percentage_value | max-sessions-per-service-utilization percentage_value | tolerance number } ]

default congestion-control overload-disconnect [ iterations-per-stage | percent | threshold { license-utilization | max-sessions-per-service-utilization | tolerance } ]

no congestion-control overload-disconnect
```

**default**

When “default” and one of the keywords is added to the command, the policy remains in its current state and the value for the specified keyword is reset to its default value.

When “default” and the command are entered without keywords, the overload-disconnect policy for congestion control is disabled.

**no**

Disables the overload-disconnect policy for congestion control.

**iterations-per-stage integer**

Specifies the number of calls to be disconnected during the defined number of seconds. `integer` is a value from 2 through 8. The default value is 8.

**percent percentage_value**

Specifies the percentage of calls to be disconnected, in stages, during an overload situation. `percentage_value` is an integer from 1 through 100. The default value is 5.
### threshold

**license-utilization**: Specifies the license-utilization percentage threshold for overload situations. If candidates are available, passive calls are disconnected when this threshold is exceeded. 

`percentage_value` is an integer from 1 through 100. The default value is 80.

**max-sessions-per-service-utilization**: Specifies a percentage of the maximum sessions per service. If candidates are available, passive calls are disconnected when this threshold is exceeded.

`percentage_value` is an integer from 1 through 100. The default value is 80.

**tolerance**: Specifies the percentage of calls the system disconnects below the values set for the other two thresholds. In either case, a Clear Traps message is sent after the number of calls goes below the corresponding threshold value. `number` is an integer from 1 through 25. The default value is 10.

### Usage

Use this command to set the policy for call disconnects when the chassis experiences call overload.

To verify the congestion-control configuration use `show congestion-control configuration` from the Exec mode.

To set overload-disconnect policies for individual subscribers, see `overload-disconnect` in Subscriber Configuration Mode Commands.

### Example

The following command sets an overload-disconnect policy for the chassis in which 5 calls would be disconnected very 5 seconds during an overload situation.

```
congestion-control overload-disconnect interactions-per-stage 5
```

Both of the following commands disable the overload-disconnect policy without changing the policy configuration.

```
default congestion-control overload-disconnect
```

or

```
no congestion-control overload-disconnect
```

To instruct the system to stop call disconnects when the number of calls goes down 85% of the total allowed calls for that service, enter both of the following commands to set the max-sessions-per-service-utilization value to 90% and the tolerance value to 5%:

```
congestion-control overload-disconnect threshold max-sessions-per-service-utilization 90
congestion-control overload-disconnect threshold tolerance 5
```
congestion-control policy

Configures congestion control policies.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

congestion-control policy { asngw-service | asnpc-service | cscf-service | fng-service | ggsn-service | ha-service | hnbgw-service | hsgw-service | ipsg-service | lma-service | lns-service | mipv6ha-service | pcc-af-service | pcc-policy-service | pdg-service | pdif-service | pdsn-service | pdsnclsdrp-service | pgw-service | phsgw-service | phspc-service | saegw-service | sgsn-service | sgw-service | wsg-service } action { drop | none | redirect | reject }

congestion-control policy epdg-service action { drop | none | reject }

congestion-control policy mme-service action { drop | none | reject | report-overload { permit-emergency-sessions | reject-new-sessions | reject-non-emergency-sessions } enodeb-percentage percentage }

congestion-control policy { critical mme-service action-profile action_profile_name | major mme-service action-profile action_profile_name | minor mme-service action-profile action_profile_name }

default congestion-control policy { asngw-service | asnpc-service | cscf-service | epdg-service | fng-service | ggsn-service | ha-service | hnbgw-service | hsgw-service | ipsg-service | lma-service | lns-service | mipv6ha-service | mme-service | pcc-af-service | pcc-policy-service | pdg-service | pdif-service | pdsn-service | pdsnclsdrp-service | pgw-service | phsgw-service | phspc-service | saegw-service | sgsn-service | sgw-service | wsg-service }

default
Specifies the Congestion Control policy action for the selected service to its default value.

asngw-service
Specifies the Congestion Control policy action for the ASN-GW service.

asnpc-service
Specifies the Congestion Control policy action for the ASN PC-LR service.
**critical**
For MME (starting with Release 14.0), this keyword associates the action-profile to be used for critical congestion thresholds for the MME service.

**cscf-service**
Specifies the Congestion Control policy action for the P-CSF/A-BG service. Supported policy actions are:
- **drop**: Specifies that the system should drop incoming packets containing new session requests.
- **none**: Specifies that the system should take no action.
- **redirect**: Specifies that the system should redirect new session requests to an alternate device.

**Important**: If this option is used, the IP address of the alternate device must be configured using the `policy overload redirect` command that is part of the CSCF policy rules configuration.

- **reject**: Specifies that the system processes new session request messages and responds with a reject message.

**epdg-service action**
Specifies the Congestion Control policy action for the ePDG service. Supported policy actions are:
- **drop**: Specifies that the system should drop incoming packets containing new session requests.
- **none**: Specifies that the system should take no action.
- **reject**: Specifies that the system processes new session request messages and responds with a reject message.

For ePDG type of session/calls, `redirect` action is not supported.

**fng-service**
Specifies the Congestion Control policy action for the FNG service.

**ggsn-service**
Specifies the Congestion Control policy action for the GGSN service.

**ha-service**
Specifies the Congestion Control policy action for the HA service.

**hnbgw-service**
Specifies the Congestion Control policy action for the HNB-GW service. Supported policy actions are:
- **drop**: Specifies that the system should drop incoming packets containing new session requests.
- **none**: Specifies that the system should take no action.
- **reject**: Specifies that the system processes new session request messages and responds with a reject message.
hsgw-service
Specifies the Congestion Control policy action for the HSGW service.
Supported policy actions are:
- drop: Specifies that the system should drop incoming packets containing new session requests.
- none: Specifies that the system should take no action.
- redirect: Specifies that the system should redirect new session requests to an alternate device.

**Important:** If this option is used, the IP address of the alternate device must be configured using the `policy overload redirect` command that is part of the HSGW service configuration.

- reject: Specifies that the system processes new session request messages and responds with a reject message.

ipsg-service
Specifies the Congestion Control Policy action for the IPSG service. The policy specifies how the IPSG service will respond when the system detects that a congestion condition threshold has been crossed.
Supported policy actions are:
- drop: Specifies that the system should drop incoming packets containing new session requests.
- none: Specifies that the system should take no action.

Default: none

lma-service
Specifies the Congestion Control policy action for the LMA service

lns-service
Specifies the Congestion Control policy action for the LNS service.

mipv6ha-service
Specifies the Congestion Control policy action for the MIPv6-HA service.

**major**
For MME (starting with Release 14.0), this keyword associates the action-profile to be used for major congestion thresholds for the MME service.

**minor**
For MME (starting with Release 14.0), this keyword associates the action-profile to be used for minor congestion thresholds for the MME service.

mme-service
Sets the congestion control policy for action to take when subscriber sessions exceeds the defined threshold limit.
For MME type of session/calls, `redirect` action is not supported.
Global Configuration Mode Commands (A-K)

**Important:** The `mme-service` keyword option is available only in releases prior to 14.0. In 14.0 and higher, you must first select either the critical, major or minor policy level first. Refer to the `congestion-action-profile` command in the LTE Policy Configuration mode to create action-profiles which in turn define the actions to be taken when thresholds are exceeded in Release 14.0 and higher for MME.

---

**pcc-af-service**

Specifies the Congestion Control policy action for the PCC Application Function (AF) service. Supported policy actions are:

- **drop:** Specifies that the system should drop incoming packets containing new session requests.
- **none:** Specifies that the system should take no action.
- **reject:** Specifies that the system processes new session request messages and responds with a reject message.

**pcc-policy-service**

Specifies the Congestion Control policy action for the PCC Policy service. Supported policy actions are:

- **drop:** Specifies that the system should drop incoming packets containing new session requests.
- **none:** Specifies that the system should take no action.
- **reject:** Specifies that the system processes new session request messages and responds with a reject message.

**pdg-service**

Specifies the Congestion Control policy action for the PDG service.

**pdif-service**

Specifies the Congestion Control policy action for the PDIF service.

**pdsn-service**

Specifies the Congestion Control policy action for the PDSN service.

**pgw-service**

Specifies the Congestion Control policy action for the P-GW service. Supported policy actions are:

- **drop:** Specifies that the system should drop incoming packets containing new session requests.
- **none:** Specifies that the system should take no action.
- **reject:** Specifies that the system processes new session request messages and responds with a reject message.

For P-GW sessions/calls, **redirect** action is not supported.

**saegw-service**

Specifies the Congestion Control policy action for the SAEGW service. Supported policy actions are:

- **drop:** Specifies that the system should drop incoming packets containing new session requests.
- **none:** Specifies that the system should take no action.
• **reject**: Specifies that the system processes new session request messages and responds with a reject message.

For SAEGW sessions/calls, **redirect** action is not supported.

---

**sgsn-service**

Specifies the Congestion Control policy - the congestion response actions for the SGSN service. Prior to Release 17.0, the supported policy actions in this command are:

- **drop**: Specifies that the system should drop incoming packets containing new session requests.
- **none**: Specifies that the system should take no action.
- **reject**: Specifies that the system processes new session request messages and responds with a reject message.

---

**sgw-service**

Specifies the Congestion Control policy action for the S-GW service. Supported policy actions are:

- **drop**: Specifies that the system should drop incoming packets containing new session requests.
- **none**: Specifies that the system should take no action.
- **reject**: Specifies that the system processes new session request messages and responds with a reject message.

For S-GW sessions/calls, **redirect** action is not supported.

---

**wsg-service**

Specifies the Congestion Control policy action for the WSG service. Supported policy actions are:

- **drop**: Specifies that the system should drop incoming packets containing new session requests.
- **none**: Specifies that the system should take no action.
- **reject**: Specifies that the system processes new session request messages and responds with a reject message.

---

**action { drop | none | redirect | reject }**

Specifies the policy action:

- **drop**: Specifies that the system should drop incoming packets containing new session requests.
- **none**: Specifies that the system should take no action. This is the default for PDIF-service.
- **redirect**: Specifies that the system should redirect new session requests to an alternate device.
  
  (CSCF, HA, HSGW, and PDSN only)

---

**Important**: If this option is used, the IP address of the alternate device must be configured using the **policy overload redirect** command that is part of the service configuration. Note that this option can not be used in conjunction with GGSN, MME, P-GW, SAEGW, or S-GW services.

- **reject**: Specifies that the system processes new session request messages and responds with a reject message.
Global Configuration Mode Commands (A-K)

congestion-control policy

(For PDSN and HA, the reply code is 130, “insufficient resources”. For the GGSN, the reply code is 199, “no resources available”.)

\[
\text{report-overload \{ permit-emergency-sessions | reject-new-sessions | reject-non-emergency-sessions \} enodeb-percentage percentage}
\]

**Important:** This set of keywords is supported only by the MME.

Enables the MME to report overload conditions to eNodeBs and take additional action to alleviate congestion situations.

- **permit-emergency-sessions**: Specifies that only emergency sessions are allowed to access the MME during the overload period.
- **reject-new-sessions**: Specifies that all new sessions destined for the MME will be rejected during the overload period.
- **reject-non-emergency-sessions**: Specifies that all non-emergency sessions will be rejected during the overload period.
- **enodeb-percentage percentage**: Configures the percentage of known eNodeBs that will receive the overload report. `percentage` must be an integer from 1 to 100.

**Usage**

Congestion policies can be configured for each service. When congestion control functionality is enabled, these policies dictate how services respond should the system detect that a congestion condition threshold has been crossed.

**Example**

The following command configures a congestion control policy of reject for PDSN services:

```
congestion-control policy psdn-service action reject
```

The following command configures a congestion control policy of reject for MME services:

```
congestion-control policy mme-service action reject
```
congestion-control threshold

Configures the congestion control threshold values that are to be monitored.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

**Syntax**

```plaintext
congestion-control threshold { license-utilization percent | max-sessions-per-service-utilization percent | message-queue-utilization percent | message-queue-wait-time time | port-rx-utilization percent | port-specific { slot/port | all } [ tx-utilization percent ] [ rx-utilization percent ] port-specific-rx-utilization critical | port-specific-tx-utilization critical | port-tx-utilization percent | service-control-cpu-utilization percent | system-cpu-utilization percent | system-memory-utilization percent | tolerance percent }


no congestion-control threshold port-specific { slot/port | all }

no congestion-control threshold port-specific { slot/port | all } [ rx-utilization percent ] [ tx-utilization percent ]

no congestion-control threshold port-specific-rx-utilization critical

no congestion-control threshold port-specific-tx-utilization critical

no congestion-control threshold { message-queue-utilization | message-queue-wait-time | port-rx-utilization percent | port-tx-utilization percent | service-control-cpu-utilization | system-cpu-utilization | system-memory-utilization }

default congestion-control threshold keyword
Sets the threshold keyword to its default value.

no congestion-control threshold port-specific { slot/port | all } This command disables port specific threshold monitoring on the specified port or on all ports. slot/port: Specifies the port for which port specific threshold monitoring is being configured. The slot and port must refer to an installed card and port.
all: Set port specific threshold monitoring for all ports on all cards.

```
no congestion-control threshold port-specific-rx-utilization critical
```
This command disables specific receive port utilization.

```
no congestion-control threshold port-specific-tx-utilization critical
```
This command disables specific transmit port utilization.

```
license-utilization percent
```
Default: 100
The percent utilization of licensed session capacity as measured in 10 second intervals.

`percent` can be configured to any integer value from 0 to 100.

```
max-sessions-per-service-utilization percent
```
Default: 80
The percent utilization of the maximum sessions allowed per service as measured in real-time. This threshold is based on the maximum number of sessions or PDP contexts configured for the a particular service. (Refer to the `bind` command for the PDSN, GGSN, SGSN, or HA services.)

`percent` can be an integer from 0 through 100.

```
message-queue-utilization percent
```
Default: 80
The percent utilization of the Demux Manager software task’s message queue as measured in 10 second intervals. The queue is capable of storing a maximum of 10000 messages.

`percent` can be an integer from 0 through 100.

```
message-queue-wait-time time
```
Default: 5
The maximum time (in seconds) messages can be held in queue as measured by packet time stamps.

`time` is measured in seconds and can be an integer from 1 through 30.

**Important:** In the event that this threshold is crossed, an SNMP trap is not triggered. The service congestion policy invocation resulting from the crossing of this threshold is enforced only for the packet that triggered the action.

```
[ no ] port-rx-utilization percent
```
Default: 80
The average percent utilization of port resources for all ports by received data as measured in 5-minute intervals.

`percent` can be an integer from 0 through 100.

```
[ no ] port-specific { slot/port | all } [ rx-utilization percent ] [ tx-utilization percent]
```
Default: Disabled
Sets port-specific thresholds. If you set port-specific thresholds, when any individual port-specific threshold is reached, congestion control is applied system-wide.

`slot/port`: Specifies the port for which port-specific threshold monitoring is being configured. The slot and port must refer to an installed card and port.
Global Configuration Mode Commands (A-K)

congestion-control threshold

**all**: Set port specific threshold monitoring for all ports on all cards.

**rx-utilization percent**: Default 80%. The average percent utilization of port resources for the specified port by received data as measured in 5-minute intervals. *percent* must be an integer from 0 through 100.

**tx-utilization percent**: Default 80%. The average percent utilization of port resources for the specified port by transmitted data as measured in 5-minute intervals. *percent* must be an integer from 0 through 100.

[ no ] port-tx-utilization percent

Default: 80

The average percent utilization of port resources for all ports by transmitted data as measured in 5-minute intervals.

*percent* can be an integer from 0 through 100.

service-control-cpu-utilization percent

Default: 80

The average percent utilization of CPUs on which a Demux Manager software task instance is running as measured in 10-second intervals.

*percent* can be an integer from 0 through 100.

system-cpu-utilization percent

Default: 80

The average percent utilization for all PSC/PSC2 CPUs available to the system as measured in 10-second intervals.

*percent* can be an integer from 0 through 100.

This threshold setting can be disabled with no congestion-control threshold system-cpu-utilization command. In case later you want to enable the same threshold setting congestion-control threshold system-cpu-utilization command will enable the CPU utilization threshold to preconfigured level.

system-memory-utilization percent

Default: 80

The average percent utilization of all CPU memory available to the system as measured in 10-second intervals.

*percent* can be an integer from 0 through 100.

tolerance percent

Default: 10

The percentage under a configured threshold that dictates the point at which the condition is cleared.

*percent* can be an integer from 0 through 100.

**Usage**

Thresholds dictate the conditions for which congestion control is to be enabled and establish limits for defining the state of the system (congested or clear). These thresholds function in a similar fashion to the operation thresholds that can be configured for the system (as described in later in this chapter). The primary difference is that when these thresholds are reached, not only is an SNMP trap generated (starCongestion), but a service congestion policy is invoked as well.

The tolerance parameter establishes the threshold at which the condition is cleared. An SNMP trap (starCongestionClear) is generated for the clear condition, as well.
**Important:** The MME (version 14.0 and higher) supports three levels of thresholds – critical, major and minor – for each condition. Refer to the `congestion-control threshold` commands immediately following this command for information specific to the MME.

### Example

The following command configures a system CPU utilization threshold of 75%.

```
congestion-control threshold system-cpu-utilization 75
```

This setting will remain in configuration unless you specify another threshold value in place of 75. This threshold setting can be disabled with `no congestion-control threshold system-cpu-utilization` command but cannot be removed from configuration. Later if you want to enable the previously configured threshold value of 75 percent, you only need to enter the `congestion-control threshold system-cpu-utilization` command without specifying any threshold value. It will enable the CPU utilization threshold to preconfigured level of 75 percent.

For example, `no congestion-control threshold system-cpu-utilization` disables the configured threshold setting and `congestion-control threshold system-cpu-utilization` again enables the threshold setting of 75%.

The following command configures a threshold tolerance of 5%:

```
congestion-control threshold license-utilization tolerance 5
```

In the above examples, the starCongestion trap gets triggered if the license utilization goes above 75% and the starCongestionClear trap gets triggered if it reaches or goes below 70%.
congestion-control threshold license-utilization

Configures the congestion threshold levels for license utilization on the system.

⚠️ Important: This command applies to MME (version 14.0 and higher) and ePDG (version 14.1 and higher).

**Product**
- MME
- ePDG

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration
- `configure`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
congestion-control threshold license-utilization { critical percent | major percent | minor percent }

default congestion-control threshold license-utilization
```

**default congestion-control threshold license-utilization**

Sets all license-utilization thresholds to the default values.

**critical percent**

Default: 100
The critical threshold value for percent utilization of licensed session capacity, measured in 10-second intervals.

`percent` can be configured to any integer value from 0 to 100.

**major percent**

Default: 0
The major threshold value for percent utilization of licensed session capacity, measured in 10-second intervals.

`percent` can be configured to any integer value from 0 to 100.

**minor percent**

Default: 0
The minor threshold value for percent utilization of licensed session capacity, measured in 10-second intervals.

`percent` can be configured to any integer value from 0 to 100.
Use this command to set the critical, major and minor threshold levels of licensed session capacity as a percentage as measured in 10-second intervals. Thresholds dictate the conditions for which congestion control is to be enabled and establish limits for defining the state of the system (congested or clear). When these thresholds are crossed, an SNMP trap is generated (starCongestion) and, if configured, a congestion action-profile is invoked as well. This command requires a valid product license.

Example

The following command configures a minor threshold level for license utilization of 25%.

```
congestion-control threshold license-utilization minor 25
```

This setting will remain in configuration unless you specify another minor threshold level in place of 25. The following command returns the critical, major, and minor thresholds levels to their default values:

```
default congestion-control threshold license-utilization
```
congestion-control threshold max-sessions-per-service-utilization

Configures the congestion thresholds for the maximum sessions allowed per service.

**Important:** This command applies to MME (version 14.0 and higher) and ePDG (version 14.1 and higher).

**Product**
- MME
- ePDG

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration
  ```
  configure
  ```
  Entering the above command sequence results in the following prompt:
  ```
  [local] host_name(config) #
  ```

**Syntax**

```congestion-control threshold max-sessions-per-service-utilization { critical percent | major percent | minor percent }
```

**default congestion-control threshold max-sessions-per-service-utilization**

Sets all max-sessions-per-service-utilization thresholds to the default values.

- **critical percent**
  - Default: 80
  - The critical threshold value for percent utilization of the maximum sessions allowed per service. *percent* can be configured to any integer value from 0 to 100.

- **major percent**
  - Default: 0
  - The major threshold value for percent utilization of the maximum sessions allowed per service. *percent* can be configured to any integer value from 0 to 100.

- **minor percent**
  - Default: 0
  - The minor threshold value for percent utilization of the maximum sessions allowed per service. *percent* can be configured to any integer value from 0 to 100.
Usage

Use this command to set the critical, major and minor threshold levels of maximum sessions per service as a percentage measured in real-time. This threshold is based on the maximum number of sessions or PDP contexts configured for the a particular service. (Refer to the bind command for the PDSN, GGSN, SGSN, or HA services.)

Thresholds dictate the conditions for which congestion control is to be enabled and establish limits for defining the state of the system (congested or clear). When these thresholds are crossed, an SNMP trap is generated (starCongestion) and, if configured, a congestion action-profile is invoked as well.

This command requires a valid product license.

Example

The following command configures a minor threshold level of 25%.

    congestion-control threshold max-sessions-per-service-utilization minor 25

This setting will remain in configuration unless you specify another minor threshold level in place of 25.

The following command returns the critical, major, and minor thresholds levels to their default values:

    default congestion-control threshold max-sessions-per-service-utilization
congestion-control threshold message-queue-utilization

Configures the congestion thresholds for the percent utilization of the Demux Manager software task’s message queue.

**Important:** This command applies to ePDG (version 14.1 and higher).

<table>
<thead>
<tr>
<th>Product</th>
<th>ePDG</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privilege</td>
<td>Security Administrator, Administrator</td>
</tr>
<tr>
<td>Mode</td>
<td>Exec &gt; Global Configuration configure</td>
</tr>
</tbody>
</table>

Entering the above command sequence results in the following prompt:

```
[local] host_name(config) #
```

**Syntax**

```
congestion-control threshold message-queue-utilization { critical percent | major percent | minor percent }

default congestion-control threshold message-queue-utilization
```

Sets all max-sessions-per-service-utilization thresholds to the default values.

### critical percent

Default: 80
The critical threshold value for percent utilization of the Demux Manager software task’s message queue as measured in 10-second intervals. 

**percent** can be configured to any integer value from 0 to 100.

### major percent

Default: 0
The major threshold value for percent utilization of the Demux Manager software task’s message queue as measured in 10-second intervals. 

**percent** can be configured to any integer value from 0 to 100.

### minor percent

Default: 0
The minor threshold value for percent utilization of the Demux Manager software task’s message queue as measured in 10-second intervals. 

**percent** can be configured to any integer value from 0 to 100.
Usage

Use this command to set the critical, major and minor threshold levels of percent utilization of the Demux Manager software task’s message queue as measured in 10-second intervals. Thresholds dictate the conditions for which congestion control is to be enabled and establish limits for defining the state of the system (congested or clear). When these thresholds are crossed, an SNMP trap is generated (starCongestion) and, if configured, a congestion action-profile is invoked as well.

This command requires a valid product license.

Example

The following command configures a minor threshold level of 25%.

    congestion-control threshold message-queue-utilization minor 25

This setting will remain in configuration unless you specify another minor threshold level in place of 25.

The following command returns the critical, major, and minor thresholds levels to their default values:

    default congestion-control threshold message-queue-utilization
congestion-control threshold message-queue-wait-time

Configures the congestion thresholds for the maximum time (in seconds) messages can be held in queue as measured by packet time stamps.

**Important:** This command applies to ePDG (version 14.1 and higher).

**Product**
ePDG

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

```
[local] host_name(config) #
```

**Syntax**

```
congestion-control threshold message-queue-wait-time { critical time | major time | minor time }

default congestion-control threshold message-queue-wait-time
```

Sets all max-queue-wait-time thresholds to the default values.

**critical time**

Default: 5
The critical threshold value for the maximum time (in seconds) that messages can be held in queue as measured by packet time stamps.

\[ time \] is measured in seconds and can be an integer from 1 through 30.

**major time**

Default: 0
The major threshold value for the maximum time (in seconds) that messages can be held in queue as measured by packet time stamps.

\[ time \] is measured in seconds and can be an integer from 1 through 30.

**minor time**

Default: 0
The minor threshold value for the maximum time (in seconds) that messages can be held in queue as measured by packet time stamps.

\[ time \] is measured in seconds and can be an integer from 1 through 30.
Usage

Use this command to set the critical, major and minor threshold levels for the maximum time (in seconds) messages can be held in queue.
Thresholds dictate the conditions for which congestion control is to be enabled and establish limits for defining the state of the system (congested or clear). When these thresholds are crossed a congestion action-profile is invoked, if configured.
This command requires a valid product license.

Example

The following command configures a major threshold level of 4 seconds.

    congestion-control threshold message-queue-wait-time major 4

This setting will remain in configuration unless you specify another minor threshold level in place of 4.
The following command returns the critical, major, and minor thresholds levels to their default values:

    default congestion-control threshold message-queue-wait-time
congestion-control threshold port-rx-utilization

Configures the congestion thresholds for average percent utilization of port resources for all ports by received data as measured in 5-minute intervals.

**Important:** This command applies to ePDG (version 14.1 and higher).

**Product**
- ePDG

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration
- `configure`

Entering the above command sequence results in the following prompt:

```
[local] host_name(config)#
```

**Syntax**

```
congestion-control threshold port-rx-utilization { critical percent | major percent | minor percent }
```

```
default congestion-control threshold port-rx-utilization
```

Sets all port-rx-utilization thresholds to the default values.

**critical percent**

Default: 80
The critical threshold value for average percent utilization of port resources for all ports by received data as measured in 5-minute intervals.
`percent` can be configured to any integer value from 0 to 100.

**major percent**

Default: 0
The major threshold value for average percent utilization of port resources for all ports by received data as measured in 5-minute intervals.
`percent` can be configured to any integer value from 0 to 100.

**minor percent**

Default: 0
The minor threshold value for average percent utilization of port resources for all ports by received data as measured in 5-minute intervals.
`percent` can be configured to any integer value from 0 to 100.
Usage

Use this command to set the critical, major and minor threshold levels of average percent utilization of port resources for all ports by received data as measured in 5-minute intervals. Thresholds dictate the conditions for which congestion control is to be enabled and establish limits for defining the state of the system (congested or clear). When these thresholds are crossed, an SNMP trap is generated (starCongestion) and, if configured, a congestion action-profile is invoked as well. This command requires a valid product license.

Example

The following command configures a minor threshold level of 25%.

```config
congestion-control threshold port-rx-utilization minor 25
```

This setting will remain in configuration unless you specify another minor threshold level in place of 25. The following command returns the critical, major, and minor thresholds levels to their default values:

```config
default congestion-control threshold port-rx-utilization
```
congestion-control threshold port-specific

Configures the congestion thresholds for specific port utilization.

**Important:** This command applies to ePDG (version 14.1 and higher).

**Product**
ePDG

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

**Syntax**

```
congestion-control threshold port-specific { slot/port { tx-utilization { critical percent | major percent | minor percent } | rx-utilization { critical percent | major percent | minor percent } | all { critical percent | major percent | minor percent } } }
```

```
no congestion-control threshold port-specific { slot/port { critical | major | minor } | all { critical | major | minor } }
```

Sets all port-specific utilization thresholds to the default values.

**slot/port**
Default: Disabled
Specifies the port for which port specific threshold monitoring is being configured. The slot and port must refer to an installed card and port. If you set port-specific thresholds, when any individual port-specific threshold is reached, congestion control is applied system-wide.

**all**
Set threshold monitoring for all ports on all cards.

**rx-utilization**
Set threshold monitoring for received data only.

**tx-utilization**
Set threshold monitoring for transmitted data only.
critical percent
Default: 80
The critical threshold value for average percent utilization of the specified port resources as measured in 5-minute intervals.
percent can be configured to any integer value from 0 to 100.

major percent
Default: 0
The major threshold value for average percent utilization of the specified port resources as measured in 5-minute intervals.
percent can be configured to any integer value from 0 to 100.

minor percent
Default: 0
The minor threshold value for average percent utilization of the specified port resources as measured in 5-minute intervals.
percent can be configured to any integer value from 0 to 100.

Usage
Use this command to set the critical, major and minor threshold levels of average percent utilization of specified resources for all ports by transmitted data as measured in 5-minute intervals. Thresholds dictate the conditions for which congestion control is to be enabled and establish limits for defining the state of the system (congested or clear). When these thresholds are crossed, an SNMP trap is generated (starCongestion) and, if configured, a congestion action-profile is invoked as well.
This command requires a valid product license.

Example
The following command configures a minor threshold level of 5% for received data on port 1 of the card in slot 17.

    congestion-control threshold port-specific 17/1 rx-utilization minor 5

This setting will remain in configuration unless you specify another minor threshold level in place of 5.
congestion-control threshold port-rx-utilization

Configures the congestion thresholds for average percent utilization of port resources for all ports by received data as measured in 5-minute intervals.

**Important:** This command applies to ePDG (version 14.1 and higher).

**Product**
ePDG

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

**configure**
Entering the above command sequence results in the following prompt:

```
[local] host_name(config) #
```

**Syntax**

```
congestion-control threshold port-rx-utilization { critical percent | major percent | minor percent }
```

```
default congestion-control threshold port-rx-utilization
```

Sets all port-rx-utilization thresholds to the default values.

**critical percent**

Default: 80
The critical threshold value for average percent utilization of port resources for all ports by received data as measured in 5-minute intervals.

`percent` can be configured to any integer value from 0 to 100.

**major percent**

Default: 0
The major threshold value for average percent utilization of port resources for all ports by received data as measured in 5-minute intervals.

`percent` can be configured to any integer value from 0 to 100.

**minor percent**

Default: 0
The minor threshold value for average percent utilization of port resources for all ports by received data as measured in 5-minute intervals.

`percent` can be configured to any integer value from 0 to 100.
Usage

Use this command to set the critical, major and minor threshold levels of average percent utilization of port resources for all ports by received data as measured in 5-minute intervals.
Thresholds dictate the conditions for which congestion control is to be enabled and establish limits for defining the state of the system (congested or clear). When these thresholds are crossed, an SNMP trap is generated (starCongestion) and, if configured, a congestion action-profile is invoked as well.
This command requires a valid product license.

Example

The following command configures a minor threshold level of 25%.

    congestion-control threshold port-rx-utilization minor 25

This setting will remain in configuration unless you specify another minor threshold level in place of 25.
The following command returns the critical, major, and minor thresholds levels to their default values:

    default congestion-control threshold port-rx-utilization
congestion-control threshold port-tx-utilization

Configures the congestion thresholds for average percent utilization of port resources for all ports by transmitted data as measured in 5-minute intervals.

**Important:** This command applies to ePDG (version 14.1 and higher).

**Product**
ePDG

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

**Syntax**

congestion-control threshold port-tx-utilization { critical percent | major percent | minor percent }

default congestion-control threshold port-tx-utilization

default congestion-control threshold port-tx-utilization
Sets all port-tx-utilization thresholds to the default values.

critical percent

Default: 80
The critical threshold value for average percent utilization of port resources for all ports by transmitted data as measured in 5-minute intervals.
percent can be configured to any integer value from 0 to 100.

major percent

Default: 0
The major threshold value for average percent utilization of port resources for all ports by transmitted data as measured in 5-minute intervals.
percent can be configured to any integer value from 0 to 100.

minor percent

Default: 0
The minor threshold value for average percent utilization of port resources for all ports by transmitted data as measured in 5-minute intervals.
percent can be configured to any integer value from 0 to 100.
Usage

Use this command to set the critical, major and minor threshold levels of average percent utilization of port resources for all ports by transmitted data as measured in 5-minute intervals. Thresholds dictate the conditions for which congestion control is to be enabled and establish limits for defining the state of the system (congested or clear). When these thresholds are crossed, an SNMP trap is generated (starCongestion) and, if configured, a congestion action-profile is invoked as well. This command requires a valid product license.

Example

The following command configures a minor threshold level of 25%.

```
congestion-control threshold port-tx-utilization minor 25
```

This setting will remain in configuration unless you specify another minor threshold level in place of 25. The following command returns the critical, major, and minor thresholds levels to their default values:

```
default congestion-control threshold port-tx-utilization
```
congestion-control threshold service-control-cpu-utilization

Configures the congestion thresholds for average percent utilization of CPUs on which a Demux Manager software task instance is running as measured in 10-second intervals.

**Important:** This command applies to MME (version 14.0 and higher) and ePDG (version 14.1 and higher).

**Product**
- MME
- ePDG

**Privilege**
- Security Administrator
- Administrator

**Mode**
- Exec > Global Configuration
- configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
congestion-control threshold service-control-cpu-utilization { critical percent | major percent | minor percent }
```

```
default congestion-control threshold service-control-cpu-utilization
```

Sets all service-control-cpu-utilization thresholds to the default values.

**critical percent**

Default: 80

The critical threshold value for average percent utilization of CPUs on which a Demux Manager software task instance is running as measured in 10-second intervals.

*percent* can be configured to any integer value from 0 to 100.

**major percent**

Default: 0

The major threshold value for average percent utilization of CPUs on which a Demux Manager software task instance is running as measured in 10-second intervals.

*percent* can be configured to any integer value from 0 to 100.

**minor percent**

Default: 0

The minor threshold value for average percent utilization of CPUs on which a Demux Manager software task instance is running as measured in 10-second intervals.

*percent* can be configured to any integer value from 0 to 100.
Usage

Use this command to set the critical, major and minor threshold levels of average percent utilization of CPUs on which a Demux Manager software task instance is running as measured in 10-second intervals. Thresholds dictate the conditions for which congestion control is to be enabled and establish limits for defining the state of the system (congested or clear). When these thresholds are crossed, an SNMP trap is generated (starCongestion) and, if configured, a congestion action-profile is invoked as well. When the service-control-cpu-utilization critical threshold setting is exceeded, ipsecmgrs running in the congested CPU are notified of the congestion. The ipsecmgrs raise traps for service-congestion exceeded and update the NPU so that no new calls are sent to those ipsecmgrs. The NPU does not send any new calls to the congested ipsecmgrs. However, if all ipsecmgrs are congested the action is always drop regardless of the setting for congestion policy action. The packet drops are silently done by the NPU. When ipsecmgrs are congested and an NPU receives a packet whose Security Parameter Index, Initiator (SPIi) in IKE_SA_INIT matches that of a currently established session, the packet is classified as belonging to the existing session. Since congestion action is applied only on new sessions, such IKE_SA_INIT packets are allowed to create sessions. If the IKE_SA_INIT uses an SPIi which does not match any of the existing sessions, it is processed according to the congestion policy action. This command requires a valid product license.

Example

The following command configures a minor threshold level of 25%.

```
congestion-control threshold service-control-cpu-utilization minor 25
```

This setting will remain in configuration unless you specify another minor threshold level in place of 25. The following command returns the critical, major, and minor thresholds levels to their default values:

```
default congestion-control threshold service-control-cpu-utilization
```
congestion-control threshold system-cpu-utilization

Configures the congestion thresholds for average percent CPU utilization of all packet processing cards available to the system as measured in 10-second intervals.

**Important:** This command applies to MME (version 14.0 and higher) and ePDG (version 14.1 and higher).

**Product**
- MME
- ePDG

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration
- `configure`

Entering the above command sequence results in the following prompt:

```
[local]hostname(config)#
```

**Syntax**

```
congestion-control threshold system-cpu-utilization { critical percent | major percent | minor percent }
```

```
default congestion-control threshold system-cpu-utilization
```

Sets all system-cpu-utilization thresholds to the default values.

**critical percent**

Default: 80

The critical threshold value for average percent CPU utilization of all packet processing cards available to the system.

`percent` can be configured to any integer value from 0 to 100.

**major percent**

Default: 0

The major threshold value for average percent CPU utilization of all packet processing cards available to the system.

`percent` can be configured to any integer value from 0 to 100.

**minor percent**

Default: 0

The minor threshold value for average percent CPU utilization of all packet processing cards available to the system.

`percent` can be configured to any integer value from 0 to 100.
Use this command to set the critical, major and minor threshold levels of average percent CPU utilization of all packet processing cards available to the system as measured in 10-second intervals. Thresholds dictate the conditions for which congestion control is to be enabled and establish limits for defining the state of the system (congested or clear). When these thresholds are crossed, an SNMP trap is generated (starCongestion) and, if configured, a congestion action-profile is invoked as well.

This command requires a valid product license.

Example

The following command configures a minor threshold level of 25%.

```
congestion-control threshold system-cpu-utilization minor 25
```

This setting will remain in configuration unless you specify another minor threshold level in place of 25. The following command returns the critical, major, and minor thresholds levels to their default values:

```
default congestion-control threshold system-cpu-utilization
```
congestion-control threshold system-memory-utilization

Configures the congestion thresholds for the average percent utilization of all CPU memory available to the system as measured in 10-second intervals.

**Important:** This command applies to MME (version 14.0 and higher) and ePDG (version 14.1 and higher).

**Product**
- MME
- ePDG

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration
- configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
congestion-control threshold system-memory-utilization { critical percent | major percent | minor percent }

default congestion-control threshold system-memory-utilization
```

Sets all system-memory-utilization thresholds to the default values.

**critical percent**
Default: 80
The critical threshold value for the average percent utilization of all CPU memory available to the system as measured in 10-second intervals.

**major percent**
Default: 0
The major threshold value for the average percent utilization of all CPU memory available to the system as measured in 10-second intervals.

**minor percent**
Default: 0
The minor threshold value for the average percent utilization of all CPU memory available to the system as measured in 10-second intervals.
Usage

Use this command to set the critical, major and minor threshold levels of average percent utilization of all CPU memory available to the system as measured in 10-second intervals. Thresholds dictate the conditions for which congestion control is to be enabled and establish limits for defining the state of the system (congested or clear). When these thresholds are crossed, an SNMP trap is generated (starCongestion) and, if configured, a congestion action-profile is invoked as well. This command requires a valid product license.

Example

The following command configures a minor threshold level of 25%.

```
congestion-control threshold system-memory-utilization minor 25
```

This setting will remain in configuration unless you specify another minor threshold level in place of 25. The following command returns the critical, major, and minor thresholds levels to their default values:

```
default congestion-control threshold system-memory-utilization
```
congestion-control threshold tolerance

Configures the percentage under a configured threshold value that dictates the point at which the condition is cleared.

**Important:** This command applies to MME (version 14.0 and higher) and ePDG (version 14.1 and higher).

**Product**
- MME
- ePDG

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration
  - configure

Entering the above command sequence results in the following prompt:

```
[local] host_name(config) #
```

**Syntax**

```
congestion-control threshold tolerance { critical percent | major percent | minor percent }
```

```
default congestion-control threshold system-cpu-utilization
```

Sets all threshold tolerances to the default values.

- **critical percent**
  - Default: 10
  - The tolerance percentage for critical thresholds. When a critical threshold drops below this level, the condition is cleared.
  - `percent` can be configured to any integer value from 0 to 100.

- **major percent**
  - Default: 0
  - The tolerance percentage for major thresholds. When a major threshold drops below this level, the condition is cleared.
  - `percent` can be configured to any integer value from 0 to 100.

- **minor percent**
  - Default: 0
  - The tolerance percentage for minor thresholds. When a minor threshold drops below this level, the condition is cleared.
  - `percent` can be configured to any integer value from 0 to 100.
Usage

Use this command to set the tolerance limits for critical, major and minor thresholds.
The tolerance parameter establishes the threshold at which the condition is cleared. An SNMP trap
(starCongestionClear) is generated for the clear condition.
This command requires a valid product license.

Example

The following command configures the tolerance level of 5% for minor thresholds.

    congestion-control threshold tolerance minor 5

This setting will remain in configuration unless you specify another tolerance for minor thresholds in place of
5.
The following command returns the critical, major, and minor threshold tolerance levels to their default
values:

    default congestion-control threshold tolerance
**connectedapps**

Enables the configuration of Connected Apps (CA) client communication with the IOS-XR CA server on an ASR 9000. This command sends you to the Connected Apps Configuration mode.

**Product**
SecGW (WSG)

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration
```
configure
```
Entering the above command sequence results in the following prompt:

```
[local] host_name(config) #
```

**Syntax**
```
connectedapps
```

**Usage**
Use this command to go to the Connected Apps Configuration mode. In this mode you can set CA client session parameters and ASR 9000 VSM High Availability (HA) chassis and network modes.

**Example**
The following command sends you to the Connected Apps Configuration mode:
```
connectedapps
```
content-filtering category database directory

This command configures the base directory to be used for storing all content-rating databases that are required for Category-based Content Filtering application.

Product
CF

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

content-filtering category database directory path  directory_path

default content-filtering category database directory path

default

Specifies the default base directory and directory path for Category-based Content Filtering application.

directory_path

Default: /pcmcia1/cf

Specifies the base directory and its path to store all of the full or incremental content rating databases for the Category-based Content Filtering application.
directory_path must be an alphanumeric string of 1 through 255 characters.

Usage

Use this command to specify the directory and its path to download all full or incremental category-rating databases to be used for the Category-based Content Filtering application.
Merging of incremental database can be done as part of the database upgrade process preformed with upgrade content-filtering category database command in the Executive Mode.

Example

The following command configures the /flash/cf_temp/DB as the base directory to download all full and incremental content-rating databases for content filtering application.

content-filtering category database directory path /flash/cf_temp/DB
content-filtering category database max-versions

This command configures the number of full content-rating databases to maintain/archive in the base directory for category-based content filtering application.

Product
CF

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

content-filtering category database max-versions num_archive

default content-filtering category database max-versions

default

Sets the default number of full databases for specified directory path/location.

num_archive

Default: 2
Specifies the maximum number of database to be archived or maintained in the specific location.
num_archive must be an integer from 1 through 3.

Usage

Use this command to set the number of full content-rating database to be maintained in the specified directory path with the base file name specified using the content-filtering database override file command. The specified directory path is the location specified using the content-filtering category database directory path command.

Example

The following command configures the system to maintain 3 full content-rating databases for category-based content filtering application.

content-filtering category database max-versions 3
content-filtering category database override

This command specifies the name of a file to be used by the category-rating database load process for category-based content filtering application.

Product
CF

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax
content-filtering category database override file file_name.extension

default content-filtering category database override file

default

Sets the default content rating database file name; for example, optcmd.bin.

file file_name.extension

Specifies the header of the file in the database directory path location to determine the newest full database. file_name must be an alphanumeric string of up to 10 characters with an extension of 3 characters after a period (.) as extension.

Usage
Use this command to configure the category-rating database file name to determine the newest version of full database. A process called "LOAD_DATABASE" invokes during the system startup or the database upgrade process by upgrade content-filtering category database command in Executive Mode. This process examines the header of each of the files in the database folder specified by content-filtering category directory path command in this mode.

Note that by default system examines the header of those files only which begins with the string “OPTCMDB” and having extension “.bin”.

Example
The following command configures the system to examine the header of files that begins with CF_sta.DB only for content filtering application.

content-filtering category database override file CF_sta.DB
context

Enters the Context Configuration mode or is used to add or remove a specified context.

Product

All

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local] host_name(config) #

Syntax

context name [ -noconfirm ]

no context name

no

Removes the specified context from the configuration.

name

Specifies the name of a context to enter, add, or remove. When creating a new context, the context name must be unique.

Important: When creating a new context, the context name specified must not conflict with the name of any existing context or domain names.

-noconfirm

Indicates that the command is to execute without any additional prompt and confirmation from the user.

Usage

Configure contexts or remove obsolete contexts.

Important: A maximum of 64 contexts may be created.

Example

context sampleContext

no context sampleContext
Global Configuration Mode Commands (A-K)

**crash enable**

Enables or disables the copying of crash data to a specified location.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

**configure**
Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
crash enable [ encrypted ] url crash_url [ filename-pattern pattern ] [ restrict mbyte ]
```  

```
no crash enable
```

Removes the specified context from the configuration.

**Important:** System crash information is generated and stored in the crash list even when the no keyword is specified. The information maintained in the crash lists is minimal crash information when the no keyword has been specified.

```
encrypted
```
Indicates that the URL encrypted for security reasons.

```
filename-pattern pattern
```
The filename-pattern is a an alphanumeric string containing any or all of the following variables:
- `%hostname%` - The system hostname.
- `%ip%` - A SPIO IP address
- `%cpu%` - CPU number
- `%card%` - Card number
- `%time%` - POSIX timestamp in hexadecimal notation
- `%filename%` - Alias for `crash-%card%-%cpu%-%time-core%`
- `%%` - A single % sign

If no pattern is specified, the result is the same as the pattern `filename`. Use '/' characters in the filename pattern part to store crashes in per-system subdirectories.
**url crash_url**

Specifies the location to store crash files. *crash_url* may refer to a local or a remote file. *crash_url* must be entered using the following format:

For the ASR 5000:

- `file: /{flash|pcmcia1|hd}/directory/`
- `tftp://host[:port]/{directory}/`
- `ftp: | sftp: //username[:password]@host[:port]/{directory}/`

For the ASR 5500:

- `file: /{flash|usb1|hd}/directory/`
- `tftp://host[:port]/{directory}/`
- `ftp: | sftp: //username[:password]@host[:port]/{directory}/`

**Important:** Use of the SMC hard drive is not supported in this release.

**Important:** Do not use the following characters when entering a string for the field names below: “/” (forward slash), “:” (colon) or “@” (at sign).

- `directory` is the directory name.
- `filename` is the actual file of interest.
- `username` is the user to be authenticated.
- `password` is the password to use for authentication.
- `host` is the IP address or host name of the server.
- `port#` is the logical port number that the communication protocol is to use.

**restrict mbyte**

Specifies a maximum amount of memory (in megabytes) to use for storing crash files as an integer from 1 through 128. Default: 128

The **restrict** keyword is only applicable to local URLs.

**Usage**

Enable crashes if there are systems that are not stable and the crash information will be useful for troubleshooting. The remote storage of the crash file reduces the memory utilized on the chassis.

**Example**

```plaintext
  crash enable ftp://remoteABC/pub/crash.dmp
  crash enable /flash/pub/data/crash.dmp restrict 64
  no crash enable
```
crypto blacklist file

Configures a blacklist (access denied) file to be used by a Wireless Security Gateway (WSG).

Product

All products supporting IPSec blacklisting

**Important**: This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

Privilege

Security Administrator

Mode

Exec > Global Configuration

`configure`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

Syntax

```
crypto blacklist file pathname

no crypto blacklist file
```

**no**

Removes the blacklist file from the system.

**pathname**

Specifies the location of the blacklist file as:

- `[ file: ]{/flash|/usbl|/hd-raid}{/directory}/{filename}
- `tftp://[host[:port]][/directory]/<filename`
- `[ ftp: | sftp: ]//username[:password]@[host][:port][/directory]/<filename`
- `http://<username>:<password>@<host>[:<port>][/<directory>]/<filename`

Usage

Use this command to configure the location of the blacklist file to be used by a WSG. A blacklist is a list or register of entities that are being denied a particular privilege, service, mobility, access or recognition. With blacklisting, any peer is allowed to connect as long as it does not appear in the list. Each entry in the blacklist file should contain the ID type so that the validation is performed for that ID type. In every entry, the ID type and ID value should be separated by a space. Only DOS and UNIX file formatting are supported. For additional information, refer to the *System Administration Guide*. 
**Important:** Either a blacklist, a whitelist or none is configured. Both listing techniques cannot be used simultaneously on the system.

Example

```plaintext
crypto blacklist file ftp://remoteABC/pub/blacklist.txt

crypto blacklist file /flash/pub/data/blacklist.txt
```
crypto remote-secret-list

Specifies the remote secret list for storing remote secrets based on the ID type. This command sends you to the Remote Secret List Configuration mode. Only one active remote-secret-list is supported per system.

Product
All products supporting IPSec remote secrets

**Important:** This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

Privilege
Security Administrator

Mode
Exec > Global Configuration

config
Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

crypto remote-secret-list listname

no crypto remote-secret-list listname

no

Deletes the remote-secret-list file from the system.

**Important:** You must unbind the remote-secret-list from any crypto maps or templates before it can be deleted.

listname

Usage

Use this command to specify the remote secret list for storing remote secrets based on the ID type. Only one remote-secret-list can be configured per system. Executing this command places you in the Remote Secret List Configuration mode.

This list of remote pre-shared keys is based on the remote ID type. The remote secret list can contain up to 1000 entries.

For additional information, refer to the Remote Secret List Configuration Commands chapter and the System Administration Guide.

Example

The following command creates a remote-secret-list named rs-list:

```
crypto remote-secret-list rs-list
```
crypto whitelist file

Configures a whitelist (access permitted) file to be used by a Wireless Security Gateway (WSG).

**Product**

All products supporting IPSec whitelisting

---

**Important:** This command appears in the CLI for this release. However, it has not been qualified for use with any current Cisco StarOS gateway products.

**Privilege**

Security Administrator

**Mode**

Exec > Global Configuration

**configure**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```plaintext
crypto whitelist file pathname [ -noconfirm ]
```

**no crypto whitelist file**

```
no
```

Removes the blacklist file from the system.

**pathname**

Specifies the location of the whitelist file as:

- `[ file: ]{/flash|/usb1|/hd-raid}/[directory]/<filename>`
- `tftp://[host[:port#]]/[directory]/<filename>`
- `[ ftp: | sftp: ]//[username[:password]@] [host][:port#]/[directory]/<filename>`
- `http://[<username>:<password>@]<host>[:<port>]/[<directory>]/<filename>`

**Usage**

Use this command to configure the location of the white file to be used by a WSG. A whitelist is a list or register of entities that are being provided a particular privilege, service, mobility, access or recognition. With whitelisting, no peer is allowed to connect unless it appears in the list. Each entry in the whitelist file should contain the ID type so that the validation is performed for that ID type. In every entry, the ID type and ID value should be separated by a space. Only DOS and UNIX file formatting are supported. For additional information, refer to the *System Administration Guide*.
**Important:** Usually either a blacklist, a whitelist or none is configured. Both listing techniques cannot be used simultaneously on the system.

**Example**

```
crypto whitelist file ftp://remoteABC/pub/whitelist.txt

crypto whitelist file /flash/pub/data/whitelist.txt
```
cs-network

This command creates/removes an HNB-CS network configuration instance for Famed UMTS access over Iu-CS/Iu-Flex interface between Home NodeB Gateway (HNB-GW) service and CS networks elements; i.e. MSC/VLR. This command also configures an existing HNB-CS network instance and enters the HNB-CS Network Configuration mode on a system.

Product
HNB-GW

Privilege
Administrator

Mode
Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local] host_name(config)#

Syntax

`cs-network cs_instance [ -noconfirm ]`

`no cs-network cs_instance`

`no`

Removes the specified HNB-CS network instance from the system.

⚠️ Caution: Removing the HNB-CS network instance is a disruptive operation and it will affect all UEs accessing MSC(s) configured in specific CS core network through the HNB-GW service.

⚠️ Caution: If any HNB-CS Network instance is removed from system all parameters configured in that mode will be deleted and Iu-CS/Iu-Flex interface will be disabled.

`cs_instance`

Specifies the name of the Circuit Switched Core Networks instance which needs to be associated with the HNB Radio Network PLMN via the HNB RN-PLMN Configuration mode. If `cs_instance` does not refer to an existing HNB-PS network instance, the new HNB-CS network instance is created.

`cs_instance` must be an alphanumeric string of 1 through 63 characters.

`-noconfirm`

Indicates that the command is to execute without any additional prompt and confirmation from the user.

Usage

Use this command to enter the HNB-CS Network Configuration mode for an existing CS network instance or for a newly defined HNB-CS network instance. This command is also used to remove an existing HNB-CS network instance.
This configuration enables/disables the Iu-CS/Iu-Flex interface on HNB-GW service with CS core network elements; i.e. MSC/VLR.
A maximum of one HNB-CS network instance per HNB-GW service instance which is further limited to a maximum of 256 services (regardless of type) can be configured per system.

⚠️ Caution: This is a critical configuration. The HNBs cannot access MSC(s) in CS core network without this configuration. Any change to this configuration would lead to disruption in HNB access to CS core network.

Entering this command results in the following prompt:

```plaintext
[context_name]hostname(config-cs-network)#
```

The various parameters available for configuration of an HNB-CS network instance are defined in the HNB-CS Network Configuration Mode Commands chapter.

**Example**

The following command enters the existing HNB-CS Network configuration mode (or creates it if it does not already exist) for the instance named `hnb-cs1`:

```plaintext
cs-network hnb-cs1
```

The following command will remove HNB-CS network instance `hnb-cs1` from the system without any warning to operator:

```plaintext
no cs-network hnb-cs1
```
css acsmgr-selection-attempts

This is a restricted command. In 9.0 and later releases this command is obsolete.
css delivery-sequence

This is a restricted command. In 9.0 and later releases this command is obsolete.
css service

This is a restricted command. In 9.0 and later releases this command is obsolete.
default

Restores the system default values for the specified parameters.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]\host_name(config)#

Syntax

```
default {  aaa { accounting-overload-protection domain-matching | username-format }  |  arp base-reachable-time | autoconfirm | banner [ lawful-intercept | motd | pre-login ] | boot [ delay | interface | nameserver | networkconfig ] | bulkstats historical collection | card-standby-priority | cdr-multi-mode | clock timezone | cli max-sessions | congestion-control [ overload-disconnect | policy | threshold ] | diameter-proxy ramdisk | enforce { imsi-min equivalence | ip optimize-ipid-assignment } | gtpp { compression-processes | ram-disk-limit } | high-availability fault-detection speed | local-user { allow-aaa-authentication | lockout-time | max-failed-logins } | logging { display | filter runtime } | network-overload-protection | operational-mode | pac-standby-priority | qos npu inter-subscriber traffic { bandwidth | priority [ assigned-to dscp { af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be | ef } ] } | require { cipher ss1 resource-percentage | demux card | session recovery } | reveal disabled commands | snmp { engine-id | heartbeat | history heartbeat | notif-threshold } | system { contact | description | hostname | location | serial-number } | system-mac | system-priority | task { facility sessmgr start | resource cpu-memory-low } | terminal { all | databits | flowcontrol | parity | speed | stopbits } | threshold { value } | timestamps | upgrade limit [ time ] [ usage ] }

aaa { accounting-overload-protection domain-matching | username-format }

Restores the aaa behavior to its default of disabled for the following options:

*domain-matching*: Restores the default domain matching method.
*username-format*: Restores the use of the default username format for global AAA services

arp base-reachable-time

Restores ARP base-reachable-time to 30 seconds.

autoconfirm

Restores the autoconfirm behavior to its default of disabled.
**banner**

*lawful-intercept* - Restores the system default message of the day for SSH CLI sessions.

*motd* - Restores the system default message of the day banner.

*pre-login* - Restores the CLI login banner to the system default.

**boot [ delay | interface | nameserver | networkconfig ]**

*interface | networkconfig* - Restores the default boot interface and network configuration options. The keywords *interface* and *networkconfig* are used to restore the default option settings for the interface and network configuration options, respectively. Defaulting the network configuration boot option removes the network boot option from the boot.sys file. It does not remove the network config options from the configuration file which is managed separately from the boot.sys file.

*delay* - Removes the boot delay setting (if any). The default for boot delay is “no boot delay”.

*nameserver* - Removes the nameserver IP address.

**card-standby-priority**

Resets the standby priority of the Packet Services Cards.

**cdr-multi-mode**

Restores the default value of this command to Single-CDRMOD mode.

**cli max-sessions**

Restores the default value of this command to *no cli max-sessions* which removes the limit on the number of allowed simultaneous CLI sessions on the system.

**clock-timezone**

Restores the system’s clock timezone to UTC.

**congestion-control [ overload-disconnect | policy | threshold ]**

Restores the system’s congestion-control functionality to its default setting of disabled. You can selectively restore other components to their default values.

**diameter-proxy ram-disk**

Restores the ram-disk size to 32MB.

**enforce { imsi-min equivalence | ip optimize-ipid-assignment }**

Disables the enforcement of either option.

**gtpp { compression-process | ram-disk-limit }**

Restores number of compression processes allowed to 1. Restores the RAM disk size to 32MB.

**high-availability fault-detection speed**

Restores speed to Normal.
local-user { allow-aaa-authentication | lockout-time | max-failed-logins }
Enables aaa-authentication.
Restores lock-time to 60 minutes.
Restores max-failed-logins to 5.

logging {display | filter runtime}
display: sets the default level of detail to display for trace log information to the system default.
fILTER runtime: resets the filtering of logged information to log in real time.

network-overload-protection
For SGSN, disables this attach rate throttle feature that provides network overload protection.

operational-mode
Sets the operational mode of the chassis to the system default.

pac-standby-priority
This parameter has been replaced by the card-standby-priority keyword.

qos npu inter-subscriber traffic {bandwidth | priority [ assigned-to dscp { af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be | ef } ] }
Restores the following NPU QoS parameters to their default values:
• bandwidth:
  • gold: 10%
  • silver: 20%
  • bronze: 30%
  • best-effort: 40%
• priority: All DSCP values are mapped to the best-effort priority queue but are not configured.

require { cipher ssl resource-percentage | demux card | session recovery }
Resets the cipher ssl resource-percentage to 0.
Disables the demux capabilities on the demux card.
Disables the session recovery feature.

snmp { engine-id | heartbeat | history heartbeat |notif-threshold }
engine-id: Restores the SNMP engine ID to the system default.
heartbeat: Restores the SNMP heartbeat interval to 60 minutes.
history heartbeat: Reenables the recording of heartbeat notifications in SNMP history.
notif-threshold: Restores the SNMP notification thresholds to the system defaults.

system { contact | description | hostname | location | serial-number }
Sets the following system parameters to their default values:
• contact: Resets to none specified.
• description: Resets to none specified.
• **hostname**: Resets to “asr5000” or asr5500”.
• **location**: Resets to none specified.
• **serial-number**: Resets to factory default.

**system-mac hostname**
Resets the system MAC address to the factory default value.

**system-priority hostname**
Resets the system priority to its default value.

**task { facility sessmgr start | resource cpu-memory-low }**

**facility sessmgr start**: Restores the default session manager start policy to Normal.
**resource cpu-memory-low**: Resets the system so that when a CPU runs very low on memory (below 12MB) the most over-limit task is killed.

**terminal { all | databits | flowcontrol | parity | speed | stopbits }**

**all**: Restores all terminal parameters to their default values.
**databits**: Resets to 8 data bits.
**flowcontrol**: Resets to none.
**parity**: Resets to none.
**speed**: Resets 9600 bits/second.
**stopbits**: Resets to one stop bit.

**threshold { value }**
Restores thresholding values to their default setting. The possible values are:
• **10sec-cpu-utilization**: CPU utilization using a 10 sec average.
• **aaa-acct-archive-queue-size<1..3>**: AAA accounting archive queue threshold settings.
• **aaa-acct-archive-size**: AAA accounting archive size.
• **aaa-acct-failure**: AAA accounting failure threshold settings
• **aaa-acct-failure-rate**: AAA accounting failure rate threshold settings
• **aaa-auth-failure**: AAA authentication failure threshold settings
• **aaa-auth-failure-rate**: AAA authentication failure rate threshold settings
• **aaa-retry-rate**: AAA retry rate threshold settings
• **aamgr-request-queue**: AAA manager internal request queue threshold settings
• **asngw-auth-failure**: ASN-GW Auth Failure related threshold
• **asngw-handoff-denial**: ASN-GW handoff denial threshold
• **asngw-max-eap-retry**: ASN-GW maximum EAP retry threshold
• **asngw-network-entry-denial**: ASN-GW Network entry denial threshold
• **asngw-session-setup-timeout**: ASN-GW session setup timeout threshold
• **asngw-session-timeout**: ASN-GW session timeout threshold
• **asnpc-idle-mode-timeout**: ASN-PC idle mode timeout threshold
• **asnpc-im-entry-denial**: ASN-PC IM entry denial threshold
• asnpc-lu-denial: ASN-PC lu denial threshold
• asnpc-session-setup-timeout: ASN-PC session setup timeout threshold
• bgp-routes: bgp routes threshold
• call-reject-no-resource: Calls rejected due to no resources threshold settings
• call-setup: Calls setup threshold settings
• call-setup-failure: Call setup failure threshold settings
• card-temperature-near-power-off-limit: Threshold for the gap between the current card temperature and the power off limit
• cdr-file-space: CDR file space threshold
• contfilt-block: Content Filtering Blocks threshold settings
• contfilt-rating: Content Filtering Ratings threshold settings
• cpu-available-memory: CPU available memory threshold settings
• cpu-load: PSC/PSC2 CPU load (5-minute average)
• cpu-memory-usage: Percentage of total CPU memory usage
• cpu-orbs-critical: ORBs process CPU usage critical level
• cpu-orbs-warn: PORBs process CPU usage warning level
• cpu-session-throughput: CPU session throughput threshold settings
• cpu-utilization: CPU utilization threshold settings
• dcca-bad-answers: Diameter Bad Answers threshold settings
• dcca-protocol-error: Diameter Protocol Error threshold settings
• dcca-rating-failed: Diameter Rating Failed threshold settings
• dcca-unknown-rating-group: Diameter Unknown Rating Group threshold settings
• diameter: Diameter threshold settings
• dns-learnt-ip-max-entries: DNS IP maximum entries threshold
• dns-lookup-failure: DNS Lookup Failure threshold
• edr-file-space: EDR file space threshold
• edr-udr-dropped-flow-control: EDR-UDRs Dropped due to flow control
• epdg-current-sessions: Current EPDG sessions threshold
• fng-current-active-sessions: Femto Network Gateway (FNG) current active sessions threshold
• fng-current-sessions: FNG current sessions threshold
• fw-deny-rule: Stateful Firewall Deny Rule threshold
• fw-dos-attack: Stateful Firewall Dos-Attacks threshold
• fw-drop-packet: Stateful Firewall Drop Packets threshold
• fw-no-rule: Stateful Firewall No-Rule threshold
• license: Session license threshold settings
• mgmt-cpu-memory-usage: Management (SMC) CPU memory usage threshold
*mgmt-cpu-utilization*: Management (SMC) CPU utilization threshold (most recent 5-minute average)

*mme-attach-failure*: MME Attach Failure related threshold

*mme-auth-failure*: MME Auth Failure related threshold

*model*: Thresholding model settings

*monitoring*: Threshold monitoring configuration settings

*nat-port-chunks-usage*: Port chunk utilization threshold

*npu-utilization*: NPU utilization threshold (most recent 5-minute average)

*packets-filtered-dropped*: Filtered/dropped packet threshold settings

*packets-forwarded-to-cpu*: Forwarded packet threshold settings

*pdg-current-active-sessions*: PDG current active sessions threshold

*pdg-current-sessions*: PDG current sessions threshold

*pdif-current-active-sessions*: Threshold monitoring for only the currently-active PDIF sessions.

*pdif-current-sessions*: Threshold monitoring for all current PDIF sessions.

*per-service-asngw-sessions*: The number of sessions per ASN-GW service

*per-service-ggsn-sessions*: The number of GGSN sessions per GGSN service

*per-service-gprs-pdp-sessions*: The number of PDP contexts per GPRS service

*per-service-gprs-sessions*: The number of GPRS sessions per GPRS service

*per-service-ha-sessions*: The number of HA sessions per HA service

*per-service-lns-sessions*: The number of LNS sessions per LNS service

*per-service-pdsn-sessions*: The number of PDSN sessions per PDSN service

*per-service-sgsn-pdp-sessions*: The number of PDP contexts per SGSN service

*per-service-sgsn-sessions*: The number of SGSN sessions per SGSN service

*phsgw-eapol-auth-failure*: Personal Handy Phone Gateway (PHSGW) EAPOL authentication failure threshold

*phsgw-handoff-denial*: PHSGW handoff denial threshold

*phsgw-max-eap-retry*: PHSGW maximum EAP retry threshold

*phsgw-max-eapol-retry*: PHSGW max EAPOL retry threshold

*phsgw-network-entry-denial*: PHSGW Network entry denial threshold

*phsgw-session-setup-timeout*: PHSGW session setup timeout threshold

*phsgw-session-timeout*: PHSGW session timeout threshold

*phspc-session-setup-timeout*: PHSPC session setup timeout threshold

*phspc-sleep-mode-timeout*: PHSPC sleep mode timeout threshold

*phspc-sm-entry-denial*: PHSPC sm entry denial threshold

*poll*: Threshold polling interval configuration settings

*ppp-setup-fail-rate*: PPP setup failure rate threshold

*rp-setup-fail-rate*: RP setup failure rate threshold
• storage-utilization: Mass storage (flash memory) utilization
• subscriber: subscriber related thresholds
• system-capacity: Percentage usage of system resources
• total-asngw-sessions: Total ASN-GW sessions threshold
• total-ggsn-sessions: Total GGSN sessions for all GGSN services in the system
• total-gprs-pdp-sessions: Total PDP contexts for all GPRS services in the system
• total-gprs-sessions: Total GPRS sessions per for all GPRS services in the system
• total-ha-sessions: Total HA sessions for all HA services in the system
• total-hnbgw-hnb-sessions: Total 3G Home NodeBGateway (HNBGW) HNB sessions for all HNB services in the system
• total-hnbgw-iu-sessions: Total HNBGW Iu sessions in the system
• total-hnbgw-ue-sessions: Total HNBGW UE sessions in the system
• total-hsgw-sessions: Total HRPD Serving Gateway (HSGW) sessions for all HSGW services in the system
• total-lma-sessions: Total Local Mobility Anchor (LMA) sessions for all LMA services in the system
• total-lns-sessions: Total L2TP Network Server (LNS) sessions for all LNS services in the system
• total-mme-sessions: Total Mobility Management Entity (MME) sessions for all MME services in the system
• total-pdsn-sessions: Total PDSN sessions for all PDSN services in the system
• total-pgw-sessions: Total Packet Data Network Gateway (PGW) sessions for all PGW services in the system
• total-saegw-sessions: Total PDP contexts for all SAEGW services in the system
• total-sgsn-pdp-sessions: Total PDP contexts for all SGSN services in the system
• total-sgsn-sessions: Total SGSN sessions for all SGSN services in the system
• total-sgw-sessions: Total Serving gateway (SGW) sessions for all SGW services in the system

timestamps
Resets the inclusion of timestamps in command.

upgrade limit [ time ] [ usage ]
Sets upgrade limit values to the defaults. If the optional keywords are not specified all values are reset to their defaults.
time: Resets the maximum time a session may exist during a software upgrade to the default of 120.
usage: Resets the minimum number of sessions before closing the sessions during a software upgrade to the system default of 100.

Usage
Restore system defaults to aid in trouble shooting or just prior to modifying additional configuration options.

Example
default banner motd
default boot

default logging display

default system hostname

default upgrade limit time
**diameter dynamic-dictionary**

This command allows configuring a Diameter dictionary dynamically at run time, and then loading the dynamic dictionary in to the system.

**Important:** The maximum number of dynamic dictionaries that can be loaded in to the system is 10.

**Product**
- GGSN
- HA
- HSGW
- IPSG
- PDSN
- P-GW
- SAEGW
- S-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

```
configure
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
diameter dynamic-dictionary name url
no diameter dynamic-dictionary name
```

**Right Margin**

```
no
Unloads the specified dynamic Diameter dictionary from the system.
```

```
name
Specifies the name of the dynamic Diameter dictionary as an alphanumeric string of 1 through 15 characters.
```

```
url
Specifies the URL of the Diameter dictionary to be loaded in to the system. The input must be an alphanumeric string of 1 through 127 characters.
```
Usage
This command is used to define a new Diameter dictionary on the fly, and load the dynamic dictionary into the system.
To perform this configuration, you should first create a text file in ABNF format and configure all the required Diameter AVPs and command codes in the file. Then, save the file in flash or some URL that will be accessible by the system.
Now, configure a dynamic dictionary with an unique name and map it to the URL of the file to be loaded dynamically into the system at the global configuration level.
When the names of the dynamic dictionaries and their URLs are configured, the corresponding files at the respective URLs are parsed and populated in all SessMgr and AAAMgr facilities as new dictionaries and kept available to be used when these dictionary names are configured under any Diameter application level or AAA group.
When a dynamic dictionary name is configured under an application such as IMS authorization service or in an AAA group, the corresponding dictionary (which is already loaded in SessMgrs and AAAMgrs) entry will be used.
There will be only one instance of a dynamic dictionary loaded into a task for one dynamic dictionary name even if the same dictionary name is configured in multiple AAA groups or multiple application configurations. That is, even if the same dictionary name is configured in several applications or several AAA groups, all these applications and AAA groups will refer to the same dynamic dictionary instance.

Example
The following command configures a Diameter dictionary named *dyn1* and loads this dictionary to the /flash/diameter_custom1.sndd path:

```
diameter dynamic-dictionary dyn1 /flash/diameter_custom1.sndd
```
diameter-host-template

Specifies the name of a Diameter host template and enters the Diameter Host Select mode. A Diameter host template is a table of peer servers that can be shared by multiple services.

Product

GGSN
HA
HSGW
IPSG
PDSN
P-GW
SAEGW
S-GW

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

```
diameter-host-template name [ -noconfirm ]

no diameter-host-template name
```

no

Removes the specified Diameter host template from the Global Configuration.

name

Specifies the name of the template as an alphanumeric string of 1 through 63 characters.

[-noconfirm ]

Executes the command without prompting for further input from the user.

Usage

Specifies the name of a new or existing Diameter host template and opens the Diameter Host Select mode. You can configure up to 256 templates on the system.

To use the template, Diameter applications must be associated with the template. When an association is made to the template, the system selects the Diameter peer to be contacted based on rows configured in the table and the algorithm configured for selecting rows in the table.
**Important:** Currently, only Gx service can be associated with the template.

If more than one service is using the same set of `peer-select` commands, then it is better to define all the peer selection CLIs in the template and associate the services to the template. Entering this command results in the following prompt:

```
[context_name] hostname (config-host-template) #
```

Diameter host select configuration commands are defined in the *Diameter Host Select Configuration Mode Commands* chapter.

**Example**

The following command specifies a Diameter host template named `diamtemplate`:

```
diameter-host-template diamtemplate
```
diameter-proxy ram-disk

This command configures the amount of extra RAM disk space in MB to be allocated to Diamproxy task when local storage (hard disk) is enabled.

**Product**
- HSGW
- P-GW
- SAEGW
- S-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

**Syntax**
```
diameter-proxy ram-disk mb space_mb
```
```
default diameter-proxy ram-disk mb
```

**Usage**
Specifies the additional storage space to be allocated to Diamproxy for file write, in MB. The specified memory in MB is added to the existing memory allocated to Diamproxy only if HDD storage is enabled. By default, 32 MB is additionally allocated.

**Example**
The following command specifies that 100 MB of additional storage space be allocated to the Diamproxy task:

```
diameter-proxy ram-disk mb 100
```
ecmp-lag hash

This command provides the configuration to select source Boxer Internal Address (SBIA) as the input to the hashing function for ECMP-LAG distribution.

**Product**
HNB-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
[no] ecmp-lag hash use-sbia-only
```

- **no**
  
  Disables the hashing function selection and sets the system to use IP Source Address, IP Destination Address, IP Protocol and Source BIA as inputs to the hashing algorithm for ECMP-LAG distribution.

**Usage**

Use this command to allow the operator to change the way hashing works in deciding which link to use for ECMP and Link Aggregation. In the default hashing algorithm the IP Source Address, IP Destination Address, IP Protocol and Source BIA are used in the hashing function. When “use-sbia-only” option is selected, only the Source BIA is used in the hashing function.

⚠️ **Caution:** When using ECMP-LAG on a HNB-GW, this configuration is **mandatory** for standalone HNB-GW deployment and highly recommended in other deployment scenarios where HNB-GW is used in combination with other services.

**Example**

The following command enables the SBIA as input to hash function for ECMP-LAG on the HNB-GW:

```
ecmp-lag hash use-sbia-only
```

The following commands sets the hashing function to use standard inputs for ECMP-LAG on HNB-GW:

```
no ecmp-lag hash use-sbia-only
```
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
```
end
```

**Usage**
Use this command to return to the Exec mode.
enforce imsi-min equivalence

Enables the PDSN/HA to treat IMSI and MIN as the same for identifying the PDSN/HA session.

**Product**
PDSN
HA

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
[ no | default ] enforce imsi-min equivalence
```

- **default**
  
  Returns the command to its default setting of disabled.

- **no**
  
  Disables the PDSN/HA from treating IMSI and MIN as the same for identifying the PDSN/HA session.

**Usage**

Generally on an HA, the IMSI and MIN are treated as different and hence the RRQs with 1x and DO PDSNs are processed as different sessions. You can use this feature to treat the IMSI and MIN with the matching lower 10-digit as the same for identifying a session. The 10-digit MIN and the 15-digit IMSI are treated as equivalent for the purpose of matching sessions if the lower 10 digits are the same. Any handoff from 1x to DO or vice-versa is treated as the same session if the NAI and HoA also match. If the NAI and/or HoA do not match, then the duplicate IMSI session detect and terminate feature is applicable.

Generally on a PDSN, the IMSI and MIN are treated as different and hence RP messages from 1x and DO PDSNs are processed as different sessions. You can use this feature to treat the IMSI and MIN with the matching lower 10-digit as the same for identifying a session. The 10-digit MIN and the 15-digit IMSI are treated as equivalent for the purpose of matching PDSN sessions if the lower 10 digits are the same. Any handoff from 1x to DO or vice-versa is treated as the same session.

**Example**

To monitor or clear subscriber session information filtered by on IMSI/MIN refer to the `show subscribers msid` command.

**Important:** This command must be executed at startup only and will not take effect when reconfigured without rebooting.
**Example**

The following command enables the treatment of the IMSI and MIN as the same for identifying the session:

```
enforce imsi-min equivalence
```

Either of the following commands disables the treatment of the IMSI and MIN as the same for identifying sessions:

```
no enforce imsi-min equivalence
default enforce imsi-min equivalence
```
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**
Use this command to return to the parent configuration mode.
fa-spi-list

Replaces a duplicate Foreign Agent- Security Parameter Index (FA-SPI) remote address list applied to multiple FA services with a list name.

Product
PDSN
FA

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

```
fa-spi-list fa_spi_list
```

```
fa_spi_list

Remote address list name expressed as an alphanumeric string of 1 through 64 characters.
```

Usage
Use this command to Replace duplicate FA-SPI remote address list applied to multiple FA or HA services with a list name.

Example
The following command configures the list FA SPI list to fa-list2:

```
fa-spi-list fa-list2
```
failure-handling-template

This command allows the user to create/modify/delete a Diameter failure handling template at the global configuration level. This command specifies the name of failure handling template and enters the Failure Handling Template mode. The users can define the failure handling configurations within this template.

**Important:** A maximum of 64 templates can be configured on the system.

**Product**
- GGSN
- HA
- HSGW
- IPSG
- PDSN
- P-GW
- SAEGW
- S-GW

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration
- `configure`

Entering the above command sequence results in the following prompt:

```
[local] host_name(config) #
```

**Syntax**

```
failure-handling-template name [ -noconfirm ]
```

```
no failure-handling-template name
```

- **no**
  - Removes the specified failure handling template from the Global Configuration.

- **name**
  - Specifies the name of the failure handling template as an alphanumeric string of 1 through 63 characters.

- **[ -noconfirm ]**
  - Executes the command without prompting for further input from the user.
Usage

Specifies the name of a new or existing failure handling template and opens the Failure Handling Template mode. Depending on which application is using the failure handling template, some of the syntactically possible configurations within the template are not applicable.

To use the template, Diameter applications must be associated with the template. When an association is made to the template, in the event of a failure, the system takes the action as defined in the failure handling template. Both IMS Authorization (Gx) and Diameter Credit Control Application (DCCA) (Gy) services can be associated with the template.

Entering this command results in the following prompt:

[context_name]hostname(config-fh-template)#

Failure handling template configuration commands are defined in the Diameter Failure Handling Template Configuration Mode Commands chapter.

Example

The following command specifies a failure handling template named FHtemplate:

`failure-handling-template FHtemplate`
get context-list

Generates an XML-formatted list of all currently configured contexts within the system.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local] host_name(config) #
```

**Syntax**

```
get context list [ | { grep grep_options | more } ]
```

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of `grep` and `more`, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter.

**Usage**

Generates a list of all currently configured contexts in XML format. The output can be copied and pasted into compatible applications.

**Example**

```
get context-list
```
get ip

Generates an XML-formatted display of IPv4-based information.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

get ip { access-list | arp [vrf name] | bgp neighbors | interface [vrf name] | ospf { interface | neighbor | vrf name | route [vrf name] | vrf } [ | { grep grep_options | more } ]

access-list
Generates an XML-formatted display of all IPv4 Access Control Lists (ACLs).

arp
Generates an XML-formatted display of all Allocation Retention Priorities (ARPs) or the ARPs for the named Virtual Routing and Forwarding (VRF) table.

bgp neighbors
Generates an XML-formatted display of all Border Gateway Protocol (BGP) neighbors.

interface [vrf name]
Generates an XML-formatted display of all interfaces or for only those associated with a specified VRF table (optional).

ospf { interface | neighbor | vrf name }
Generates an XML-formatted display of all Open Shortest Path First (OSPF) routing information.

*interface: Displays interface information for OSPF.
*neighbor: Displays summarized information about all known OSPF neighbors.
*vrf name: Displays information for the named VRF table.

route [vfr name]
Generates an XML-formatted display of all IPv4-based routes or for only those associated with a specified VRF table (optional).
**get ip**

<table>
<thead>
<tr>
<th>vrf</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generates an XML-formatted display of all VRF tables.</td>
</tr>
</tbody>
</table>

`vrf` | \{ grep grep_options | more \}

Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.

For details on the usage of *grep* and *more*, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter.

---

**Usage**

Generates a display of IPv4-based information in XML format. The output can be copied and pasted into compatible applications.

**Example**

```
get ip access-list
```
get ipv6

Generates an XML-formatted display of IPv6-based information.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
get ip { access-list | interface [vrf name] | ospf { interface | neighbor } | route [vrf name] } [ | { grep grep_options | more } ]
```

<table>
<thead>
<tr>
<th><strong>access-list</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Generates an XML-formatted display of all IPv6 Access Control Lists (ACLs).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>interface [vrf name]</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Generates an XML-formatted display of all IPv6 interfaces or for only those associated with a specified VRF table (optional).</td>
</tr>
</tbody>
</table>

| **ospf { interface | neighbor }** |
|------------------------------|
| Generates an XML-formatted display of all Open Shortest Path First version 3 (OSPFv3) routing information. |
| *interface*: Displays interface information for OSPFv3. |
| *neighbor*: Displays summarized information about all known OSPFv3 neighbors. |

<table>
<thead>
<tr>
<th><strong>route [vrf name]</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Generates an XML-formatted display of IPv6 routes or for only those associated with a specified VRF table (optional).</td>
</tr>
</tbody>
</table>

| | { grep grep_options | more } |
|-----------------------------|
| Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent. |
| For details on the usage of **grep** and **more**, refer to the Regulating a Command’s Output section of the Command Line Interface Overview chapter. |

**Usage**

Generates a display of IPv6-based information in XML format. The output can be copied and pasted into compatible applications.
Example

```
get ipv6 access-list
```
get port info

Generates an XML-formatted display for all physical ports or a specific port in the system.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

`configure`

Entering the above command sequence results in the following prompt:

`[local]host_name(config)#`

**Syntax**

```
get port info [slot/port ] [ | { grep grep_options | more } ]
```

- `slot/port`
  Generates an XML-formatted display of information for the port specified by its chassis slot and card port number.

- `| { grep grep_options | more }`
  Pipes (sends) the output of this command to the specified command. You must specify a command to which the output of this command will be sent.
  For details on the usage of `grep` and `more`, refer to the *Regulating a Command’s Output* section of the *Command Line Interface Overview* chapter.

**Usage**

Generates a display of IP-based information in XML format. The output can be copied and pasted into compatible applications.

**Example**

```
get ip port
```
global-title-translation address-map

Creates an instance of a Global Title Translation (GTT) address-map, a database, for global titles (ISDN-type address) used for SCCP routing. Upon creating the instance, the system enters global title translation address-map configuration mode. For the commands to configure the database, go to the Global Title Translation Address-Map Configuration Mode Commands chapter.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
global-title-translation address-map instance instance

no global-title-translation address-map instance instance
```

no

Removes the specified GTT address-map database from the SCCP portion of the configuration.

```
instance
```

This value uniquely identifies a specific instance of a GTT address-map. `instance` must be an integer from 1 through 4096.

**Usage**

Create a GTT address-map with a unique identifier and enter the GTT address-map configuration mode.

**Example**

```
global-title-translation address-map instance 324
```
global-title-translation association

Creates an instance of a Global Title Translation (GTT) association which defines the rules for handling global title translation. Upon creating the instance, the system enters global title translation association configuration mode. For the commands to configure the rules, go to the Global Title Translation Association Configuration Mode Commands chapter.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

```
global-title-translation association instance instance

no global-title-translation association instance instance
```

Usage

Removes the specified instance of a GTT association from the SCCP portion of the configuration.

```
instance
```

This value uniquely identifies a specific instance of a GTT association.

`instance` must be an integer from 1 through 16.

Example

Create a GTT association with a unique identifier and enter the GTT association configuration mode.

```
global-title-translation association instance 2
```
gtpp compression-process

This command configures the maximum number of child compression processes that AAA proxy can have.

Product
- GGSN
- SAEGW
- SGSN

Privilege
- Security Administrator, Administrator

Mode
Exec > Global Configuration
```
configure
```
Entering the above command sequence results in the following prompt:
```
[local]host_name(config)#
```

Syntax
```
gtpp compression-process max_number
default gtpp compression-process
```

**default**
Restores the system to the default settings for the number of child compression processes allowed.

**max_number**
Specifies the maximum number of child processes. The default is 1

```
max_number: must be an integer from 1 through 4.
```

Usage
This command configures the maximum number of child compression processes that AAA proxy can have only if hard disk storage is enabled.

Example
```
gtpp compression-process 3
```
**gtpp ram-disk-limit**

This command configures additional storage space to be allocated for writing files.

**Product**
- GGSN
- SAEGW
- SGSN

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration
- configure

Entering the above command sequence results in the following prompt:

```
[local] host_name(config)#
```

**Syntax**

```
gtpp ram-disk-limit mb mega_bytes
```

```
default gtpp ram-disk-limit
```

**default**

Restores the system to the default settings of 32 MB of storage.

```
mb mega_bytes
```

Specifies the number of megabytes of storage allocated for files.

`mega_bytes`: must be an integer from 10 through 256. The default is 32 MB.

**Usage**

The memory specified with this command would be added to the existing memory allocated to the AAA proxy only if hard disk storage is enabled.

**Example**

```
gtpp ram-disk-limit mb 256
```
gtpp single-source

Configures the system to reserve a CPU for performing a proxy function for accounting.

**Product**
- GGSN
- SGSN
- P-GW
- SAEGW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

```
configure
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config) #
```

**Syntax**

```
gtpp single-source [ centralized-lrsn-creation | private-extensions ]
```

**no gtpp single-source**

```
centralized-lrsn-creation
```
Defines Log Record Sequence Number (LRSN) generation at proxy. The AAA proxy will generate the LRSN for all CDR types generated by either the GGSN or the SGSN. Default: disabled

```
private-extensions
```
This optional keyword enables the proprietary use of customer-specific GTPP extensions. If `private-extensions` is not configured, all customer specific private extensions related to GTPP message transfer with CGF and recovery through GSS are disabled.

**Important:** In order for the customer-specific extensions to work properly, the `gtpp max-pdu-size` command in the Context Configuration Mode should be set to 65400 and the `gtpp server` command’s `max` value should be set to “1”.

```
no
```
Disables GTPP single-sourcing. This is the default setting.

**Caution:** Entering this command while PDP contexts are in process could cause the loss of pending CDRs. The configuration must be saved and the chassis reloaded for this option to take effect.

---

**Note:**
- The `gtpp single-source` command is used to configure the system to reserve a CPU for performing a proxy function for accounting. It is typically used in scenarios where there is a need to monitor and track traffic at the network level, such as in QoS (Quality of Service) applications or traffic management systems.
- The command can be configured with optional parameters like `centralized-lrsn-creation` and `private-extensions` to define specific behaviors for handling CDRs (Call Detail Records).
- The `no` option is used to disable the `gtpp single-source` configuration and revert to the default settings.
- Proper configuration of this command, especially with the `max-pdu-size` parameter, is crucial to avoid any loss of data during network operations.

---

**Product:**
- GGSN: Gateway General Packet Radio Service Node
- SGSN: Serving GPRS Support Node
- P-GW: Packet Data Network Gateway
- SAEGW: Service Access Gateway

**Privilege:**
- Security Administrator
- Administrator

**Mode:**
- Exec > Global Configuration
Usage

When GTPP single-sourcing is enabled, the system’s AAA proxy function generates requests to the accounting server using a single UDP source port number, instead of having each AAA Manager generate independent requests with unique UDP source port numbers. This is accomplished by the AAA Managers forwarding their GTPP PDUs to the AAA Proxy function that runs on a reserved packet processing card CPU. Since a packet processing card CPU is being reserved, fewer Session Managers and AAA Managers will be started on that card.

⚠️ Caution: This command must be entered prior to the configuration of other services. Specifying it later may return an error due to a lack of CPU availability.

Example

The following command enables GTPP single-sourcing with the use of private GTPP extensions:

```
    gtpp single-source private-extensions
```

The following command disables GTPP single-sourcing:

```
    no gtpp single-source
```
**ha-spi-list**

Replaces a duplicate Home Agent-Security Parameters Index (HA-SPI) remote address list applied to multiple HA services with a list name.

**Product**

PDSN

HA

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration

`configure`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
ha-spi-list ha_spi_list
```

- **ha_spi_list**

Remote address list name expressed as an alphanumeric string of 1 through 64 characters.

**Usage**

Use this command to Replace duplicate HA-SPI remote address list applied to multiple HA services with a list name.

**Example**

The following command configures the list HA SPI list to `ha-list2`:

```
ha-spi-list ha-list2
```
**hd raid**

Performs RAID management operations on the platform hard disk drives.

### Product

All

### Privilege

Security Administrator, Administrator

### Mode

Exec > Global Configuration

**configure**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

### Syntax

For the ASR 5000:

```
hd raid { check | create | insert | overwrite | remove select } local1 | remote1 } [ -force ] [ -noconfirm ]
```

For the ASR 5500:

```
hd raid { check | create | insert | overwrite | remove select } hd_num [ -force ] [ -noconfirm ]
```

---

**check**

 Starts a background check on RAID disks unless the RAID is running in degraded mode.

---

**create local1 | remote1**

On the ASR 5000, creates a new RAID that could run in degraded mode on the specified drive:

- `local1`: specifies the RAID is to be established on the primary SMC.
- `remote1`: specifies the RAID is to be established on the backup SMC.

---

**create hd_num**

On the ASR 5500, creates a new RAID that could run in degraded mode on the hard drive array of a specific FSC.

- `hd_num`: specifies the RAID is to be established on the FSC in slot numbers 13 through 18 (hd13, hd14, ..., hd18).

---

**insert local1 | remote1**

On the ASR 5000, inserts the specified disk to the running RAID causing it to recover from degraded mode.

- `local1`: specifies the primary SMC is to be inserted into the RAID.
- `remote1`: specifies the backup SMC is to be inserted into the RAID.
Global Configuration Mode Commands (A-K)

**hd raid**

### insert hd_num

On the ASR 5500, inserts the specified FSC disk array into the running RAID causing it to recover from degraded mode.

**hd_num** specifies the RAID is to be established on the FSC in slot numbers 13 through 18 (hd13, hd14, ..., hd18).

### insert { | local1 | local2 }

On VPC, inserts the specified vHD into the running RAID causing it to recover from degraded mode.

### overwrite local1 | remote1

On the ASR 5000, overwrites the specified disk and adds it to the current running RAID to construct a fully mirrored array.

**local1** specifies the primary SMC is to be added to the current RAID. **remote1** specifies the backup SMC is to be added to the current RAID.

### overwrite hd_num

On the ASR 5500, overwrites the specified FSC disk array and adds it to the current running RAID to construct a fully mirrored array.

**hd_num** specifies the RAID is to be established on the FSC in slot numbers 13 through 18 (hd13, hd14, ..., hd18).

### overwrite { | local1 | local2 }

On VPC, overwrites the specified vHD and adds it to the current running RAID to construct a fully mirrored array.

### remove local1 | remote1

On the ASR 5000, removes the specified disk from the running RAID causing it to run in degraded mode or to fail.

**local1** specifies the primary SMC is to be removed from the RAID. **remote1** specifies the backup SMC is to be removed from the RAID.

### remove hd_num

On the ASR 5500, removes the specified FSC disk array from the running RAID causing it to run in degraded mode or to fail.

**hd_num** specifies the RAID is to be established on the FSC in slot numbers 13 through 18 (hd13, hd14, ..., hd18).

### remove { | local1 | local2 }

On the VPC, removes the specified vHD from the running RAID causing it to run in degraded mode or to fail.

### select local1 | remote1

On the ASR 5000, selects the specified disk to assemble a RAID when two unrelated RAID disks are present in the system. The resulting RAID runs in degraded mode.

**local1** specifies the primary SMC is to assemble the RAID. **remote1** specifies the backup SMC is to assemble the RAID.
**select hd_num**

On the ASR 5500, selects the specified FSC disk array to assemble a RAID when two or more unrelated RAID disks are present in the system. The resulting RAID runs in degraded mode.

*hd_num* specifies the RAID is to be established on the FSC in slot numbers 13 through 18 (hd13, hd14, ..., hd18).

**-noconfirm**

Executes the command without displaying “are you sure” prompts.

**-force**

Executes the command and overrides warnings.

---

**Usage**

All commands need confirmation unless the `--noconfirm` is included in the command. If the result will bring down a running RAID, you have to force the command using `--force`. RAID commands are needed to intervene in the following situations:

- the hard disk controller task can not determine the correct operation,
- administrator action is required by policy
- the administrator wants to wipe out an unused disk.

In an automated system, the policies created with this CLI address the possibility of a manually partitioned disk, a disk resulting from a different version of software, a partially constructed disk, or the case of two unrelated disks in the system.

To reduce administrator intervention, a set of policies can be configured to set the default action using the commands in the HD RAID configuration mode. These commands are described in the *HD Storage Policy Configuration Mode Commands* chapter of this guide.

**Example**

The following instructs the system to setup a RAID on the primary ASR 5000 SMC hard drive.

```bash
hd raid create local1 --force
```
**hd storage-policy**

Provides access to the local hard drive configuration mode in order to manage parameters supporting local storage of records.

**Product**

GGSN
SGSN
HSGW
P-GW
SAEGW
S-GW

**Privilege**

Administrator

**Mode**

Exec > Global Configuration

`configure`

Entering the above command sequence results in the following prompt:

```
[local] host_name(config)#
```

**Syntax**

```
[ no ] hd storage-policy name
```

**no**

Removes a configured HD storage policy from the system.

```
storage-policy name
```

Specifies a name for an HD storage policy and then enters the HD Storage Policy Configuration Mode. `name` must be an alphanumeric string of 1 through 63 characters.

**Usage**

Creates a new policy or specifies an existing policy and enters the HD Storage Policy Configuration Mode. Entering this command results in the following prompt:

```
[context_name]hostname(config-hd-storage-policy)#
```

HD Storage Policy Configuration Mode commands are defined in the HD Storage Policy Configuration Mode Commands chapter.

**Example**

The following command creates an HD storage policy named `policy3` and enters the HD Storage Policy Configuration Mode:

```
hd storage-policy policy3
```
high-availability

Configures the speed for detection of packet processing card task failures.

**Product**
- PDSN
- GGSN
- ASN-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
high-availability fault-detection speed { aggressive | normal }

default high-availability fault-detection speed

{ aggressive | normal }

Default: normal

• aggressive: Initiates packet processing card failover without performing additional checks.
• normal: Initiates packet processing card failover after additional checks are performed.
```

**Usage**

Use this command to increase the fault detection speed for faster switchovers after a packet processing card task failure.

Setting fault detection speed to aggressive will trigger packet processing card failover as soon as possible if a potential failure is detected. Aggressive mode will reduce the duration of subscriber outages caused by a failed packet processing card if session recovery is enabled.

Aggressive mode also bypasses most information gathering steps and logs that can be used to determine the root cause of the failure.

In normal mode, additional checks are performed before triggering a packet processing card failover to ensure that the card has actually failed. In aggressive mode these checks are bypassed so that session recovery can start as soon as possible. These additional checks reduce the likelihood of a false positive failure.

**Example**

The following command sets the fault detection speed for packet processing card tasks to **aggressive**:

```
high-availability fault-detection speed aggressive
```
**hybrid-mode**

Enables an ASR 5000 chassis to run a mix of Packet Services Cards (PSCs) and PSC Type A (PSCAs). When enabled, PSCAs will boot and be compatible with the PSCs as long as encryption services are disabled. The default is to run the chassis in non-hybrid mode; PSCAs will not boot when inserted in the chassis.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

```
configure
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config)#
```

**Syntax**

```
[ no ] hybrid-mode [ force ]
```

- `no`
  Returns the chassis to non-hybrid mode. PSCAs will not boot.

- `force`
  Always updates the configuration, even if the encryption services could not be disabled. However, the PSC and PSCA cards will continue to be incompatible until encryption services are manually disabled.

**Usage**

To allow a chassis to run in PSC/PSCA hybrid-mode with encryption services disabled you must configure `hybrid-mode force` once.

To go from hybrid mode to non-hybrid mode, you must enter the `no hybrid-mode force` command. Non-hybrid chassis mode allows encryption services to be started through the appropriate CLI commands. However, all PSCAs in the chassis will be disabled.

For additional information, see the *ASR 5000 Installation Guide*.

**Example**

The following command enables the chassis to run a mix of PSCs and PSCAs without encryption services:

```
hybrid-mode force
```
imei-profile

Creates an instance of an International Mobile Equipment Identity (IMEI) profile.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration  
  configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
[ no ] imei-profile imei_profile_name
```

- **no**
  Deletes the IMEI profile instance from the configuration.

- **imei_profile_name**
  Specifies the name of the IMEI profile as an alphanumeric string of 1 through 64 characters.

**Usage**

Use this command to create an instance of an IMEI profile and to enter the IMEI Profile Configuration mode. An IMEI profile is a template which groups a set of device instructions, such as blacklisting, that may be applicable to one or more calling devices. See the **IMEI Profile Configuration Mode Commands** chapter for information regarding the definition of the rules contained within the profile and the use of the profile.

**Important:** An IMEI profile is a key element of the Operator Policy feature and is only valid when associated with at least one operator policy.

To see what IMEI profiles have already been created, return to the Exec mode and enter the `show imei-profile all` command.

**Example**

The following command creates a configuration instance of an IMEI profile:

```
imei-profile imeiprof1
```
Chapter 141
Global Configuration Mode Commands (L-S)

This section includes the commands license through system.
The Global Configuration Mode is used to configure basic system-wide parameters.

Mode

Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
license

Configures the session license key.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

`configure`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
license key key_value [ -force ] session-limit

no license key key_value [ -force ] session-limit
```

- **no**
  - Removes the license key(s) installed.

- **key key_value**
  - Installs the license key specified by `key_value`. `key_value` is provided by Cisco operations staff.

- **session-limit**
  - Use this keyword to suppress fail-over calls from being rejected if the licensed threshold is crossed.

**Important:** This is a customer-specific command that is available for HA, PDSN, EHA, and PDIF. Please contact your local Cisco sales representative for more information.

- **-force**
  - Sets the license key even if resources are not available. The system supports the dynamic resizing of demultiplexor software tasks based on the licensed session capacity and feature type. When installing a license, the system automatically attempts to resize currently functioning tasks. Warning messages are displayed if there is an issue. Though its use is not recommended, the `-force` keyword can be used to suppress these warning messages.

**Caution:** Use of this option is not recommended.

**Usage**

Install or update system session keys when necessary due to expiration and/or capacity needs.

**Example**

Install or update system session keys when necessary due to expiration and/or capacity needs.
license key sampleKeyValue

no license key
**line**

Enters the terminal display line configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

```
configure
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
line
```

**Usage**

Change the terminal display configuration based upon the users own terminal characteristics.
link-aggregation

Configures system MAC address and priority for Link Aggregation. These parameters are usually changed to match the feature requirements of the remote Ethernet switch.

Product
WiMAX
PDSN
HA
FA
GGSN
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

link-aggregation { system-mac { MAC_address | auto } | system-priority priority } [-noconfirm ]

{ default | no } link-aggregation { system-mac | system-priority } [-noconfirm ]

---

default

Resets the configuration to the default.

---

system-mac { MAC_address | auto }

Sets the system MAC address used along with the system priority to form the system ID.
MAC_address is manually entered as six groups of two hexadecimal digits separated by hyphens (for example, 01-23-45-67-89-ab).
Auto is the default and is the MAC address of the LAG master port.

---

system-priority priority

This command sets the system priority used by Link Aggregation Control Protocol (LACP) to form the system ID.
priority is a hexadecimal value from 0x0000 through 0xFFFF. Default is 0x8000 (32768).

---

-noconfirm

Executes the command without additional prompting for command confirmation.
link-aggregation

Usage

The system MAC address (6 bytes) and system priority (2 bytes) combine to form the system ID. A system consists of a packet processing card and its associated QGLC or XGLC traffic ports. The highest system ID priority (the lowest number) handles dynamic changes.

For additional usage and configuration information for the link aggregation feature, refer to the System Administration Guide.

Important: Not supported on all platforms

Example

The following command configures the link aggregation system-priority to 10640 (0x2990):

```
link-aggregation system-priority 0x2990
```
**local-policy-service**

This command enables creating, configuring, or deleting a local QoS policy.

**Product**

P-GW
SAEGW

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
local-policy-service name [ -noconfirm ]
no local-policy-service name
```

*no*

Deletes the specified local QoS policy service from the system.

*name*

Specifies name of the local QoS policy service as an alphanumeric string of 1 through 63 characters.

**Important:** The *name* must be unique across all contexts.

If the named local QoS policy service does not exist, it is created, and the CLI mode changes to the Local Policy Service Configuration Mode wherein the local QoS policy service can be configured. If the named local QoS policy service already exists, the CLI mode changes to the Local Policy Service Configuration Mode for that local QoS policy service.

*noconfirm*

Specifies that the command must execute without prompting for confirmation.

**Usage**

Use this command to specify a local QoS policy service name to allow configuration of a local QoS policy service.

**Important:** This feature is license dependent. Please contact your local sales representative for more information.
A local QoS policy service can be used to control different aspects of a session, such as QoS, data usage, subscription profiles, or server usage, by means of locally defined policies. Local QoS policies are triggered when certain events occur and the associated conditions are satisfied. For example, when a new call is initiated, the QoS to be applied for the call could be decided based on the IMSI, MSISDN, and APN.

**Important:** A maximum of 16 local QoS policy services are supported.

Entering this command results in the following prompt:

```
[context_name] hostname(config-local-policy-service)#
```

Local Policy Service Configuration Mode commands are defined in the *Local Policy Service Configuration Mode Commands* chapter.

**Example**

The following command creates a local QoS policy service named `lctest` and enters the Local Policy Service Configuration Mode:

```
local-policy-service lctest
```
local-user allow-aaa-authentication

Enables or disables the use of administrative accounts other than local-user administrative accounts.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

**Syntax**

```
[ default | no ] local-user allow-aaa-authentication
```

- **default**
  Returns this parameter to its default setting of enabled.

- **no**
  Disables administrative user accounts other than local-user accounts.

**Usage**

Local-user administrative accounts are separate from other administrative user accounts configured at the context level (Security Administrator, Administrator, Operator, and Inspector). Context-level administrative users rely on the system’s AAA subsystems for validating user names and passwords during login. This is true for both administrative user accounts configured locally through a configuration file or on an external RADIUS server. Since the T1.276-2003 password security mechanisms are supported only for local-user administrative accounts and not for the AAA-based administrative accounts, this command provides a mechanism for disabling AAA-based administrative accounts.

By default, AAA-based administrative accounts are allowed.

**Example**

The following command forces the system to authenticate local-user accounts based only on the information in the security account file on its CompactFlash:

```
no local-user allow-aaa-authentication
```
local-user lockout-time

Configures the lockout period for local-user administrative accounts.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[[local]host_name(config)#

Syntax

local-user lockout-time time

default local-user lockout-time

default
Restores the parameter to its default setting.

time
Default: 60
Specifies the amount of time (in minutes) that must elapse before a previously locked-out local-user account can attempt to login again. time is an integer from 1 through 10080.

Usage
Local-user administrative accounts can become locked for reasons such as exceeding the configured maximum number of login failures.

Once an account is locked, this parameter specifies the lockout duration. Once the amount of time configured by this parameter has elapsed, the local-user can once again attempt to login.

Example
The following command configures a lockout time of 120 minutes (2 hours):

      local-user lockout-time 120
local-user max-failed-logins

Configures the maximum number of failed login attempts a local-user can have before their account is locked out.

Product  
All

Privilege  
Security Administrator, Administrator

Mode  
Exec > Global Configuration  
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

```plaintext
local-user max-failed-logins number
```

| [ default | no ] local-user max-failed-logins |
|-----------------------------|
| no |
| Disables this functionality. |
| default |
| Restores this parameter to its default setting. |
| number |
| Default: 5 |
| Specifies the maximum number of times a local-user could experience a login failure before their account is locked out. `number` is an integer from 2 through 100. |

Usage

This command configures the maximum number of failed login attempts a local-user can have before their account is locked out. For example if, this parameter is configured to “3” then after the third failed login attempt, the account would be locked.

**Important:** Local-user accounts can be configured to either enforce or reject a lockout due to the maximum number of failed login being reached. Refer to the `local-user username` command for more information.

Example

Refer to the `local-user lockout-time` command for more information.

The following command configures a maximum of three login attempts:

```plaintext
local-user max-failed-logins 3
```
local-user password

Configures local-user administrative account password properties.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

local-user password { [ complexity { ansi-t1.276-2003 | none } ] [ history length number ] [ duration days ] [ max-age days ] [ min-change-char number ] [ min-change-interval days ] [ min-length number ] }

no local-user password { [ history ] [ max-age ] [ min-change-interval ] }

default local-user password { [ complexity ] [ history ] [ max-age ] [ min-change-char ] [ min-change-interval ] [ min-length ] }

no
Disables the specified parameter.

default
Restores the specified parameter to its default setting.

[ complexity { ansi-t1.276-2003 | none } ]

Default: ansi-t1.276-2003

Specifies the password strength as one of the following:

ansi-t1.276-2003: If this option is selected, the following rules are enforced:

• Passwords may not contain the username or the reverse of the username
• Passwords may contain no more than three of the same characters used consecutively
• Passwords must contain at least three of the following:
  • uppercase alpha character
  • lowercase alpha character
  • numeric character
  • special character

none: No additional password checks are performed.
[ **Global Configuration Mode Commands (L-S)**](#)

### local-user password

```
[ history length number [ duration days ] ]
```

Default: length is 5
Specifies the number of previous password entries kept in the history list maintained by the system. A password cannot be reused if it is one of the entries kept in the history list unless the time it was last used was more than the number of days specified by the `duration` keyword.

If the `duration` keyword is not used, the only check performed by the system is that it is not in the history list. `number` is the number of entries for each account stored in the history list entered as an integer from 1 through 100. `days` is the number of days during which a password can not be reused entered an integer from 1 through 365.

```
[ max-age days ]
```

Default: 90
Specifies the maximum age for a password. Users logging in with a password older than the specified limit are locked out. Once the lockout period expires, at their next login attempt, they are prompted to change their password before accessing the CLI.

**Important:** Local-user accounts can be configured to either enforce or reject a lockout due to a password’s maximum age being reached. Refer to the `local-user username` command for more information.

`days` is the number of days that passwords remain valid entered as an integer from 1 through 365.

```
[ min-change-char number ]
```

Default: 2
Specifies the minimum number of characters that must be changed (in comparison to the current password) when a user changes their password.

**Important:** Changes in password length are counted as “character” changes. For example: changing a password from “password” to “passwo” is a 2-character change, changing a password from “password” to “password2” is a 1-character change, and changing a password from “password” to “apassword” is a 9-character change.

`number` is the number of characters entered as an integer from 0 through 16.

```
[ min-change-interval days ]
```

Default: 1
Specifies the frequency that passwords can be changed (other than first login).
`days` is the minimum number of days that must pass before a user can change their password. It is an integer from 1 through 365.

**Important:** If the `no local-user password min-change-interval` command is used, users may change their password as often as desired which could allow them to circumvent the password history function.

```
[ min-length number ]
```

Default: 8
Specifies the minimum length allowed for user-defined password.
`number` is the minimum number of alphanumeric characters that the password must contain, entered as an integer from 3 through 32.
Usage
This command is used to set the property requirements for user-defined passwords and system behavior in relation to those passwords. Information pertaining to user passwords, login failures, and password history are stored on the packet processing cards and in the software’s Shared Configuration Task (SCT). The system uses the information in the SCT for runtime operations such as determining password ages and determining if new passwords meet the criteria specified by this command.

Example
The following command configures a minimum password length requirement of 6 characters:

```
local-user password min-length 6
```

The following command configures the system to store the 4 most recently used passwords per user-account in the history list:

```
local-user password history length 4
```
local-user username

Adds or removes local-user administrative accounts.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

local-user username name [ authorization-level { administrator | inspector | operator | security-admin } ] [ ecs | noecs ] [ ftp | noftp ] [ timeout-min-absolute time ] [ no-lockout-login-failure ] [ no-lockout-password-aging ] [ password password | nopassword ] [ timeout-min-idle time ]

no local-user username name

no

Removes a previously configured user.

name

Specifies the name of the user as an alphanumeric string of 3 through 16 characters that is case sensitive.

[ authorization-level { administrator | inspector | operator | security-admin } ]

Default: Operator

Configures the authorization level for the user as one of the following:

• administrator: Administrator users have read-write privileges and can execute any command throughout the CLI except for a few security functions allowed only in the administrator mode. Administrators can configure or modify the system and are able to execute all system commands, including those available to the operator and inspector user. This level corresponds to the both the System Administrator and Application Administrator levels in the T1.276-2003.

• inspector: Inspector users are limited to a small number of read-only Exec Mode commands. The bulk of these are “show” commands giving the inspector the ability to view a variety of statistics and conditions. The Inspector cannot execute show configuration commands and do not have the privilege to enter the Config Mode.

• operator: Operator users have read-only privileges to a larger subset of the Exec Mode commands as depicted in the following figure. Operator users can execute all commands that are part of the inspector mode, plus some system monitoring, statistical, and fault management functions. Operators do not have the ability to enter the Config Mode.
• **security-admin**: Security Administrator users have read-write privileges and can execute any command throughout the CLI. Security Administrators can execute all system commands, including those available to the administrator, operator, and inspector users. This level corresponds to both the System Security Administrator and Application Security Administrator levels in T1.276-2003.

```plaintext
[ ecs | noecs ]
```

Specifies whether or not the user has access to Active Charging Service configuration parameters.
- **ecs**: The user has access.
- **noecs**: The user does not have access.

Default: **ecs**

```plaintext
[ ftp | noftp ]
```

Default: **ftp**

Specifies whether or not the user is allowed to access the system via the File Transfer Protocol (FTP) and/or the Secure File Transfer Protocol (SFTP).
- **ftp**: The user has access.
- **noftp**: The user does not have access.

```plaintext
[ no-lockout-login-failure ]
```

Default: **Disabled**

Specifies that this user will never be locked out due to login attempt failures.

```plaintext
[ no-lockout-password-aging ]
```

Default: **Disabled**

Specifies that this user will never be locked out due to the age of their password.

```plaintext
[ password password | nopassword ]
```

Specifies the initial password for this user. **password** must an alphanumeric string of 6 through 32 characters that is case sensitive.

**Important**: The user is requested to change their password upon their first login.

```plaintext
[ timeout-min-absolute time ]
```

Default: **0**

Specifies the maximum session time (in minutes) for this user. **time** is an integer from 0 through 525600. A value of “0” indicates no limit.

**Important**: This limit applies only to the user’s CLI sessions.

```plaintext
[ timeout-min-idle time ]
```

Default: **0**

Specifies the maximum idle time (in minutes) for this user. **time** is an integer from 0 through 525600. A value of “0” indicates no limit.
**Global Configuration Mode Commands (L-S)**

**local-user username**

- **Usage**
  - The ability to configure administrative local-users is provided in support of the login security mechanisms specified in ANSI T1.276-2003.
  - Like administrative users configured at the context level, local-users can be assigned one of 4 security levels:

<table>
<thead>
<tr>
<th>Local-User Level User</th>
<th>Context Level User</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Administrator</td>
<td>Administrator</td>
</tr>
<tr>
<td>Administrator</td>
<td>Config-Administrator</td>
</tr>
<tr>
<td>Operator</td>
<td>Operator</td>
</tr>
<tr>
<td>Inspector</td>
<td>Inspector</td>
</tr>
</tbody>
</table>

- Local-user configuration support is handled differently from that provided for administrative users configured at the context level.
  - Context-level administrative users rely on the system’s AAA subsystems for validating user names and passwords during login. This is true for both administrative user accounts configured locally through a configuration file or on an external RADIUS server. Passwords for these user types are assigned once and are accessible in the configuration file.
  - Local-user account information (passwords, password history, lockout states, etc.) is maintained in non-volatile memory and in the software’s Shared Configuration Task (SCT). This information is maintained in a separate file – not in configuration files used by the system. As such, the configured local-user accounts are not visible with the rest of the system configuration.
  - Local-user and context-level administrative accounts can be used in parallel.

- **Example**
  - The following command configures a security-administrator level local-user administrative account for a user named *User672* that has FTP privileges, a temporary password of *abc123*, and that does not lockout due to either login attempt failures or password aging:

    ```
    local-user username User672 authorization-level security-admin ftp no-lockout-login-failure no-lockout-password-aging password abc123
    ```

  - The following command deletes a previously configured local-user administrative account called admin32:

    ```
    no local-user username admin32
    ```

**Important:** This limit applies only to the user’s CLI sessions.
**logging console**

Enables the output of logged events to be displayed on the console terminal.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration

**Syntax**

[ no ] logging console

no

Disables the output of events to the console port.

**Usage**

Log console output to allow for offline review during system monitoring and/or trouble shooting.
logging disable

Enables/disables the logging of the specified event ID or range of IDs.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

**Configure**
Entering the above command sequence results in the following prompt:

```
[local] host_name(config)#
```

**Syntax**

```
logging disable eventid id [ to to_id ]
no logging disable eventid id [ to to_id ]
```

- **no**
  Indicates the event IDs specified are to be enabled for logging.

- **eventid id**
  Specifies the event for which no logging is to occur.
  In 14.1 and earlier releases, *id* is an integer from 1 through 202699.
  In 15.0 and later releases, *id* is an integer from 1 through 204999.

- **to to_id**
  Specifies the end ID of the events when a range of event ID is to be disabled from being logged. *to_id* must be an integer from 1 through 204999. The *to_id* must be equal to or larger than the *id* specified.

**Usage**

Disable common events which may occur with a normal frequency are not of interest in monitoring the system for troubles.

**Example**

The following commands disables the logging of event ID 4580 and the range of events from 4500 through 4599, respectively.

```
logging disable eventid 4580 4580
logging disable eventid 4500 to 4599
```

The following enables the subset of disabled event IDs:

```
no logging disable eventid 4500 to 4549
```
logging display

Configures the level of detail for information to be logged.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

```bash
configure
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```bash
logging display event-verbosity evt_level ] [ pdu-data format ] [ pdu-verbosity pdu_level ]
```

- `event-verbosity evt_level`
  Specifies the level of verboseness to use in logging of events as one of:
  - min
  - concise
  - full

- `pdu-data format`
  Specifies output format for packet data units when logged as one of:
  - none: outputs in raw format
  - hex: displays out in hexadecimal format
  - hex-ascii: displays output in hexadecimal and ASCII similar to a main-frame dump

- `pdu-verbosity pdu_level`
  Specifies the level of verboseness to use in logging of packet data units as an integer from 1 through 5, where 5 is the most detailed.

**Usage**

Tune the level of information to be logged so as to avoid flooding a log file with information which is not useful or critical.

**Example**

The following sets the logging display for events to the maximum.

```bash
logging display event-verbosity full
```

The following command sets the logging display level of detail for packet data units to level 3 and sets the output format to the main-frame style hex-ascii:
logging display pdu-data hex-ascii pdu-verbosity 3
logging filter

Configures the logging of events to be performed in real time for the specified facility.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

```bash
configure
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```bash
logging filter runtime facility facility level report_level [ critical-info | no-critical-info ]
```

```bash
facility facility
```

Specifies the facility to modify the filtering of logged information. The following list displays the valid facilities for this command:

- **a10**: A10 interface facility
- **a11**: A11 interface facility
- **a11mgr**: A11 Manager facility
- **aaa-client**: Authentication, Authorization and Accounting (AAA) client facility
- **aaamgr**: AAA manager logging facility
- **aaaproxy**: AAA Proxy facility
- **aal2**: ATM Adaptation Layer 2 (AAL2) protocol logging facility
- **acl-log**: Access Control List (ACL) logging facility
- **ascctrl**: Active Charging Service (ACS) Controller facility
- **acsmgr**: ACS Manager facility
- **afctrl**: Fabric Controller facility [ASR 5500 only]
- **afmgr**: Fabric Manager logging facility [ASR 5500 only]
- **alarmctrl**: Alarm Controller facility
- **alcap**: Access Link Control Application Part (ALCAP) protocol logging facility
- **alcapmgr**: ALCAP manager logging facility
- **all**: All facilities
- **asngwmg**: Access Service Network (ASN) Gateway Manager facility
- **asnpcmgr**: ASN Paging Controller Manager facility
- **bfd**: Bidirectional Forwarding Detection (BFD) protocol logging facility
- **bgp**: Border Gateway Protocol (BGP) facility
- **bindmux**: IPCF BindMux-Demux Manager logging facility
- **bngmgr**: Broadband Network Gateway (BNG) Demux Manager logging facility
- **bssap+**: Base Station Sub-system Application Part+ protocol facility for the login interface between the SGSN and the MSC/VLR (2.5G and 3G)
- **bssgp**: Base Station Sub-system GPRS Protocol logging facility handles exchange information between the SGSN and the BSS (2.5G only)
- **callhome**: Call Home application logging facility
- **cap**: CAMEL Application Part (CAP) logging facility for protocol used in prepaid applications (2.5G and 3G)
- **cbsmgr**: Cell Broadcasting Service (CBS) logging facility [HNBGW]
- **cdf**: Charging Data Function (CDF) logging facility
- **cgw**: Converged Access Gateway (CGW) logging facility
- **cli**: Command Line Interface (CLI) logging facility
- **cmp**: Certificate Management Protocol (IPSec) logging facility
- **connectedapps**: SecGW ASR 9000 oneP communication protocol
- **connproxy**: Controller Proxy logging facility
- **credit-control**: Credit Control (CC) facility
- **cscf**: IMS/MMD Call Session Control Function (CSCF)
- **cscfcpmgr**: CSCFCPMGR logging facility
- **cscfmgr**: SIP CSCF Manager facility
- **cscfnpdb**: CSCF Number Portability Database (NPDB) logging facility
- **cscfrtcp**: IMS/MMD CSCF RTCP log facility
- **cscfrtp**: IMS/MMD CSCF RTP log facility
- **cscfttmgr**: SIP CSCF Tunnel and Transport Manager facility
- **csp**: Card/Slot/Port controller facility
- **css**: Content Service Selection (CSS) facility
- **css-sig**: CSS RADIUS Signaling facility
- **cx-diameter**: Cx Diameter Messages facility [CSCF <-> HSS]
- **dcardctrl**: IPSec Daughter Card Controller logging facility
- **dcardmgr**: IPSec Daughter Card Manager logging facility
- **demuxmgr**: Demux Manager API facility
- **dgmnbmgr**: Diameter Gmb Application Manager logging facility
- **dhcp**: Dynamic Host Configuration Protocol (DHCP) logging facility
- **dhcpv6**: DHCPv6
- **dhost**: Distributed Host logging facility
- **diabase**: Diabase messages facility
- **diameter**: Diameter endpoint logging facility
Global Configuration Mode Commands (L-S)

- **diameter-acct**: Diameter Accounting
- **diameter-auth**: Diameter Authentication
- **diameter-dns**: Diameter DNS subsystem
- **diameter-ecs**: ACS Diameter signaling facility
- **diameter-hdd**: Diameter Horizontal Directional Drilling (HDD) Interface facility
- **diameter-svc**: Diameter Service
- **diamproxy**: DiamProxy logging facility
- **dpath**: IPSec Data Path facility
- **drvctrl**: Driver Controller facility
- **doulosuemgr**: Doulos (IMS-IPSec-Tool) user equipment manager
- **eap-diameter**: Extensible Authentication Protocol (EAP) IPSec facility
- **eap-ipsec**: Extensible Authentication Protocol (EAP) IPsec facility
- **eap-sta-s6a-s13-s6b-diameter**: EAP/STA/S6A/S13/S6B Diameter messages facility
- **ecs-ess**: ACSMGR <-> Session Manager Signalling Interface facility
- **egtpc**: eGTP-C logging facility
- **egtpmgr**: enhanced GPRS Tunneling Protocol (eGTP) manager logging facility
- **egtpu**: eGTP-U logging facility
- **epdg**: evolved Packet Data (ePDG) gateway logging facility
- **event-notif**: Event Notification Interface logging facility
- **evlog**: Event log facility
- **famgr**: Foreign Agent manager logging facility
- **firewall**: Firewall logging facility
- **fng**: Femto Network Gateway (FNG) logging facility
- **gbmgr**: SGSN Gb Interface Manager facility
- **gmm**:  
  - For 2.5G: Logs the GPRS Mobility Management (GMM) layer (above LLC layer)  
  - For 3G: Logs the access application layer (above the RANAP layer)
- **gprs-app**: GPRS Application logging facility
- **gprs-ns**: GPRS Network Service Protocol (layer between SGSN and the BSS) logging facility
- **gq-rx-tx-diameter**: Gq/Rx/Tx Diameter messages facility
- **gss-gcdr**: GTPP Storage Server GCDR facility
- **gtpc**: GTP-C protocol logging facility
- **gtpcmgr**: GTP-C protocol manager logging facility
- **gtp**: GTP-prime protocol logging facility
- **gtpu**: GTP-U protocol logging facility
- **gtpumgr**: GTP-U Demux manager
- **gx-ty-diameter**: Gx/Ty Diameter messages facility
• gy-diameter: Gy Diameter messages facility
• h248prt: H.248 port manager facility
• hamgr: Home Agent manager logging facility
• hat: High Availability Task (HAT) process facility
• hdctrl: HD Controller logging facility
• henhapp: Home Evolved NodeB (HENB) App facility
• henhgw: HENB-GW facility
• henhgw-pws: HENB-GW Public Warning System logging facility
• henhgw-sctp-acs: HENB-GW access Stream Control Transmission Protocol (SCTP) facility
• henhgw-sctp-nw: HENBGW network SCTP facility
• henhgwdemux: HENB-GW Demux facility
• henhgwmgr: HENB-GW Manager facility
• hnb-gw: HNB-GW (3G Femto GW) logging facility
• hnbmgm: HNB-GW Demux Manager logging facility
• hss-peer-service: Home Subscriber Server (HSS) Peer Service facility
• igmp: Internet Group Management Protocol (IGMP)
• ikev2: Internet Key Exchange version 2 (IKEv2)
• ims-authoriztn: IP Multimedia Subsystem (IMS) Authorization Service facility
• ims-sh: HSS Diameter Sh Interface Service facility
• imsimgr: SGSN IMSI Manager facility
• imsue: IMS User Equipment (IMSUE) facility
• ip-arp: IP Address Resolution Protocol facility
• ip-interface: IP interface facility
• ip-route: IP route facility
• ipms: Intelligent Packet Monitoring System (IPMS) logging facility
• ipne: IP Network Enabler (IPNE) facility
• ipsec: IP Security logging facility
• ipsg: IP Service Gateway interface logging facility
• ipsgmgr: IP Services Gateway facility
• ipsp: IP Pool Sharing Protocol logging facility
• kvstore: Key/Value Store (KVSTORE) Store facility
• l2tp-control: Layer 2 Tunneling Precool (L2TP) control logging facility
• l2tp-data: L2TP data logging facility
• l2tpdemux: L2TP Demux Manager logging facility
• l2tpmgr: L2TP Manager logging facility
• lagmgr: Link Aggregation Group (LAG) manager logging facility
• lcs: Location Services (LCS) logging facility
• **ldap**: Lightweight Directory Access Protocol (LDAP) messages logging facility
• **li**: Refer to the *Lawful Intercept Interface Reference* for a description of this command.
• **linkmgr**: SGSN/BSS SS7 Link Manager logging facility (2.5G only)
• **llc**: Logical Link Control (LLC) Protocol logging facility; for SGSN: logs the LLC layer between the GMM and the BSSGP layers for logical links between the MS and the SGSN
• **local-policy**: Local Policy Service facility
• **location-service**: Location Services facility
• **m3ua**: M3UA Protocol logging facility
• **magmgr**: Mobile Access Gateway manager logging facility
• **map**: Mobile Application Part (MAP) protocol logging facility
• **megadiammgr**: MegaDiameter Manager (SLF Service) logging facility
• **mme-app**: Mobility Management Entity (MME) Application logging facility
• **mme-misc**: MME miscellaneous logging facility
• **mmedemux**: MME Demux Manager logging facility
• **mmemgr**: MME Manager facility
• **mmgr**: Master Manager logging facility
• **mobile-ip**: Mobile IP processes
• **mobile-ip-data**: Mobile IP data facility
• **mobile-ipv6**: Mobile IPv6 logging facility
• **mpls**: Multiprotocol Label Switching (MPLS) protocol logging facility
• **mrme**: Multi Radio Mobility Entity (MRME) logging facility
• **mseg-app**: Mobile Services Edge Gateway (MSEG) application logging facility (This option is not supported in this release.)
• **mseg-gtpc**: MSEG GTP-C application logging facility (This option is not supported in this release.)
• **mseg-gtpu**: MSEG GTP-U application logging facility (This option is not supported in this release.)
• **msegmgr**: MSEG Demux Manager logging facility (This option is not supported in this release.)
• **mtp2**: Message Transfer Part 2 (MTP2) Service logging facility
• **mtp3**: Message Transfer Part 3 (MTP3) Protocol logging facility
• **multicast-proxy**: Multicast Proxy logging facility
• **nas**: Non-Access Stratum (NAS) protocol logging facility [MME 4G]
• **netwstrg**: Network Storage facility
• **npuctrl**: Network Processor Unit Control facility
• **npudrv**: Network Processor Unit Driver facility [ASR 5500 only]
• **npumgr**: Network Processor Unit Manager facility
• **npumgr-acl**: NPUMGR ACL logging facility
• **npumgr-drv**: NPUMGR DRV logging facility
• **npumgr-flow**: NPUMGR FLOW logging facility
- `npumgr-fwd`: NPUMGR FWD logging facility
- `npumgr-init`: NPUMGR INIT logging facility
- `npumgr-lc`: NPUMGR LC logging facility
- `npumgr-port`: NPUMGR PORT logging facility
- `npumgr-recovery`: NPUMGR RECOVERY logging facility
- `npumgr-rri`: NPUMGR RRI (Reverse Route Injection) logging facility
- `npumgr-vpn`: NPUMGR VPN logging facility
- `npusim`: NPUSIM logging facility [ASR 5500 only]
- `ntfy-intf`: Notification Interface logging facility [Release 12.0 and earlier versions only]
- `orbs`: Object Request Broker System logging facility
- `ospf`: OSPF protocol logging facility
- `ospfv3`: OSPFv3 protocol logging facility
- `p2p`: Peer-to-Peer Detection logging facility
- `pagingmgr`: PAGINGMGR logging facility
- `pccegr`: Intelligent Policy Control Function (IPCF) Policy Charging and Control (PCC) Manager library
- `pdg`: Packet Data Gateway (PDG) logging facility
- `pdgdmgr`: PDG Demux Manager logging facility
- `pdif`: Packet Data Interworking Function (PDIF) logging facility
- `pgw`: Packet Data Network Gateway (PGW) logging facility
- `pmm-app`: Packet Mobility Management (PMM) application logging facility
- `ppp`: Point-To-Point Protocol (PPP) link and packet facilities
- `pppoe`: PPP over Ethernet logging facility
- `push`: VPNMGR CDR push logging facility
- `radius-acct`: RADIUS accounting logging facility
- `radius-auth`: RADIUS authentication logging facility
- `radius-coa`: RADIUS change of authorization and radius disconnect
- `ranap`: Radio Access Network Application Part (RANAP) Protocol facility logging info flow between SGSN and RNS (3G)
- `rct`: Recovery Control Task logging facility
- `rdt`: Redirect Task logging facility
- `resmgr`: Resource Manager logging facility
- `rf-diameter`: Diameter Rf interface messages facility
- `rip`: Routing Information Protocol (RIP) logging facility [RIP is not supported at this time.]
- `rlf`: Rate Limiting Function (RLF) logging facility
- `rohc`: Robust Header Compression (RoHC) facility
logging filter

• **rsvp**: Reservation Protocol logging facility
• **rua**: RANAP User Adaptation (RUA) [3G Femto GW - RUA messages] logging facility
• **s1ap**: S1 Application Protocol (S1AP) Protocol logging facility
• **sabp**: Service Area Broadcast Protocol (SABP) logging facility
• **saegw**: System Architecture Evolution (SAE) Gateway facility
• **sccp**: Signalling Connection Control Part (SCCP) Protocol logging (connection-oriented messages between RANAP and TCAP layers).
• **set**: Shared Configuration Task logging facility
• **sctp**: Stream Control Transmission Protocol (SCTP) Protocol logging facility
• **sef ecs**: Severely Errored Frames (SEF) APIs printing facility
• **sess-gr**: SM GR facility
• **sessctrl**: Session Controller logging facility
• **sessmgr**: Session Manager logging facility
• **sesstrc**: session trace logging facility
• **sft**: Switch Fabric Task logging facility
• **sgs**: SGs interface protocol logging facility
• **sgsn-app**: SGSN-APP logging various SGSN “glue” interfaces (for example, between PMM, MAP, GPRS-FSM, SMS).
• **sgsn-failures**: SGSN call failures (attach/activate rejects) logging facility (2.5G)
• **sgsn-gtpc**: SGSN GTP-C Protocol logging control messages between the SGSN and the GGSN
• **sgsn-gtpu**: SGSN GTP-U Protocol logging user data messages between the SGSN and GGSN
• **sgsn-mbms-bearer**: SGSN Multimedia Broadcast/Multicast Service (MBMS) Bearer app (SMGR) logging facility
• **sgsn-misc**: Used by stack manager to log binding and removing between layers
• **sgsn-system**: SGSN System Components logging facility (used infrequently)
• **sgsn-test**: SGSN Tests logging facility; used infrequently
• **sgtpcmgr**: SGSN GTP-C Manager logging information exchange through SGTPC and the GGSN
• **sgw**: Serving Gateway facility
• **sh-diameter**: Sh Diameter messages facility
• **sitmain**: System Initialization Task main logging facility
• **sm-app**: SM Protocol logging facility
• **sms**: Short Message Service (SMS) logging messages between the MS and the SMSC
• **sndep**: Sub Network Dependent Convergence Protocol (SNDCP) logging facility
• **snmp**: SNMP logging facility
• **sprmgr**: IPCF Subscriber Policy Register (SPR) manager logging facility
• **srdb**: Static Rating Database
• **srp**: Service Redundancy Protocol (SRP) logging facility
• **sscfnni**: Service-Specific Coordination Function for Signaling at the Network Node Interface (SSCF-NNI) logging facility
• **sscop**: Service-Specific Connection-Oriented Protocol (SSCOP) logging facility
• **ssh-ipsec**: Secure Shell (SSH) IP Security logging facility
• **ssl**: Secure Socket Layer (SSL) message logging facility
• **stat**: Statistics logging facility
• **supserv**: Supplementary Services logging facility [H.323]
• **system**: System logging facility
• **tacacplus**: TACACS+ Protocol logging facility
• **tcap**: TCAP Protocol logging facility
• **testctrl**: Test Controller logging facility
• **testmgr**: Test Manager logging facility
• **threshold**: threshold logging facility
• **ttg**: Tunnel Termination Gateway (TTG) logging facility
• **tucl**: TCP/UDP Convergence Layer (TUCL) logging facility
• **udr**: User Data Record (UDR) facility (used with the Charging Service)
• **user-data**: User data logging facility
• **user-l3tunnel**: User Layer 3 tunnel logging facility
• **usertcp-stack**: User TCP Stack
• **vim**: Voice Instant Messaging (VIM) logging facility
• **vinfo**: VINFO logging facility
• **vmgctrl**: Virtual Media Gateway (VMG) controller facility
• **vmgctrl**: VMG Content Manager facility
• **vpn**: Virtual Private Network logging facility
• **wimax-data**: WiMAX DATA
• **wimax-r6**: WiMAX R6
• **wsg**: Wireless Security Gateway (ASR 9000 Security Gateway)

```
level report_level [ critical-info | no-critical-info ]
```

**level report_level**: specifies the level of information to be logged, *report_level*, as one of:
• **critical**
• **debug**
• **error**
• **info**
• **trace**
• **unusual**
• **warning**
**logging filter**

**critical-info | no-critical-info**: indicates if critical information is to be displayed or not. The keyword `critical-info` specifies that events with a category attribute of critical information are to be displayed. Examples of these types of events can be seen at bootup when system processes and tasks are being initiated. The `no-critical-info` keyword specifies that events with a category attribute of critical information are not to be displayed.

**Usage**

This command is useful when it is necessary to get real-time output of events. Event output may be cached otherwise which may make it difficult to troubleshoot problems which do not allow the last cache of events to be output prior to system problems.

**Caution:** Issuing this command could negatively impact system performance depending on system loading, the log level, and/or the type of facility(ies) being logged.

**Example**

Set real time output for the point-to-point protocol facility and all facilities, respectively, to avoid logging of excessive information.

```
logging filter runtime facility ppp
logging filter runtime facility all level warning
```
logging monitor

Enables or disables the monitoring of a specified user.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

[ no ] logging monitor { ipaddr ip_address | ipv6addr ipv6_address | msid ms_id | username user_name }

no
Disables the monitoring of the user specified by the options given.

ipaddr ip_address
Specifies the IP address of the user for which the monitoring filter is to be set. ip_address must entered using IPv4 dotted-decimal notation.

ipv6addr ipv6_address
Specifies the IPv6 address of the user for which the monitoring filter is to be set. ipv6_address must be followed by IPv6 address in a xx:yy:zz format .

msid ms_id
msid ms_id: specifies the mobile subscriber ID for which the monitoring filter is to be set. ms_id must be from 7 to 16 digits.
This keyword/option can be used to specify the Mobile Subscriber ISDN (MSISDN) for GGSN calls which enables logging based on MSISDN.

username user_name
username user_name: specifies a user for which the monitoring filter is to be set. user_name must refer to a previously configured user.

Usage

Monitor subscribers which have complaints of service availability or to monitor a test user for system verification.
**Caution:** Issuing this command could negatively impact system performance depending on the number of subscribers for which monitoring is performed and/or the amount of data they’re passing.

**Example**

The following command enables the monitoring of user `user1` and mobile subscriber ID 4441235555, respectively.

```sh
logging monitor username user1
logging monitor msid 4441235555
```

The following disables the monitoring of user `user1`.

```sh
no logging monitor username user1
```
logging runtime

Enables events to be filtered and logged in real time.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

logging runtime buffer store { all-events | filtered-events-only }

buffer store { all-events | filtered-events-only }

Determines which logs are stored in internal logging daemon runtime buffer.

*all-events*: Logging daemon runtime buffer stores all logs that come to it.

*filtered-events-only*: Logging daemon runtime buffer stores only logs that pass the runtime filter.

Usage
Sets the filtering of logged information to log in real time.

Example
The following command enables storage of logs that pass the runtime filter:

 logging runtime buffer store filtered-events-only
**lte-policy**

This command enters the LTE Policy Configuration Mode where LTE policy parameters can be configured.

**Product**
- MME
- SAEGW
- S-GW
- SGSN

**Privilege**
- Administrator

**Mode**
- Exec > Global Configuration
  - `configure`

Entering the above command sequence results in the following prompt:

```
[local] host_name(config)#
```

**Syntax**

```
lte-policy
```

**Usage**

Enters the LTE Policy Configuration Mode.

Entering this command results in the following prompt:

```
[context_name] hostname(lte-policy)#
```

LTE Policy Configuration Mode commands are defined in the *LTE Policy Configuration Mode Commands* chapter.
**mediation-device**

This command is obsolete. Even though the CLI accepts the command no function is performed.

**Product**
- GGSN

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration
  - `configure`

Entering the above command sequence results in the following prompt:

```
[local] host_name(config) #
```

**Syntax**

```
[ no ] mediation-device mode { tcs }
```
mobile-services-edge-gateway

This command is not supported in this release.
network-overload-protection mme-new-connections-per-second

This command configures an attach rate throttle mechanism to control the number of new connections allowed on a per-second basis.

**Product**
MME

**Privilege**
Administrator

**Mode**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```plaintext
network-overload-protection mme-new-connections-per-second #_new_connections action
attach { drop | reject-with-emm-cause { congestion | network-failure | no-suitable-cell-in-tracking-area } } tau { drop | reject-with-emm-cause { congestion | network-failure | no-sec-ctxt-in-nw | no-suitable-cell-in-tracking-area } } fwd-reloc { drop | reject } [ queue-size queue_size ] [ wait-time wait_time ]
```

**default network-overload-protection mme-new-connections-per-second**

- **default**
  Disables the MME attach rate throttle feature.

- **mme-new-connections-per-second #_new_connections**
  Define the number of new connections to be accepted per second.
  `#_new_connections`: Must be an integer from 50 to 5000.

- **action**
  Specifies the action to be taken by the MME when the new connection queue is full. Specific actions can be defined for each of the following connection types:
  - **UE-initiated attaches** (see `attach` keyword).
  - **UE-initiated inter-CN node TAU requests** (see `tau` keyword).
  - **Peer SGSN/MME initiated forward relocation requests** (see `fwd-reloc` keyword).

```plaintext
attach { drop | reject-with-emm-cause { congestion | network-failure | no-suitable-cell-in-tracking-area } }
```

Specifies the action to be taken for all types of UE-initiated initial attaches (IMSI, local GUTI, foreign GUTI, mapped GUTI, etc.). Select one of the following actions:

- **drop**: Drop the new connection request.
**reject-with-cause**: Reject the new connection request. Include one of the following as the cause in the reject message:

- congestion
- network-failure
- no-suitable-cell-in-tracking-area

```
tau { drop | reject-with-emm-cause { congestion | network-failure | no-sec-ctxt-in-nw | no-suitable-cell-in-tracking-area } }
```

Specifies the action to be taken for UE-initiated inter-CN TAU requests requiring context transfer from old MME/SGSN, including TAU requests with foreign GUTI or mapped GUTI. Select one of the following actions:

- **drop**: Drop the new connection request.
- **reject-with-cause**: Reject the new connection request. Include one of the following as the cause in the reject message:
  - congestion
  - network-failure
  - no-sec-ctxt-in-nw
  - no-suitable-cell-in-tracking-area

```
fwd-reloc { drop | reject }
```

Specifies the action to be taken for peer SGSN/MME initiated forward relocation requests via Gn/S10/S3. Select one of the following actions:

- **drop**: Drop the new connection request.
- **reject**: Reject the new connection request. If the inbound forward-relocation requests are rejected, the following cause codes shall be used:
  - GTPv1 - No resources available (199)
  - GTPv2 - No resources available (73)

In the event of an MME failure, the surviving MME in the pool may receive a very large number of IMSI requests, which may overwhelm the IMSI Manager. To avoid congestion, the MME can be configured using this keyword to throttle the IMSI-based DDN requests it receives if the configured #new_connections rate is exceeded. Select one of the following actions:

- **drop**: Drop new IMSI-based DDN requests.
- **reject**: Reject the IMSI-based DDN request. Include one of the following as the cause in the reject message:
  - unable-to-page-ue
  - context-not-found
Global Configuration Mode Commands (L-S)

network-overload-protection mme-new-connections-per-second

queue-size  queue_size
Defines the maximum size of the pacing queue used for buffering the packets. If configured, the queue-size should be greater than or equal to the #_new_connections value and less than or equal to the optimal value (the wait_time * #_new_connections). This validation is done in the CLI.
queue_size Must be an integer from 250 to 25000.
Default: unconfigured. The default value is the #_new_connections * wait-time. This will be the optimal value.

wait-time  wait_time
Defines the maximum life-time (number of seconds) of the packets in the queue beyond which the packets are considered to be “stale” and are dropped.
wait_time Must be an integer from 1 to 15
Default: 5

Usage
Use this command to configure attach rate throttling on the MME.
When enabled, new connections (except emergency requests) are buffered and paced through the queue. Messages in the queue are processed (FIFO) until they age-out when the queued message's lifetime crosses the configured wait-time. The wait-time and the attach rate decide the optimal size of the queue. If the queue is full, packets are rejected or dropped based on the configured action.
This feature functions at a system (chassis) level for all MME services. All MME services on the system are controlled by a single pacing queue. For a combo MME-SGSN node, each type of service shall be controlled by its own queue and its own configuration.
Emergency attaches are not be throttled when this feature is enabled.

Important: This command is available only if a valid license (MME Resiliency) is installed. Contact your Cisco account representative for more information.

Example
Configure the new connections per second rate at 2500, reject all (non-emergency) attaches and TAU requests, and drop forward relocation requests if the new connection rate is exceeded. Rejects will return emm cause code “Congestion”.

    network-overload-protection mme-new-connections-per-second 2500 action
    attach reject-with-emm-cause congestion tau reject-with-emm-cause
    congestion fwd-reloc drop ddn drop wait-time 5

Set the attach rate to 500 per second, the same actions as the previous example, but set the wait time to 5 seconds, and the queue size to be calculated (as follows: wait_time * #_new_connections - i.e., 2500)

    network-overload-protection mme-new-connections-per-second 500 action
    attach reject-with-emm-cause congestion tau reject-with-emm-cause
    congestion fwd-reloc drop ddn drop wait-time 5 5
network-overload-protection sgsn-new-connections-per-second

This command configures an attach rate throttle mechanism to control the number of new connections (attaches or inter-SGSN RAUs), through the SGSN, on a per second basis.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
network-overload-protection sgsn-new-connections-per-second #_new_connections action { drop | reject with cause { congestion | network failure } } [ queue-size queue_size ] [ wait-time wait_time ]

default network-overload-protection sgsn-new-connections-per-second

default
```

Using `default` in the command, disables this attach rate throttle feature that provides network overload protection.

```
sgsn-new-connections-per-second #_new_connections
```

Define the number of new connections to be accepted per second.

`#_new_connections`: Must be an integer from 50 to 5000.

**action**

Specifies the action to be taken by the SGSN when the attach rate exceeds the configured limit on the number of attaches. Select one of the following actions:

- **drop**: Drop the new connection request.
- **reject-with-cause**: Reject the new connection request. Include one of the following as the cause in the reject message:
  - **congestion**
  - **network failure**

**queue-size queue_size**

Defines the maximum size of the pacing queue used for buffering the packets. If configured, the queue-size should be greater than or equal to the `#_new_connections` value and less than or equal to the optimal value (the `wait_time` * `#_new_connections`). This validation is done in the CLI.

`queue_size` Must be an integer from 250 to 25000.
Global Configuration Mode Commands (L-S)

network-overload-protection sgsn-new-connections-per-second

Default: unconfigured. The default value is the \( \# \_new \_connections \times wait \_time \). This will be the optimal value.

**wait-time wait_time**

Defines the maximum life-time (number of seconds) of the packets in the queue beyond which the packets are considered to be "stale".

*wait_time* Must be an integer from 1 to 15

Default: 5

**Usage**

Use this command to configure the rate at which the SGSN must process new connection requests. The rate is the number of new connections to be accepted per second.

With basic network overload protection, the incoming new connection rate is higher than this configured rate. When this occurs, all of the new connection requests cannot be processed. This command can also be used to configure the action to be taken when the rate limit is exceeded. The new connection requests, which cannot be processed, can be either dropped or rejected with a specific reject cause.

The SGSN’s *optimized* network overload protection performs attach-rate throttling to avoid overloading Gr, Gn, and Gf interfaces. This is enabled with queue-size and wait-time keywords so that the IMSIMgr throttles the attach rate to values configured with these keywords.

If the SGSN receives more than the configured number of attaches in a second, then the attaches are buffered in the pacing queue and requests are only dropped when the buffer overflows due to high incoming attach rate. Messages in the queue are processed (FIFO) until they age-out when the queued message's lifetime crosses the configured wait-time. The wait-time and the attach rate decide the optimal size of the queue.

Counters for this feature are available in the `show gmm-sm statistics` command display in the Network Overload Protection portion of the table.

**Example**

Configure the throttle rate or limit to 2500 attaches per second and to drop all requests if the limit is exceeded.

```
network-overload-protection sgsn-new-connections-per-second 2500 action drop
```

Disables the network-overload protection feature and set the default queue size to 1000 and the wait time to 5 seconds:

```
default network-overload-protection sgsn-new-connections-per-second
```

Set the attach rate to 500 per second, the action to drop, the wait time to 5 seconds, and the queue size to be calculated (as follows: `wait_time * \#_new_connections` e.g., 2500)

```
network-overload-protection sgsn-new-connections-per-second 500 action drop wait-time 5
```
network-service-entity

This command creates a new instance of an SGSN network service entity (NSE) for either the IP environment or the Frame Relay environment.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

```
configure
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config)#
```

**Syntax**

```
[ no ] network-service-entity ( ip-local | peer-nsei peer_nsei_number frame-relay )
```

<table>
<thead>
<tr>
<th><strong>no</strong></th>
<th>Deletes the network service entity definition from the system configuration.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ip-local</strong></td>
<td>Configures the local endpoint for NS/IP and enters the NSE-IP configuration mode. The prompt will change to:</td>
</tr>
<tr>
<td><code>no</code></td>
<td><code>[local]&lt;hostname&gt;(nse-ip-local)#</code></td>
</tr>
</tbody>
</table>

| **peer-nsei peer_nsei_number frame-relay** | Configures a peer NSE with frame relay connectivity. This set of keywords also provides access to the NSE-FR Configuration mode. The prompt will change to: |
| `no` | `[local]<hostname>(nse-fr-peer-nsei=<peer_nsei_number>)#` |

**Usage**

Use this command to access the configuration modes for either the IP or Frame Relay network service entities.

**Example**

Enter the NSE for a Frame Relay configuration instance identified as 4554:

```
network-service-entity peer-nsei 4554 frame-relay
```
network-service-entity ip

This command has been deprecated. See the replacement command network-service-entity.
**ntp**

Enters the Network Time Protocol (NTP) configuration mode or disables the use of NTP on the system.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration

```console
configure
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config) #
```

**Syntax**

```
[ no ] ntp
```

- **no**

  Disables the use of NTP for clock synchronization. When omitted, NTP client support is enabled on the chassis. By default NTP synchronization to external servers is disabled.

**Important:** If the use of NTP is disabled the system clock may drift over a period of time. This may require manual updates to the system clock to synchronize the clock with other network elements.

**Usage**

Used when it is necessary to enable or configure NTP settings. For additional information refer to the *NTP Configuration Mode Commands* chapter and the *System Administration Guide*.

**Example**

The following command enters the NTP configuration mode:

```console
ntp
```

The following disables the use of the network timing protocol for system clock synchronization.

```console
no ntp
```
**ntsr pool-id**

Configures a pool ID and pool type (either MME or S4-SGSN) for Network Triggered Service Restoration (NTSR). Once executed, the user is placed in NTSR Pool Configuration Mode.

### Product
S-GW

### Privilege
Administrator, Security Administrator

### Mode
Exec > Global Configuration  
**configure**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

### Syntax

```
ntsr pool-id number pool-type [ mme | s4-sgsn ]
```

```
no ntsr pool-id
```

```
ntsr pool-idnumber
```

Specifies an ID number for this NTSR pool. Valid entries are from 1 to 65535.

```
pool-type
```

Specifies the type of pool for the pool-id. Options are MME or S4-SGSN.

### Usage

This command is used to configure a pool ID and pool type (either MME or S4-SGSN) for NTSR. Once executed, the operator must configure a peer IP address in NTSR Pool Configuration mode using the **peer-ip-address** command.

### Example

This example configures an NTSR pool ID of 1 and a pool type of mme.

```
ntsr pool-id 1 pool-type mme
```
operator-policy

This command creates an operator policy and enters the operator policy configuration mode. Commands for configuration of the policies are available in the Operator Policy Configuration Mode Commands chapter.

**Product**
- MME
- SGSN
- SAEGW
- S-GW

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration
- `configure`

Entering the above command sequence results in the following prompt:

```
[local] host_name(config)#
```

**Syntax**

```
operator-policy ( default | name policy_name ) [ -noconfirm ]

no operator-policy ( default | name policy_name )
```

- `-noconfirm`
  Indicates that the command is to execute without any additional prompt and confirmation from the user.

- `no`
  Removes the specified operator policy from the system configuration.

- `default`
  `default`, in this case, is the name of a specific operator policy. This default policy is used when no other defined operator policy matches the incoming IMSI.

**Important:** You should configure this default operator policy to be it available to handle IMSIs that are not matched with other defined policies.

- `name policy_name`
  Specifies the unique name of an operator policy. `policy_name` is entered as an alphanumeric string of 1 through 64 characters.
Usage

Use this command to create an operator policy and to enter the operator policy configuration mode to define or modify policies.

An operator policy associates APNs, APN profiles, IMEI ranges, IMEI profiles, an APN remap table and a call-control profile to ranges of IMSIs. These profiles and tables are created and defined within their own configuration modes to generate sets of rules and instructions that can be reused and assigned to multiple policies. In this manner, an operator policy manages the application of rules governing the services, facilities and privileges available to subscribers. These policies can override standard behaviors and provide mechanisms for an operator to get around the limitations of other infrastructure elements such as DNS servers and HLRs.

The system supports up to 1,000 operator policies, including the default operator policy.

Important: An operator policy is the key element of the Operator Policy feature. After defining an instance of an operator policy, you must go to the SGSN Global Configuration Mode (from the Global Configuration mode) to define the IMSI range(s). This requirement does not hold if you are using a default operator policy.

To see what operator policies have already been created, return to the Exec mode and enter the show operator-policy all command.

Example

The following command accesses the default operator policy and enters the operator policy configuration mode to view or modify the specified policy:

```
operator-policy default
```
orbem

Enters the Object Request Broker Element Manager (ORBEM) Configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

```
[local] host_name(config) #
```

**Syntax**

```
orbem
```

**Usage**
Set the configuration mode to allow modification of the ORBEM configuration data.
pac-standby-priority

This command has been renamed to card-standby-priority. Please refer to that command for details. Note that for backwards compatibility, the system accepts this command as valid.
peer-profile

This command creates a peer profile based on service type and interface and enters the Peer-Profile Configuration mode. Commands for configuration of the policies are available in the Peer Profile Configuration Mode Commands chapter.

Product

GGSN
P-GW
SAEGW
S-GW

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

peer-profile service-type { ggsn-access | pgw-access | sgw-access | sgw-network } { default | name peer_profile_name } [ -noconfirm ]

no peer-profile service-type { ggsn-access | pgw-access | sgw-access | sgw-network } name peer_profile_name

[ -noconfirm ]

Indicates that the command is to execute without any additional prompt and confirmation from the user.

no

Removes the specified peer profile for specific service type from the system configuration.

service-type

Specifies service type for which peer profile is being configured.

\textbf{ggsn-access} configure profile for peer nodes of GGSN.

\textbf{pgw-access} configures profile for peer nodes of P-GW.

\textbf{sgw-access} configures profile for peer nodes of S-GW toward S4/S11 interfaces.

\textbf{sgw-network} configures profile for peer nodes of S-GW toward S5/S8 interfaces.

name peer_profile_name

Specifies the unique name of a peer profile for specific service type.

\textit{peer_profile_name} is entered as an alphanumeric string of 1 through 64 characters.
default

`default`, in this case, is the name of a specific peer profile. This default profile is used when no other defined peer profile matches.

**Important:** When there is no association of peer-map in any of the services, then “default” peer profile of the corresponding service-interface type shall be applied, except for GTP-C parameters. In addition, GTP-C parameter configuration shall be applied from eGTP service-level configuration for P-GW/S-GW service and GGSN service-level configuration for GGSN.

### Usage

Use this command to create a peer profile for specific service type and to enter the service specific Peer Profile configuration mode to define or modify the peer profile parameters.

The peer profile feature allows flexible profile-based configuration to accommodate growing requirements of customizable parameters with default values and actions for peer nodes of GGSN/P-GW/S-GW. With this feature, configuration of GTP-C echo parameters and disabling/enabling of Lawful intercept per MCC/MNC or IP address based on rules can be managed.

Before StarOS Release 15.0, the GGSN service allowed operator to configure list of SGSNs. Using this configuration, operator can also control some parameters associated with the configured SGSN, such as RAT type. This would be taken from configuration if CPC request does not have RAT type.

**Important:** The system supports up to 64 peer profiles configured for each of the peer profile types; there can be up to 1024 peer map rules configured, including all the peer maps.

### Example

The following command accesses the default peer profile for GGSN service and enters the GGSN Peer Profile configuration mode to view or modify the specified profile:

```
peer-profile service-type ggsn-access default
```
**plugin**

Specifies a previously installed software plugin module and enters the Plugin Configuration Mode. This function is associated with the patch process for dynamic software upgrades. A plugin module is a loadable dynamic link library (DLL) of shared objects.

**Product**
ADC

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local] host_name(config)#
```

**Syntax**

```
plugin module_name
```

*module_name*

Specifies the name of an existing plugin module that you want to downgrade as an alphanumeric string of 1 through 16 characters. If the named module is not known to the system, an error message is displayed.

**Usage**

Specify a previously loaded software plugin module that you wish to configure. The specified module must have been previously copied onto the system and unpacked/verified via the `patch plugin` and `install patch plugin` commands.

For additional information, refer to the `Plugin Configuration Mode Commands` chapter.

**Example**

To specify the plugin module named `p2p_odyssey` enter the following command:

```
plugin p2p_odyssey
```
**port atm**

Identifies a physical port on a line card that supports ATM signaling and then enters the configuration mode for the specific interface-type. For the commands to configure the port interface, see the CLI chapter ATM Port Configuration Mode.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

*configure*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
port atm slot/port
```

- **atm**
  Indicates the port identified is an ATM interface port.

- **slot/port**
  To determine valid ATM slot and port numbers, use the Exec mode’s command `show port table slot`.

  - **slot**: Identifies the chassis slot holding the line card that supplies ATM ports. The slot ID number can be an integer from 17 through 48.
  - **port**: Identifies the physical port that is to be configured to support ATM signaling. The ID number can be an integer from 1 through 4.

**Usage**

Change the current configuration mode to Ethernet Port Configuration mode.

**Important**: This command is not supported on all platforms.

**Example**

The following enters the ATM port configuration mode for ATM port 1 on the card in slot 19:

```
port atm 19/1
```
**port bits**

Enters the Building Integrated Timing Supply (BITS) port configuration mode by identifying the BITS port on the active or standby SPIO.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

**Syntax**

```plaintext
port bits slot/port
```

**Usage**
Change the current configuration mode to BITS port configuration mode.

**Important:** This command is not supported on all platforms.

**Example**
The following enters the BITS port configuration mode for the active SPIO:

```plaintext
port bits 24/4
```
port channelized

Identifies a physical port on a Channelized Line Card (CLC) that supports Frame Relay signaling and creates a Frame Relay interface. This command enters the configuration mode for the commands that configure the Frame Relay interface and the channelized port interface. For additional information, see the Channelized Port Configuration Mode Commands chapter.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

```
port channelized slot/port
```

channelized
Selects the channelized frame relay interface for the selected line card and port.

```
slot/port
```

To determine valid slots and port numbers, use the Exec mode’s command `show port table` to find the channelized line card.

- `slot`: Identifies the chassis slot holding the Channelized Line Card that sources Frame Relay ports. The slot ID number can be an integer from 17 through 48.
- `port`: Identifies the physical port that is to be configured to support Frame Relay signaling. The ID number can only be 1.

Usage

Change the current configuration mode to Channelized Port configuration mode.

Example

The following enters the Channelized port configuration mode for port 1 on the card in slot 20:

```
port channelized 20/1
```
port ethernet

Enters the Ethernet Port Configuration mode for the identified port.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

```
configure
```
Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
port ethernet slot/port
```

- **ethernet**
  Indicates the port identified is an Ethernet interface port.

- **slot/port**
  Specifies the slot and port for which Ethernet Port Configuration mode is being entered. The slot and port must refer to an installed card and port.

**Usage**

Change the current configuration mode to Ethernet Port Configuration mode.

**Example**

The following command enters the Ethernet Port Configuration mode for ethernet port 1 in slot 17 (ASR 5000):

```
port ethernet 17/1
```

The following command enters the Ethernet Port Configuration mode for ethernet port 11 in slot 5 (ASR 5500):

```
port ethernet 5/11
```
port mac-address virtual-base-address

This command defines a block of 256 consecutive media access control (MAC) addresses and enables virtual MAC addressing for Ethernet line card ports. Not available for the XT2 platform.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

port mac-address virtual-base-address MAC_Address

no port mac-address virtual-base-address

no

Disables virtual MAC addressing for Ethernet line card ports. The block of virtual MAC addresses is not saved.

MAC_Address

Specifies the beginning address of a block of 256 MAC addresses that are used for virtual MAC addressing.

Usage

Use this command to disregard the MAC addresses assigned and stored in card firmware and assign MAC addresses for all Ethernet ports from the specified block of virtual MAC addresses. This command does not affect the MAC addresses on SPIO cards.
There are 65536 MAC addresses (00:05:47:FF:00:00 - 00:05:47:FF:FF:FF) reserved for use by customers. This range allows for the creation of 256 address blocks each containing 256 MAC addresses (for example, 00:05:47:FF:00:00, 00:05:47:FF:01:00, 00:05:47:FF:02:00, 00:05:47:FF:03:00, 00:05:47:FF:04:00, etc.).

⚠️ Caution: This configuration requires the configuration of a valid block of unique MAC addresses that are not used anywhere else. Use of non-unique MAC addresses can degrade and impair the operation of your network.

❗ Important: This command is not supported on all platforms.

Example

To enable virtual MAC addressing for Ethernet ports on all Ethernet line cards in the system using a block of MAC addresses starting at 00:05:47:FF:00:00, enter the following command:
port mac-address virtual-base-address 00:05:47:FF:00:00
port rs232

Enters the RS-232 Port Configuration mode for the RS-232 console port on the specified SPIO card. Not available on the XT2 platform.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
port rs232 slot 3
```

<table>
<thead>
<tr>
<th>rs232</th>
</tr>
</thead>
<tbody>
<tr>
<td>Indicates the port identified is an RS-232 port on a SPIO card.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>slot 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the slot of the SPIO for which RS-232 Port Configuration mode is being entered. The slot must refer to an installed SPIO card. The specified port must always be 3 for an RS-232 port. The value for <code>slot</code> must be either 24 or 25.</td>
</tr>
</tbody>
</table>

**Usage**
Change the current configuration mode to RS-232 Port Configuration mode.

**Example**
The following command enters the RS-232 Port Configuration mode for the SPIO in slot 24;

```
port rs232 24 3
```
profile-id-qci-mapping

Creates a Qos Class-Identifier-Radio Access Network (QCI-RAN) ID mapping table or specifies an existing table and enters the QCI Mapping Configuration mode for the system.

Product
HSGW

Privilege
Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

[ no ] profile-id-qci-mapping name [ -noconfirm ]

- no
  Removes the specified mapping table from the system

- name
  Creates a new or enters an existing mapping table configuration. name must be an alphanumeric string of 1 through 63 alphanumeric.

- -noconfirm
  Indicates that the command is to execute without any additional prompt and confirmation from the user.

Usage

Enters the QCI-RAN ID mapping configuration mode for an existing table or for a newly defined table. This command is also used to remove an existing table.

Entering this command results in the following prompt:

[context_name]hostname(config-hsgw-association-table)#

QCI Mapping Configuration Mode commands are defined in the QCI Mapping Configuration Mode Commands chapter.
Use this command when configuring the HSGW eHRPD component.

Important: This command creates a mapping table available to any HSGW context configured on the system.

Example

The following command enters the existing QCI mapping configuration mode (or creates it if it doesn’t already exist) for a mapping table named qci_table1:
profile-id-qci-mapping qci_table1

The following command will remove qci_table1 from the system:

no profile-id-qci-mapping qci_table1
ps-network

This command creates/removes an HNB-PS network configuration instance for Femto UMTS access over Iu-PS/Iu-Flex interface between Home NodeB Gateway (HNB-GW) service and PS networks elements; i.e. SGSN. This command also configures an existing HNB-CS network instance and enters the HNB-CS Network Configuration mode on a system.

Product
HNB-GW

Privilege
Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:
[local]host_name(config)#

Syntax

[ no ] ps-network ps_instance [ -noconfirm ]

no ps-network ps_instance

no

Removes the specified HNB-PS network instance from the system.

⚠️ Caution: Removing the HNB-PS network instance is a disruptive operation and it will affect all UEs accessing SGSN(s) in specific PS core network through the HNB-GW service.

⚠️ Caution: If any HNB-PS Network instance is removed from the system, all parameters configured in that mode will be deleted and Iu-PS/Iu-Flex interface will be disabled.

ps_instance

Specifies the name of the Packet Switched Core Networks instance which needs to be associated with HNB Radio Network PLMN in HNB RN-PLMN configuration mode. If ps_instance does not refer to an existing HNB-PS instance, the new HNB-PS network instance is created.

ps_instance must be an alphanumeric string of 1 through 63 characters.

-noconfirm

Indicates that the command is to execute without any additional prompt and confirmation from the user.

Usage

Use this command to enter the HNB-PS Network Configuration mode for an existing PS network instance or for a newly defined HNB-PS network instance. This command is also used to remove an existing HNB-PS network instance.
This configuration enables the Iu-PS/Iu-Flex interface on HNB-GW service with CS core network elements; i.e. MSC/VLR.
A maximum of 1 HNB-PS networks instance which is further limited to a maximum of 256 services (regardless of type) can be configured per system.

⚠️ **Caution:** This is a critical configuration. The HNBs can not access SGSNs in PS core network without this configuration. Any change to this configuration would lead to disruption in HNB access to PS core network.

Entering this command results in the following prompt:

```
[context_name]hostname(config-ps-network)#
```

The various parameters available for configuration of an HNB-PS network instance are defined in the *HNB-PS Network Configuration Mode Commands* chapter.

**Example**

The following command enters the existing HNB-PS Network configuration mode (or creates it if it doesn’t already exist) for the instance named `hnb-ps1`:

```
ps-network hnb-ps1
```

The following command will remove HNB-PS network instance `hnb-ps1` from the system without any prompt to user:

```
no ps-network hnb-ps1
```
qci-qos-mapping

Global QCI-QoS mapping tables are used to map QoS Class Identifier (QCI) values to appropriate Quality of Service (QoS) parameters.

Product
- ePDG
- GGSN
- HSGW
- P-GW
- SAEGW
- S-GW

Privilege
- Administrator

Mode
- Exec > Global Configuration
  - configure
  Entering the above command sequence results in the following prompt:

  [local]host_name(config)#

Syntax

qci-qos-mapping name [ -noconfirm ]

no qci-qos-mapping name

no
- Removes the specified mapping configuration from the system

name
- Creates a new or enters an existing mapping configuration. name must be an alphanumeric string of 1 through 63 characters.

-noconfirm
- Indicates that the command is to execute without any additional prompt and confirmation from the user.

Usage

Enter the QCI-QoS mapping configuration mode for an existing table or for a newly defined table. This command is also used to remove an existing table.

Entering this command results in the following prompt:

[context_name]host_name(config-qci-qos-mapping)#
QCI - QoS Mapping Configuration Mode commands are defined in the *QCI - QoS Mapping Configuration Mode Commands* chapter.
Use this command when configuring the following eHRPD component: HSGW, P-GW, SAEGW, S-GW.

**Important:** This command creates a mapping configuration available to any GGSN, HSGW, P-GW, SAEGW, S-GW context configured on the system.

**Example**

The following command enters the existing QCI - QoS mapping configuration mode (or creates it if it doesn’t already exist) for a mapping configuration named `qci-qos3`:

```
qci-qos-mapping qci-qos3
```
**qci**

Defines QCI value.

**Product**
ePDG
HSGW
P-GW
SAEGW
S-GW

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > qci-qos-mapping

`configure > qci-qos-mapping mapping_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-gtpu-service)#
```

**Syntax**

```
quci num [ delay-class delay-class-value [ precedence-class precedence-class-value [ reliability-class reliability-class-value ] ] ] [ downlink [ 802.1p-value value ] [ encaps-header { copy-inner | dscp-marking dscp-marking-value } ] [ gbr ] [ max-packet-delay max-packet-delay-value max-error-rate max-error-rate ] [ non-gbr ] [ traffic-policing interval value ] [ uplink [ 802.1p-value value ] [ encaps-header { copy-inner | dscp-marking dscp-marking-value } ] [ mpls-exp-value value ] [ user-datagram dscp-marking dscp-marking-value ] ]
```

```
no | default qci num
```

| no | Removes the specified QCI value. |
| default | Sets the default QCI value. |

```
quci num
```

`num` must be an integer from 1 through 256.

```
delay-class delay-class-value
```

Defines Pre Release 8 value for configuring packet delay.

`delay-class delay-class-value:` Defines Pre Release 8 value for configuring packet delay as an integer from 1 through 9.
**precedence-class** *precedence-class-value*
Defines Pre Release 8 value for configuring packet precedence.
`precedence-class` *precedence-class-value*: Defines Pre Release 8 value for configuring packet precedence as an integer from 1 through 32.

**reliability-class** *reliability-class-value*
Defines Pre Release 8 value for configuring packet reliability.
`reliability-class` *reliability-class-value*: Defines Pre Release 8 value for configuring packet reliability as an integer from 1 through 32.

downlink
Configures for downlink traffic.

**802.1p-value** *value*
`802.1p-value` *value*: Configures for downlink traffic 802.1p-value as an integer from 1 through 7.

caps-header { copy-inner | dscp-marking dscp-marking-value }
`caps-header`: Defines the DSCP value to be applied to caps header.
`copy-inner`: Copy inner DSCP to outer.
`dscp-marking` *dscp-marking-value*: Defines the DSCP value to be applied to packets with this QCI.
`dscp-marking-value`: A Hexadecimal number between 0x0 and 0x3F.

gbr
Sets the type of the QCI to GBR.

**max-packet-delay** *max-packet-delay-value*
Defines the maximum packet delay in ms for the data with the QCI as an integer from 10 through 1000.

**max-error-rate** *max-error-rate*
Defines the maximum error rate that the data stream can handle in power of 10 as an integer from 1 through 6.

**non-gbr**
Sets the type of the QCI to non GBR.

**traffic-policing interval** *value*
Sets the parameters for traffic policing interval in seconds as an integer from 1 through 100.

uplink
Configures for uplink traffic.

**mpls-exp-value** *value*
Configures for uplink traffic mpls-exp-value as an integer from 1 through 7.
user-datagram
Defines DSCP value to be applied to user data gram.

Usage
Use this command to define QCI value in qci-qos-mapping.

Example
The following command defines QCI value as 56:

```
qci 56
```
qos npu inter-subscriber traffic bandwidth

Configures NPU QoS bandwidth allocations for the system.

Product
PDSN
GGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

qos npu inter-subscriber traffic bandwidth gold percent silver percent bronze percent best-effort percent

no qos npu inter-subscriber traffic bandwidth

no

Removes a previous bandwidth allocation.

gold percent

Default: 10%
Specifies the maximum percentage of bandwidth to be allocated to the gold queue priority. percent can be configured to an integer from 0 through 100.

silver percent

Default: 20%
Specifies the maximum percentage of bandwidth to be allocated to the silver queue priority. percent can be configured to an integer from 0 through 100.

bronze percent

Default: 30%
Specifies the maximum percentage of bandwidth to be allocated to the bronze queue priority. percent can be configured to an integer from 0 through 100.

best-effort percent

Default: 40%
Specifies the maximum percentage of bandwidth to be allocated to the best-effort queue priority. percent can be configured to an integer from 0 through 100.
Usage

The bandwidth of a subscriber queue is maintained by rate limiting functions which implement packet-rate
limiting at the first level and bit-rate limiting at the next level.
The packet-rate limit of a queue is defined by the number of packets-per-second (PPS) permitted for queuing.
Before queuing a packet on a subscriber queue, the NPU ensures that the packet falls within the limit. If the
packet to be queued exceeds the packet rate limit, it is dropped.
Each subscriber queue is configured with a bit rate limit, measured in megabits-per-second (Mbps), referred
to as CP-BPS (bit-per-second to CP). The CP-BPS is available as the total bandwidth for the subscriber traffic
that a CP can sustain. Each subscriber queue receives an allocation of a certain percentage of the CP-BPS.
The following maximum CP-BPS values are supported:
• Lead CP (CP0) = 128 Mbps
• Remaining CPs (CP1, CP2, CP3) = 256 Mbps
For additional information on the NPU QoS functionality, refer to the System Administration and
Configuration Guide.

Important: This functionality is not supported for use with the PDSN at this time.

Example

The following command configures bandwidth allocations of 20, 30, 40, and 50% for the gold, silver, bronze,
and best-effort queues respectively:

```
qos npu inter-subscriber traffic bandwidth gold 20 silver 30 bronze 40 best-effort 50
```

Upon executing this command, the priority queues will have the following packet processing card CP
bandwidth allocations based on the maximum CP bandwidth specifications:

<table>
<thead>
<tr>
<th>Priority</th>
<th>Lead CP (CP 0) Bandwidth (Mbps)</th>
<th>CP 1 through CP 3 Bandwidth (Mbps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gold</td>
<td>25.6</td>
<td>51.2</td>
</tr>
<tr>
<td>Silver</td>
<td>38.4</td>
<td>76.8</td>
</tr>
<tr>
<td>Bronze</td>
<td>51.2</td>
<td>102.4</td>
</tr>
<tr>
<td>Best-effort</td>
<td>64</td>
<td>128</td>
</tr>
</tbody>
</table>
**qos npu inter-subscriber traffic bandwidth-sharing**

Configures NPU QoS bandwidth sharing properties for the system.

**Product**
- PDSN
- GGSN

**Privilege**
Administrator

**Mode**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
qos npu inter-subscriber traffic bandwidth-sharing { { enable | disable } { all | slot slot_num cpu cpu_num } }
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable</td>
<td>Enables bandwidth sharing for the specified criteria.</td>
</tr>
<tr>
<td>disable</td>
<td>Disables bandwidth sharing for the specified criteria.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies that the bandwidth action is to be applied to all packet processing cards and every CPU on each packet processing card.</td>
</tr>
<tr>
<td>slot slot_num</td>
<td>Specifies that the bandwidth action is to be applied to a packet processing card in a specific chassis slot number.</td>
</tr>
<tr>
<td>cpu cpu_num</td>
<td>Specifies a specific control processor (CP) on a packet processing card for which to perform the bandwidth action.</td>
</tr>
</tbody>
</table>

**Usage**

The available bandwidth of a subscriber queue can be shared equally among the other subscriber queues. Any unutilized bandwidth of a queue can be shared with the other queues equally. For example, if only one DSCP
is configured and it is mapped to best-effort, that DSCP would get the bandwidth allocated to the best-effort in addition to the rest of the bandwidth allocated to the gold, silver, and bronze. By default, the system enables sharing for all packet processing cards and their CPs. For additional information on the NPU QoS functionality, refer to the System Administration Guide.

**Important:** This functionality is not supported for use with the PDSN at this time.

**Example**

The following command disables bandwidth sharing for the fourth CP (CP 3) on a packet processing card installed in chassis slot 3:

```
qos npu inter-subscriber traffic bandwidth-sharing disable slot 4 cpu 3
```
**qos npu inter-subscriber traffic priority**

Configures the DSCP-to-Priority assignments for the system.

**Product**

- PDSN
- GGSN

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
qos npu inter-subscriber traffic priority { best-effort | bronze | gold | silver }
assigned-to dscp { af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be | ef | dscp_num }
```

```
no qos npu inter-subscriber traffic priority [ assigned-to dscp { af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be | ef } ]
```

---

**best-effort**

Specifies the best-effort queue priority.

---

**bronze**

Specifies the bronze queue priority.

---

**gold**

Specifies the gold queue priority.

---

**silver**

Specifies the silver queue priority.

---

**afXX**

Assigns the Assured Forwarding XX PHB (per-hop behavior) DSCP.

Each Assured Forwarding PHB has a corresponding DSCP value as follows:

- af11 through af13: DSCP values 5 through 7 respectively
- af21 through af23: DSCP values 9 through 11 respectively
- af31 through af33: DSCP values 13 through 15 respectively
- af41 through af43: DSCP values 17 through 19 respectively
**qos npu inter-subscriber traffic priority**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>be</strong></td>
<td>Assigns the Best Effort forwarding PHB which has a corresponding DSCP value of 0.</td>
</tr>
<tr>
<td><strong>ef</strong></td>
<td>Assigns the Expedited Forwarding PHB which has a corresponding DSCP value of 23.</td>
</tr>
<tr>
<td><strong>dscp_num</strong></td>
<td>Specifies a specific DSCP value as an integer from 0 through 31.</td>
</tr>
</tbody>
</table>

**Usage**

The differentiated services (DS) field of a packet contains six bits (0-5) that represent the differentiated service code point (DSCP) value. Five of the bits (1-5) represent the DSCP. Therefore, up to 32 (2^5) DSCPs can be assigned to the various priorities. By default, they're all assigned to the lowest priority (best-effort). For additional information on the NPU QoS functionality, refer to the System Administration Guide.

**Important:** This functionality is not supported for use with the PDSN at this time.

**Example**

The following command maps the ef DSCP to the gold priority queue:

```
qos npu inter-subscriber traffic priority gold assigned-to dscp ef
```
ran-peer-map

Creates a Radio Access Network (RAN) Peer Map and enters the RAN Peer Map Configuration Mode.

Product
ASN-GW
PHSGW

Privilege
Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

[ no ] ran-peer-map name [ -noconfirm ]

no
Removes the RAN Peer Map from the system.

name
Specifies the name of the RAN Peer Map. name must be an alphanumeric string of 1 through 31 characters.

Usage
Use this command to create a new RAN Peer Map or edit an existing one. RAN peer maps reconcile base station MAC addresses received in R6 protocol messages to the base station’s IP address. Entering this command results in the following prompt:

[context_name]hostname(config-ran-peer-map)#

RAN Peer Map Configuration Mode commands are defined in the ASN RAN Peer Map Configuration Mode Commands chapter in this guide.

Example
The following command creates a RAN peer map named ran12:

   ran-peer-map ran12
**require active-charging**

This command enables/disables Active Charging Service (ACS) with or without the Category-based Content Filtering application.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

`configure`

Entering the above command sequence results in the following prompt:

`[local]host_name(config)#`

**Syntax**

```
require active-charging [ isolated-mode ] [ content-filtering category [ static-and-dynamic ] ] [ optimized-mode ]
```

no require active-charging

```
no
```

Disables ACS on the system.

```
isolated-mode
```

Enables ACS and separates ACS-related resources from other sub-system resource sharing.

**Important:** In 8.1 and later releases, this keyword is not supported.

```
optimized-mode
```

Enables ACS in Optimized mode, wherein ACS functionality is managed by SessMgrs.

**Important:** In 8.0 and earlier releases and in 9.0 and later releases, this keyword is not supported.

**Important:** In Release 8.1, ACS must be configured in the Optimized mode.

**Important:** In Release 8.1, if the active-charging mode is changed from the default (non-optimized) mode to the Optimized mode, or vice-versa, the system must be rebooted for the change to take effect.

**Important:** In Release 8.3, this keyword is obsolete. With or without this keyword ACS is always enabled in the Optimized mode.
Use the `require active-charging` command to enable ACS in the non-optimized mode. Wherein, ACS Managers will spawn to support ACS.

Use the `require active-charging optimized-mode` command to enable ACS in the Optimized mode. Wherein, ACS is enabled as part of Session Managers.

```
content-filtering category [ static-and-dynamic ]
```

Enables the Category-based Content Filtering application with ACS support and creates the necessary Static Rating Database (SRDB) tasks to utilize the internal database of static/dynamic URLs.

For Dynamic Content Filtering support, the `static-and-dynamic` keyword must be configured to specify that the Dynamic Rater Package (model and feature files) must be distributed to rating modules on startup, recovery, etc. If not configured, by default, the static-only mode is enabled.

---

**Usage**

Use this command to enable/disable ACS with or without Category-based Content Filtering application on the chassis.

---

**Important:** This command triggers the resource subsystem to switch to ACS-enabled mode and start ACS-related tasks. This CLI command must be configured before any services are configured, so that the resource subsystem can appropriately reserve adequate memory for the ACS-related tasks. After configuring this command, the configuration must be saved and the system rebooted in order to allocate the resources for ACS upon system startup.

In 8.0 and 8.1 releases, this command must be configured before configuring any services. This is to ensure that the resource subsystem can appropriately reserve adequate memory for ACS Manager tasks. If this command is configured after all the Session Manager tasks are already active, the ACS Manager tasks will not be started even if additional cards are added to the chassis—instead, the chassis must be rebooted.

---

**Example**

In Release 8.0, the following command enables resource subsystem to configure ACS in isolated mode:

```
require active-charging isolated-mode
```

In Release 8.1, the following command enables ACS in Optimized mode:

```
require active-charging optimized-mode
```

In Release 8.3, the following command enables ACS in Optimized mode:

```
require active-charging
```
**require cipher ssl resource-percentage**

Assigns the 8 processing cores on the PSC2 card and splits the hardware acceleration resources between SSL protocol and IPSec protocol processing.

**Product**
SCM (P-CSCF, A-BG)

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

```sh
configure
```

Entering the above command sequence results in the following prompt:

```sh
[local]host_name(config)#
```

**Syntax**

```sh
require cipher ssl resource-percentage percentage_value
```

**default require cipher ssl resource-percentage**

`percentage_value`

The system converts the specified resource percentage value to the nearest number of processing cores assigned to SSL processing. The system assigns the remaining processing cores to IPSec processing. This value can be within the range of 0 to 100.

For example, if 20% of the hardware acceleration resources are assigned to SSL processing, the system translates this value to INT((20*8+50)/100) = 2 processing cores assigned to SSL processing, and (8-2) = 6 processing cores assigned to IPSec processing.

**default**

Sets the default percentage value to 0%, assigning all 8 processing cores to IPSec processing.

**Usage**

Use this command to split the 8 processing cores on the PSC2 card between SSL protocol and IPSec protocol processing.

**Example**

The following command assigns 20% of the hardware acceleration resources on the PSC2 card (2 processing cores) to SSL processing, and 80% of the hardware acceleration resources (6 processing cores) to IPSec processing:

```sh
require cipher ssl resource-percentage 20
```
require cscf-connection-proxy

Configures one Diameter proxy per card (multiple) or one proxy per system (single).

**Product**
SCM (P-CSCF, A-BG)

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration
   configure
Entering the above command sequence results in the following prompt:

   [local]host_name(config)#

**Syntax**

   require cscf-connection-proxy { multiple | single }

   { multiple | single }
   Configures one Diameter proxy per card (support for multiple proxies) or one CSCF proxy per system.

**Usage**
Use this command to establish a single Diameter proxy per system or multiple Diameter proxies (one per card). For additional information refer to the **CSCF Proxy-CSCF Configuration Mode Commands** chapter.

**Example**
The following command allows one Diameter proxy per system:

   require cscf-connection-proxy single
require demux

Enables or disables demux capabilities on an ASR 5x00 system. On an ASR 5500 when demux tasks are enabled on a management card, the Active and Standby MIOs will host and migrate all demux tasks.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

```
configure
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
[ default | no ] require demux { card | management-card | processing-card }
```

- **default**
  Demux functions will be run on a processing card.

- **no**
  Disables the demux capabilities except when session recovery is enabled.

**Important:** On a system with session recovery licensed and enabled, a processing or management card must be designated to run demux functions.

**Usage**

Use this command to configure the system to direct demux task placement.

The following restrictions apply when enabling an MIO/UMIO as a demux card:

- The `require demux management-card` command must be configured before any service or contexts have been created on the system. The command will not execute after a mode of operation has been selected for the chassis.

- Only the following services currently support the designation of an MIO/UMIO card for demux functions: GGSN, SGW, PGW, HA and SAE-GW.

- Ex-GW, L2TP, MME, NEMO and SGSN are not supported.
After the ASR 5500 has booted with demux functions running on an MIO/UMIO, you cannot configure non-supported services. A maximum of eight Demux Managers are supported. Any attempt to add more than eight Demux Managers will be blocked.

Service/products requiring a large number of VPN Managers, VRFs and/or Demux Managers must not enable demux functions on an MIO.

With demux functions running on an MIO, the ASR 5500 supports a maximum of 10 contexts, 15 interfaces per context, with a maximum of 64 interfaces and 250 VRFs per system.

Implementation of this feature assumes that CEPS (Call Events Per Second) and the number of subscribers will remain constant, and only the data rate will increase. This ensures that the CPU demand will not increase on the MIO/UMIO.

**Caution:** Enabling the Demux on MIO/UMIO feature changes resource allocations within the system. This directly impacts an upgrade or downgrade between StarOS versions in ICSR configurations. Contact Cisco TAC for procedural assistance prior to upgrading or downgrading your ICSR deployment.

**Important:** Contact Cisco TAC for additional assistance when assessing the impact to system configurations when enabling the Demux on MIO/UMIO feature.

**Example**

For releases prior to 15.0, to configure a DPC/UDPC as a demux card enter the following CLI commands:

```plaintext
require demux card
```

For release 15.0+, to configure a DPC/UDPC as a demux card enter the following CLI commands:

```plaintext
require demux processing-card
```

To configure an MIO/UMIO as a demux card enter the following CLI commands:

```plaintext
require demux management-card
```
require detailed-rohc-stats

Enables or disables context-specific Robust Header Compression (RoHC) statistics.

**Product**
- HSGW
- PDSN

**Privilege**
- Administrator

**Mode**
- Exec > Global Configuration
- `configure`

Entering the above command sequence results in the following prompt:

```
[local] host_name(config)#
```

**Syntax**

```
[ no ] require detailed-rohc-stats
```

- `no`
  Disables statistics for RoHC calls. This is the default condition.

**Usage**

Enables context-specific statistics for RoHC calls.

**Example**

Enter the following command to enable context specific statistics for RoHC calls:

```
require detailed-rohc-stats
```
require diameter-proxy

This command enables or disables Diameter Proxy mode.

Product
IPCFC

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

require diameter-proxy { master-slave | multiple | single }

no require diameter-proxy

no
Disables Diameter Proxy mode. This is the default configuration.

master-slave
Sets the Diameter-Proxy to Master-Slave mode.
In Master-Slave mode, multiple Diameter proxies are running, one on each packet processing card. One proxy serves as the Master and the other proxies are Slaves. The Master proxy relays the traffic across multiple Slave Diameter proxies.

multiple
Configures one Diameter proxy for each active packet processing card.

single
Configures one Diameter proxy for the entire chassis.

Usage
When the Diameter Proxy mode is enabled, each proxy process is a Diameter host, instead of requiring every Diameter application user (such as, every ACSMgr and/or every SessMgr, depending on the application) to be a host.
In Master-Slave mode, multiple Diameter proxies are running, one on each packet processing card. One proxy serves as the Master and the other proxies are Slaves. The Master relays the traffic from an incoming connection to a specific Slave Diameter proxy.

Example
The following command configures a Diameter proxy for each active packet processing card:

require diameter-proxy multiple
The following command configures a single Diameter proxy for the entire chassis:

```
require diameter-proxy single
```
**require ecs credit-control**

This command configures the Diameter Credit-Control Application (DCCA) to work in per subscriber-PDN level Gy mode.

**Product**
- GGSN
- HA
- IPSG
- PDSN
- P-GW

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration
- `configure`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

**In 14.0 and earlier releases:**

```
[ no ] require ecs credit-control subscriber-mode
```

**In 14.1 and later releases:**

```
[ no ] require ecs credit-control session-mode per-subscriber
```

**Usage**

**In 14.0 and earlier releases:**

This command is applicable to all products using the Gy interface. Use this command to configure DCCA/Gy to work in per subscriber-PDN level Gy mode, wherein one Diameter session is created per subscriber PDN rather than per bearer, and only one DCCA/Gy session is created for multi-bearer PDNs. If this command is not configured, or the `no require ecs credit-control subscriber-mode` command is configured, DCCA/Gy sessions are created per bearer/PDP-context, and as a result when there are multiple PDP contexts or multiple bearers in a PDN as many DCCA/Gy sessions are created.

**Important:** This command will take effect only when the system is booted/rebooted. When configured after the system comes up, the command will be accepted but will not be applied until after the system is rebooted with the saved configuration.
**Important:** This command is independent of the `require active-charging` command. The `ecs` keyword in this command is license dependent.

**In 14.1 and later releases:**
This CLI command is made configurable on the fly, that means, the credit control mode can be seamlessly changed from subscriber (PDN) to sub-session and vice-versa without requiring a system reboot.

This change is done to align with the new CLI commands “`credit-control-client override session-mode { per-sub-session | per-subscriber }`” introduced in APN and Subscriber Group configuration modes.

This will be the default mode for all subscribers unless overwritten by APN/Subscriber configuration mode CLI commands.

Releases prior to 14.1, subscriber mode Gy and bearer mode Gy were implemented based on the configuration of CLI command `require ecs credit-control subscriber-mode`. This CLI is used as a chassis level configuration which mandates that all subscribers anchored to this chassis should always be running in only one of these two modes. Enabling and disabling the CLI requires system reboot. ICSR switchover between two chassis running in two different modes will not work.

Release 14.1 and later, the Subscriber/Bearer mode Gy is selected based on APN/Subscriber mode instead of chassis wide configuration. This will provide the following:

- Flexibility to configure different modes for different subscriber.
- Flexibility to switch between modes without system reboot.
- Flexibility to switchover between two chassis working in different modes.
require session recovery

Enables session recovery when hardware or software fault occurs within system.

Product
- ePDG
- GGSN
- ASN-GW
- HA
- HSGW
- LNS
- MME
- PDG/TTG
- PDIF
- PDSN
- P-GW
- SAEGW
- SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

[ no ] require session recovery

no

Disables session recovery feature after configuration file is saved and system is restarted.

Usage

When this feature is enabled, the system attempts to recover any home agent-based Mobile IP sessions that would normally be lost due to a hardware or software fault within the system. This functionality is available for the following call types:

- ASN-GW services supporting simple IP, Mobile IP, and Proxy Mobile IP
- PDSN services supporting simple IP, Mobile IP, and Proxy Mobile IP
- HA services supporting Mobile IP and/or Proxy Mobile IP session types with or without per-user Layer 3 tunnels
require session recovery

- GGSN services for IPv4 and PPP PDP contexts
- SGSN services for all attached and/or activated subscribers
- LNS session types
- PDIF services supporting Simple-IP, Mobile-IP and Proxy Mobile-P
- MME services

The default setting for this command is disabled.
The no option of this command disables this feature.
This command only works when the Session Recovery feature is enabled through a valid Session and Feature Use License Key.

**Important:** After entering this command, you must restart the system for the command takes effect. Remember to save the configuration file before issuing the **reload** command.
reveal disabled commands

Enables the input of commands for features that do not have license keys installed. The output of the command `show cli` indicates when this is enabled. This command effects all future CLI sessions. This is disabled by default.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration
`configure`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
[ no ] reveal disabled commands
```

- **no**
  
  Do not show disabled commands.

**Usage**

When this is enabled and a disabled command is entered, a message is displayed that informs you that the required feature is not enabled and also lists the name of the feature that you need to support the command. When this is disabled and a disabled command is entered, the CLI does not acknowledge the existence of the command and displays a message that the keyword is unrecognized.

**Example**

Set the CLI to accept disabled commands and display the required feature for all future CLI sessions with the following command:

```
reveal disabled commands
```

Set the CLI to reject disabled commands and return an error message for all future CLI sessions:

```
no reveal disabled commands
```
**rlf-template**

This command enters the Rate Limiting Function (RLF) Template Configuration Mode. This mode is used to configure the RLF template to control the throttling parameters.

**Important:** RLF template cannot be deleted if it is bound to any application (peers/endpoints).

**Product**

- GGSN
- P-GW

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
[ no ] rlf-template rlf_template_name
```

- **no**
  
  Remove the specified RLF template from global configuration.

- **rlf_template_name**

  The name of the RLF template to create or remove. `rlf_template_name` must be an alphanumeric string of 1 through 127 characters.

**Usage**

Use this command to enter the RLF Template Configuration mode. The users can define the rate limiting configurations within this template.

**Important:** Rate Limiting Function (RLF) is a license-controlled feature. A valid feature license must be installed prior to configuring this feature. Contact your Cisco account representative for more information.

This feature implements a generic framework that can be used by multiple interfaces and products for rate-limiting/throttling outgoing messages like Diameter messages on Gx, Gy interface towards PCRF. When applications send messages to peers at a high rate, (e.g. when a large number of sessions goes down at the same time, accounting stop messages for all the sessions are generated at the same time) the peer may not be able to handle the messages at such high rates. To overcome this situation, the Rate Limiting Function (RLF) framework is developed so that the application sends messages at an optimal rate such that peer is capable of receiving all the messages and does not enter an overload condition.
When RLF feature is enabled, all the messages from the application are pushed to the RLF module for throttling and rate control, and depending on the message-rate configured the RLF module sends the messages to the peer. Once the rate or a threshold value is reached, the RLF module notifies the application to slow down or stop sending messages. RLF module also notifies the application when it is capable of accepting more messages to be sent to the peer. RLF module typically uses a Token Bucket Algorithm to achieve rate limiting.

Currently in the deployment of the Diameter applications (Gx, Gy, etc.), many operators make use of “max-outstanding <number>” as a means of achieving some rate-limiting on the outgoing control traffic. With RLF in place, this is no longer required since RLF takes care of rate-limiting in all cases. If RLF is used and max-outstanding is also used, there might be undesirable results.

**Important:** If RLF is being used with an "diameter endpoint", then set the max-outstanding value of the peer to be 255.

To use the template, Diameter or any other applications must be associated with the template. The RLF provides only the framework to perform the rate limiting at the configured Transactions Per Second (TPS). The applications (like Diameter) should perform the configuration specific to each application.

Entering this command results in the following prompt:

```
[context_name]host_name(cfg-rlf-template)#
```

RLF Template Configuration Mode commands are defined in the *RLF Template Configuration Mode Commands* chapter.

**Example**

The following command creates an RLF template named `rlf_1` and enters the RLF Template Configuration mode:

```
rlf-template rlf_1
```
**rohc-profile**

This command allows you to create an RoHC (Robust Header Compression) profile and enter the RoHC Profile Configuration Mode. This mode is used to configure RoHC Compressor and Decompressor parameters. RoHC profiles can then be assigned to specific subscriber sessions when RoHC header compression is configured.

**Product**

HSGW

PDSN

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local] host_name(config) #

**Syntax**

```
rohc-profile profile-name name [ -noconfirm ] [ common-options | compression-options | decompression-options ]
```

```
no rohc-profile profile-name name
```

---

**common-options**

Configures common parameters for compressor and decompressor.

**compression-options**

Configures ROHC compression options.

**decompression-options**

Configures ROHC decompression options.

**no**

Remove the specified RoHC profile.

**name**

The name of the RoHC profile to create or remove. *name* must be an alphanumeric string of 1 through 63 characters.

**-noconfirm**

Do not prompt for additional verification when executing this command.
Usage

Use this command to enter the RoHC Profile Configuration mode. Entering this command results in the following prompt:

```
[context_name]host(config-rohcprofile-<profile_name>)#
```

RoHC Profile Configuration Mode commands are defined in the RoHC Profile Configuration Mode Commands chapter.

Example

Enter the following command to create an RoHC profile named HomeUsers and enter the RoHC Configuration mode without prompting for verification:

```
rohc-profile profile-name HomeUsers
```

The following command removes the RoHC profile named HomeUsers:

```
no rohc-profile profile-name HomeUsers
```
**sccp-network**

This command creates or removes a Signaling Connection Control Part (SCCP) network instance which is used to define the SS7 end-to-end routing in a UMTS network. As well, this command enters the SCCP network configuration mode. The SGSN supports up to 12 SCCP network instances at one time.

**Product**
SGSN  
HNB-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

```
[local] host_name(config)#
```

**Syntax**

```
sccp-network sccp_net_id [ -noconfirm ]
```

```
no sccp-network sccp_net_id
```

- **no**
  Remove the SCCP network configuration with the specified index number from the system configuration.

- **sccp_net_id**
  This number identifies a specific SCCP network configuration.

  - **sccp_net_id**: must be an integer from 1 through 12.

- **-noconfirm**
  Indicates that the command is to execute without any additional prompt and confirmation from the user.

**Usage**

Use this command to create or modify an SCCP network and enter the SCCP network configuration mode. The SCCP network is not a standard SS7 or UMTS concept - this concept is specific to this platform. For details about the commands and parameters needed to create and edit the SCCP Network configuration, check the **SCCP Network Configuration Mode** chapter.

**Example**

The following command creates an SCCP network with the index number of 1:

```
sccp-network 1
```

The following command creates an SCCP network with the index number of 2 to associate with HNB-GW service for HNB access network users without any prompt:
sccp-network 2 -noconfirm
sctp-param-template

This command allows you to create an SCTP parameter template and enter the SCTP Parameter Template Configuration Mode. This mode is used to configure parameters for SCTP associations.

**Product**
MME

**Privilege**
Administrator

**Mode**
Exec > Global Configuration
   *configure*
Entering the above command sequence results in the following prompt:

```
[local] host_name(config) #
```

**Syntax**

```
[ no ] sctp-param-template name
```

- **no**
  Removes the specified SCTP parameter template from the system.

- **name**
  Specifies the name of the SCTP parameter template being created or accessed. *name* must be an alphanumeric string of 1 through 63 characters.

**Usage**
Use this command to enter the SCTP Parameter Template Configuration mode.
Entering this command results in the following prompt:

```
[context_name] host(sctp-param-template) #
```

SCTP Parameter Template Configuration Mode commands are defined in the *SCTP Parameter Template Configuration Mode Commands* chapter.

**Example**
The following command creates a new SCTP parameter template or enters an existing template named *sctp-tmpl2*:

```
sctp-param-template sctp-tmpl2
```
**session trace**

This command configures the type of network elements, file transfer protocol, and Trace collection entity mode to be used for the transportation of trace files collected for the subscriber session tracing on the UMTS/EPC network element(s) along with network connection parameters and timers.

**Product**
- GGSN
- MME
- P-GW
- SAEGW
- S-GW

**Privilege**
Administrator

**Mode**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```plaintext
session trace network-element { all | mme | pgw | sgw | ggsn | saegw } [ collection-timer sec ] [ file-type { a-type | b-type } ] [ tce-mode { none | push transport sftp path string username name { encrypted password enc_pw | password password } } ]
```

**no session trace network-element { all | mme | pgw | sgw | ggsn saegw }

**no**

Removes the entire session trace configuration from the system or a specific network element trace configuration.

**Important:** To modify the session trace network-element configuration, you must first enter the `no session trace network-element` form of the command to remove the session trace configuration and then enter an entirely new configuration.

```plaintext
network-element { all | mme | pgw | sgw | ggsn saegw }
```

Identifies the type of service to the session trace application in order to determine the applicable interfaces.
- **all:** Specifies that all network elements and their associated interfaces are to be made available to the session trace application.
- **ggsn:** Specifies that the GGSN and its associated interfaces is to be made available to the session trace application.
- **mme:** Specifies that the MME and its associated interfaces is to be made available to the session trace application.
pgw: Specifies that the P-GW and its associated interfaces is to be made available to the session trace application.

sgw: Specifies that the S-GW and its associated interfaces is to be made available to the session trace application.

saegw: Specifies that the SAEGW and its associated interfaces is to be made available to the session trace application.

collection-timer sec

Specifies the amount of time (in seconds) to wait from initial activation/data collection before data is reported to the Trace Collection Entity (TCE). sec must be an integer from 0 through 255.

tce-mode none

Specifies that session trace files are to be stored locally and must be pulled by the TCE.

tce-mode push transport sftp path string username name { encrypted password enc_pw | password password }

Specifies that session trace files are to be pushed to the Trace Collection Entity (TCE).
sftp: Specifies that Secure FTP is used to push session trace files to the TCE.
path string: Specifies the directory path on the TCE where files will be placed.
username name: Specifies the username to be used when pushing files to the TCE.
encrypted password enc_pw: Specifies the encrypted password to be used when pushing files to the TCE.
password password: Specifies the password to be used when pushing files to the TCE.

Usage

Use this command to configure the file transfer methods and modes for subscriber session trace functionality and to how and where session trace files are sent after collection. This configuration contains collection timer, UMTS/EPC network element, type of file transfer, and user credentials setting to send the collected trace files to the TCE.

Example

The following command configures the collection time for session traces to 30 seconds, identifies the network element as all elements (GGSN, MME, S-GW, SAEGW, and P-GW), and pushes session trace files to a TCE via SFTP into a directory named /trace/agw using a username admin and a password of pw123:

```
session trace network-element all collection-timer 30 tce-mode push transport sftp path /trace/agw username admin password pw123
```

The following command configures the collection time for session traces to 30 seconds, identifies the network element as an MME, and pushes session trace files to a TCE via SFTP into a directory named /trace/sgw using a username admin and a password of pw123:

```
session trace network-element mme collection-timer 30 tce-mode push transport sftp path /trace/mme username admin password pw123
```

The following command configures the collection time for session traces to 30 seconds, identifies the network element as GGSN, and pushes session trace files to a TCE via SFTP into a directory named /trace/ggsn using a username admin and a password of pw123:

```
session trace network-element ggsn collection-timer 30 tce-mode push transport sftp path /trace/ggsn username admin password pw123
```
sgsn-global

This command gives access to the SGSN Global configuration mode to set parameters relevant to the SGSN and HNB-GW as a whole.

Product
SGSN
HNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

sgsn-global

Usage
Using this command moves into SGSN Global Configuration mode. In this mode, you can set system-wide parameters on SGSN and HNB-GW to perform the following tasks:
On SGSN:
• monitoring and managing TLLIs in the BSSGP layer.
• defining IMSI ranges used as filters in the operator policy selection process.
On HNB-GW:
• setting system-wide IPC message aggregation parameters

Example
Enter the SGSN Global configuration mode with the following:

sgsn-global
snmp authentication-failure-trap

Enables or disables the SNMP traps for authentication failures.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

```bash
configure
```
Entering the above command sequence results in the following prompt:

```
[local] host_name(config) #
```

**Syntax**

```
[ no ] snmp authentication-failure-trap
```

---

**no**

Disables SNMP traps for authentication failures. When omitted, SNMP traps for authentication failures will be generated.

---

**Usage**

Disables authentication failure traps if they are not of interest. At this time the option may be changed to support trouble shooting.

By default SNMP authentication failure traps are disabled.
**snmp community**

Configures the SNMP v1 and v2 community strings.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

`configure`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

In StarOS 12.3 and later releases:

```
snmp community [ encrypted ] name string [ context context_name | read-only | read-write | view view_name ]
```

```
no snmp community [ encrypted ] name string
```

In StarOS 12.2:

```
snmp community [ encrypted ] name string | read-only | read-write ]
```

```
no snmp community [ encrypted ] name string
```

In StarOS 12.1 and earlier releases:

```
snmp community string [ read-only | read-write ]
```

```
no snmp community string
```

**no**

The specified community string is removed from the configuration.

**encrypted**

Specifies the use of an encrypted string when entering the community name. Without the encrypted option, the plain-text community name must be provided.

**name string**

Specifies a community string whose options are to be modified. An unencrypted string must be an alphanumeric string of 1 through 31 characters. An encrypted string is an alphanumeric string of 1 through 80 characters.
context context_name
Default: community string applies to all contexts.
Specifies a the context to which the community string shall be applied. context_name must be an alphanumeric string of 1 through 31 characters.

read-only | read-write
Default: read-only
Specifies if access rights for the community string.
read-only: the configuration may only be viewed.
read-write: the configuration may be viewed and edited.

view view_name
Default: community string applies to all views.
Specifies the view to which the community string shall be applied. view_name must be an alphanumeric string of 1 through 31 characters.

Usage
The community strings define the privileges of SNMP users. It may be desirable to give read-only access to front line operators.

Example

snmp community name plain_text_string
snmp community encrypted name encrypted_string
snmp community name plain_text_string context sampleContext
snmp community name plain_text_string context sampleContext view sampleView
snmp community name plain_text_string read-write view sampleView
no snmp community plain_text_string
snmp discard-snmpv3-pdu

Configures the system to discard all SNMPv3 protocol data units (PDUs) received.

**Product**
All

**Privilege**
Administrator

**Mode**
Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

**Syntax**

```
snmp discard-snmpv3-pdu

no snmp discard-snmpv3-pdu
```

**Usage**

Use this command to configure the system to discard all SNMPv3 messages received. By default, the system processes SNMPv3 PDUs.

**Example**

The following command configures the system to discard all SNMPv3 messages received.

```
snmp discard-snmpv3-pdu arg1
```
**snmp engine-id**

Configures the SNMP engine to use for SNMP requests when SNMPv3 agents are utilized.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

**configure**

Entering the above command sequence results in the following prompt:

```
[local] host_name(config) #
```

**Syntax**

```
snmp engine-id local id
```

- **id**

  Specifies the SNMPv3 engine to employ. *id* must be an alphanumerical string of 1 through 31 characters.

**Usage**

When SNMPv3 is used for SNMP access to the chassis the engine ID can be used to quickly change which schema is used for SNMP access.

**Important:** The system can send either SNMPv1, SNMPv2c, or SNMPv3 traps to numerous target devices. However, the Web Element Manager can only process SNMP version 1 (SNMPv1) and SNMP version 2c (SNMPv2c) traps. If the SNMP target being configured is Web Element Manager application, then you must not configure this command to use.

**Example**

```
snmp engine-id local id
```
snmp heartbeat

Enables the sending of periodic “heartbeat” notifications (traps).

Product
All

Privilege
Administrator

Mode
Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

```
snmp heartbeat { interval [ minutes ] | second-interval [ seconds ] }
[ default | no ] snmp heartbeat
```

- **default**
  Returns the command to its default setting of disabled.

- **no**
  Disables the feature.

- **interval [ minutes ]**
  Default: 60
  Specifies the interval time (in minutes) between notifications. minutes must be an integer from 1 through 1440.

- **second-interval [ seconds ]**
  Default: 30
  Specifies the secondary interval time, in seconds, between notifications. seconds must be an integer from 10 through 50.

Usage

Use this command to enable the sending of a heartbeat notification periodically to confirm a system is up and communicating.

Example

The following command sets the SNMP heartbeat notification interval to 2 hours, 15 minutes and 30 seconds:

```
snmp heartbeat interval 135 second-interval 30
```
**snmp history heartbeat**

Enables the recording of heartbeat notifications in SNMP history.

**Product**
All

**Privilege**
Administrator

**Mode**
Exec > Global Configuration
  - `configure`

Entering the above command sequence results in the following prompt:

```
[local] host_name(config) #
```

**Syntax**

```
[ default | no ] snmp history heartbeat
```

- **default**
  Returns the command to the default setting of enabled.

- **no**
  Disables the history recording feature.

**Usage**

Use this command to enable the recording of SNMP heartbeat notifications in SNMP history files.
**snmp mib**

Enables or disables a specified SNMP Management Information Base (MIB).

**Product**
All

**Privilege**
Administrator

**Mode**
Exec > Global Configuration

**Syntax**
```
[ no ] snmp mib mib_name
```

*no*
Disables the specified MIB.

*mib_name*
 Specifies a MIB by its name. You can find the currently supported MIBs by running the Exec mode `show snmp server` command. Enter the MIB name as a text string exactly as displayed under “SNMP Agent Mib Configuration”. By default the STARENT-MIB is enabled.

**Usage**

Use this command to enable or disable system support for an SNMP MIB.

**Example**
The following command enables the SNMP MIB entitled “CISCO-MOBILE-WIRELESS-SERVICE-MIB”.

```
snmp mib CISCO-MOBILE-WIRELESS-SERVICE-MIB
```
**snmp notif-threshold**

Configures the number of SNMP notification that need to be generated for a given event before it is propagated to the SNMP users.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration
*configure*

Entering the above command sequence results in the following prompt:

```
[local] host_name(config)#
```

**Syntax**

```
snmp notif-threshold count [ low low_count ] [ period seconds ]
```

```
no snmp notif-threshold
```

- **count**
  - Default: 100
  - The traps creation rate will be monitored periodically (as configured by the period field). If the number of traps created over one period cycle exceeds the count value configured, then the trap creation will be disabled. count must be an integer from 1 through 10000.

- **low low_count**
  - Default: 20
  - The traps creation rate will be monitored periodically (as configured by the period field). The trap creation will be enabled again only if the number of trap creation drops below the low_count value configured. Otherwise, trap creation remains disabled. low_count must be an integer from 1 through 10000.

- **period seconds**
  - Default: 300
  - Specifies the number of seconds of the monitoring window size before any subsequent notification may be broadcast to users. seconds must be an integer from 10 through 3600.

**Usage**

Set the notification threshold to avoid a flood of events which may be the result of a single failure or maintenance activity.

**Example**
snmp notif-threshold 100

snmp notif-threshold 100 period 30
snmp server

 Enables the SNMP server as well the configuration of the SNMP server port.

 **Product**
 All

 **Privilege**
 Security Administrator, Administrator

 **Mode**
 Exec > Global Configuration

 configure
 Entering the above command sequence results in the following prompt:

 [local]host_name(config)#

 **Syntax**

 snmp server [ port number ]

 no snmp server

  no
  Restores the default SNMP port assignment.

  port number
  Default: 161
  Specifies the port number to use for SNMP communications. *number* must be an integer from 1 to 65535.

 **Usage**
 Set the SNMP port for communications when SNMP is enabled.

 **Important:** This will result in restarting the SNMP agent when the **no** keyword is omitted. SNMP queries as well as notifications/traps will be blocked until the agent has restarted.

 **Example**

 snmp server port 100

 no snmp server
snmp target

Configures remote receivers for SNMP notifications.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

```
configure
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
snmp target name ip_address [ port number ] [ non-default ] [ security-name string ] [ version { 1 | 2c | 3 | view } [ security-level { noauth | { auth | priv-auth privacy [ encrypted ] des privpassword } authentication [ encrypted ] { md5 | sha } authpassword } } [ informs | traps ]
```

```
no snmp target name
```

- **no**
  Removes the specified target as a receiver of unsolicited SNMP messages (traps).

- **authentication** { md5 | sha } authpassword
  Reads the authentication type and password if the security level of the SNMP messages is set to auth or priv-auth. Authentication types are:
  - **md5**: Configures the hash-algorithm to implement MD5 per RFC 1321.
  - **sha**: Specifies that the hash protocol is Secure Hash Algorithm.

- **security-level** { noauth | { auth | priv-auth privacy [ encrypted ] des privpassword } }
  Sets the security level of the SNMPv3 messages, as follows:
  - **noauth**: No authentication and encryption is used.
  - **auth**: Only authentication will be used.
  - **priv-auth**: Both authentication and encryption will be used.
  - **privacy des privpassword**: Reads the privacy type and password.

- **name**
  Specifies a logical name to use to refer to the remote receiver. *name* must be an alphanumeric string of 1 through 31 characters.
**ip_address**

Specifies the IP address of the receiver. *ip_address* must be specified using IPv4 dotted-decimal notation.

**non-default**

Specifies that this destination is only used for SNMP traps which have been specifically identified.

**port number**

Default: 162

Specifies the port which is to be used in communicating with the remote receivers. *number* must be an integer from 0 through 65535.

**security-name string**

Default: no community string included

Specifies the community string to use in the unsolicited messages. *string* must be an alphanumeric string of 1 through 31 characters.

**version { 1 | 2c | 3 } | view**

Default: 1

Specifies the SNMP version the target supports and consequently the version of the SNMP protocol to use for communications.

**Important:** The system can send either SNMPv1, SNMPv2c, or SNMPv3 traps to numerous target devices. However, the Web Element Manager can only process SNMP version 1 (SNMPv1) and SNMP version 2c (SNMPv2c) traps. If the SNMP target being configured is Web Element Manager application, then you must configure this command to use version 1 or version 2c.

**informs | traps**

Default: traps

Specifies the type of SNMP event to use to send notifications to SNPM targets. *traps* are unacknowledged (fire and forget) whereas *informs* require a response from the SNMP target.

If the notification type is set to *informs*, the notification is resent if no response is received within 5 seconds. The notification is resent at most two times.

**Usage**

The target manages the list of remote receivers to which unsolicited messages are sent. Use this command to add/remove a monitoring system to/from a network.

**Example**

```
snmp target sampleReceiver 1.2.3.4 security-name sampleComm

snmp target sampleReceiver 1.2.5.6 port 100

snmp target sampleReceiver 1.2.7.8 version 2c traps

no snmp target sampleReceiver
```
**snmp trap**

This command enables or disables generation of specific or all SNMP traps.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
snmp trap { enable | suppress } [ trap_name1 trap_name2 ... trap_nameN | all ]
```

<table>
<thead>
<tr>
<th>enable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enables or allows the generation of one or more SNMP traps by the system.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>suppress</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disables the generation of one or more SNMP traps by the system.</td>
</tr>
</tbody>
</table>

```
trap_name1 trap_name2 ... trap_nameN
```

The name of the specific SNMP trap to enable or disable. Multiple traps can be listed for a single instance of this command.

**Important:** The system disregards character case (case insensitive) when entering trap names.

```
all
```

Default: Enable All

Specifies that all SNMP traps will be affected by the specified operation (enable or suppress).

**Usage**

SNMP traps are used by the system to indicate that certain events have occurred. A complete listing of the traps supported by the system and their descriptions can be found in the *SNMP MIB Reference*. Additionally, a trap listing can be viewed using the following command:

```
snmp trap { enable | suppress } ?
```

By default, the system enables the generation of all traps. However, individual traps can be disabled allowing only traps of a certain type or alarm level to be generated. This command can be used to disable un-desired traps and/or re-enable previously suppressed traps.

**Example**

The following command suppresses the LogMessage trap:
snmp trap suppress logmessage

The following command suppresses the CLISessEnd and CLISessStart:

```
snmp trap suppress clisessend clisessstart
```
snmp trap-timestamps

Adds an additional system-time varbind to generated traps.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

[ no ] snmp trap-timestamps

  no

  Disables the adding of timestamps to generated traps.

Usage

The timestamp added to the generated trap reflects the current system time. The timestamp is proprietary. This functionality is disabled by default.

Important: If the Web Element Manager application is used as your alarm server, the application relies on the timestamp provided by enabling this command to identify duplicate traps. As a result, it is recommended that this parameter be enabled for this case.

Example

The following command enables the inclusion of a timestamp with each generated trap:

    snmp trap-timestamps
snmp user

Configures an SNMPv3 user for SNMP access.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
snmp user user_name [ [ encrypted ] password password ] | engine id | group grp_name | security-model model auth [ [ encrypted ] password password ] ]

no snmp user user_name
```

**no snmp user user_name**

Removes the specified user from the list of valid SNMPv3 users.

**user_name**

Specifies the user which is to use SNMPv3 interfaces to the system. *user_name* must be an alphanumeric string of 1 through 31 characters.

**engine id**

The SNMP engine ID. *id* must be an alphanumeric string of 1 through 31 characters.

**group grp_name**

Default: undefined (not a member of any group)

Specifies the user SNMPv3 group the into which user will be added. *grp_name* must be an alphanumeric string of 1 to 1023 characters.

**security-model model auth**

Default: USM

Specifies the security model used to authenticate the user. *model* must be configured to the following:

- usm: User Security Model

**[ encrypted ] password password**

Default: undefined

Specifies the password for authenticating the user when the security model is set to User-based Security Model (USM).
The encrypted keyword indicates the password will be received in an encrypted form. password must be an alphanumeric string of 8 through 31 characters.
The encrypted keyword is intended only for use by the chassis while saving configuration scripts. The system displays the encrypted keyword in the configuration file as a flag that the variable following the password keyword is the encrypted version of the plain text password. Only the encrypted password is saved as part of the configuration file.

Usage
Add and remove SNMPv3 users as operations staff or automated systems are updated. The security model will be user dependant based upon the support the user's system provides.

Important: The system can send either SNMPv1, SNMPv2c, or SNMPv3 traps to numerous target devices. However, the Web Element Manager can only process SNMP version 1 (SNMPv1) and SNMP version 2c (SNMPv2c) traps. If the SNMP target being configured is the Web Element Manager application, then you must not configure this command to use.

Example

```
snmp user user1
snmp user user1 security-model 2c auth
snmp user user1 group user1 group sampleGroup security-model usm auth
no snmp user user1
```
ss7-routing-domain

This command creates an SS7 routing domain instance and enters the SS7 Routing Domain Configuration mode.

**Product**

SGSN
HNB-GW

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local] host_name(config) #
```

**Syntax**

```
ss7-routing-domain rd_id variant v_type [ -noconfirm ]
no ss7-routing-domain rd_id
```

**no**

Removes the specified SS7 routing domain from the system configuration.

**rd_id**

Identifies a specific SS7 routing domain. Once it has been created, it can be accessed for further configuration and modification by entering the `rd_id` without entering the variant.

`rd_id` must be an integer from 1 through 12.

**variant v_type**

Identifies the national standard to be used for call setup, routing and control, signaling. Select one of the following:

- **ansi**: American National Standards Institute (U.S.A.)
- **bici**: Broadband Intercarrier Interface standard
- **china**: Chinese standard
- **itu**: International Telecommunication Union (ITU-T) Telecommunication Standardization Sector
- **ntt**: Japanese standard
- **ttc**: Japanese standard

**-noconfirm**

Indicates that the command is to execute without any additional prompt and confirmation from the user.
Usage

Use this command to create an SS7 routing domain configuration instance or to enter the SS7 routing domain configuration mode to edit the configuration.

A routing domain groups configuration items to facilitate the management of the SS7 connection resources for an SGSN service. An Access Gateway supports up to 12 configured SS7 routing domains at one time.

After entering this command, the prompt appears as:

[context_name]<hostname>(config-ss7-routing-domain-routing_domain_id)#

For details about the commands and parameters used to define or edit an SS7 routing domain, refer SS7 Routing Domain Configuration Mode chapter.

Example

The following creates an SS7 routing domain with an index of 1 and the variant selection of Broadcast Intercarrier Interface (bici):

```
ss7-routing-domain 1 variant bici
```

The following command creates an SS7 routing domain instance with an index of 2 and the variant selection of Broadcast Intercarrier Interface (bici) to be associated with HNB RN-PLMN in an HNB access network:

```
ss7-routing-domain 2 variant bici
```
statistics-backup-interval

This command defines the time between backups of the service’s key KPI statistics.

Product
MME
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

statistics-backup-interval minutes

no statistics-backup-interval

no

Disables the interval configuration.

minutes

Enter an integer from 1 to 60 to define the number of minutes for the interval between each backup.

Usage

This interval should only be defined after the statistics-backup command has been entered to configure the MME or SGSN to enable backup of statistics. For details on the feature, refer to the Backup and Recovery of Key KPI Statistics feature chapter in either the MME Administration Guide or the SGSN Administration Guide.

Example

Set the interval between backups to 30 minutes with the following command:

statistics-backup-interval 30
support collection

Modifies and/or enables the Support Data Collector (SDC) process. If record collection has been previously disabled, this command enables the collection activity. If the record collection is currently enabled, this command may be used to modify the sleep-duration interval and/or the maximum number of Support Data Records (SDRs) that can be collected and stored.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

support collection sleep-duration { hours | minutes } value max-records number_records

no support collection

default support collection

---

no

Removes the settings for support collection and effectively disables the SDC.

---

default

Resets the sleep duration and maximum number of records to their default values.

---

support collection

Enables the SDC.

---

sleep-duration { hours | minutes } value

Specifies the hours and/or minutes between record collection activity. value must be an integer from 1 through 1000. The default setting is one hour (60 minutes).

---

**Important:** The period between SDRs is equal to the configured sleep-duration interval + the time taken to collect the previous record.

---

max-records number_records

Specifies the maximum number of records to maintain within the record collection. number_records must be an integer from 1 through 1000. When this value is exceeded, a new SDR overwrites the oldest SDR. Default is 168.
**Usage**

Use this command to control the amount of support information that is collected by the Support Data Collector. Increasing the sleep interval for data collection and reducing the number of records to be collected frees system resources for processing calls and storing other data records. For additional information, refer to the *System Administration Guide*.

**Example**

The following command sets the collection sleep interval to 30 minutes with a maximum of 100 records being stored:

```
support collection sleep-duration minutes 30 max-records 100
```
support record

Specifies the `show` commands that will be collected and output by the Support Data Collector (SDC) process in the specified record section(s). The order in which the record section commands are specified defines the order in which the collected support data record sections are saved.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration
`configure`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
support record section section_name command "command_string" [ section section_name command "command_string" ] ...

do support record { all | section section_name }

default support record section { all | section section_name }
```

- `no support record { all | section section_name }`
  Removes the specified record section or all sections from the output of the SDC. This effectively disables the support data collector mechanism.

- `default support record section { all | section section_name }`
  Resets all support record sections or the specified section to the default command listing.

- `section section_name`
  Identifies the record section as an alphanumeric string of 1 through 64 characters.

- `command "command_string"`
  Identifies a CLI `show` command to be included in the record section as an alphanumeric string of 1 through 256 characters enclosed in double quotation marks.

---

**Important:** Refer to the *System Administration Guide* for a comprehensive list of command strings that can be entered via this keyword.

You can add command strings to the record section by repeating the `section section_name command "command_string"` keywords.
Usage

Use this command to tune the output of the Support Data Collector to meet specific site requirements. Refer to the System Administration Guide for a complete description of the SDC feature.

**Important:** If the support record section command is not explicitly configured by the user, a default set of record section commands are used. These default record section commands are displayed when you run the show configuration verbose command. If support record section commands are explicitly configured, they replace the default commands.

Example

The following command creates a record section named show_ip_vrf containing the CLI command show ip vrf:

```
support record section vrf command "show ip vrf"
```
suspend local-user

Suspends a local-user administrative account.

Product
All

Privilege
Administrator

Mode
Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

[ no ] suspend local-user name

no
Removes the suspended status for the specified local-user account.

name
The name of the local-user account expressed as an alphanumeric string of 3 through 16 characters that is case sensitive.

Usage

This command allows a security administrator to suspend local-user administrative accounts. A “suspended” user cannot login to the system. The user’s account information (passwords, password history, etc.), however, is preserved.

Example

The following command suspends a local-user account called Inspector1:

    suspend local-user Inspector1

The following command removes the suspension from a local-user account called Admin300:

    no suspend local-user Admin300
**system**

Configures system information which is accessible via SNMP.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

```
configure
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
system { carrier-id mcc mcc_id mnc mnc_id | contact who | description string | hostname host_name | location text | serial-number ser_number | sysdesc-sysoid-style [ default | new ] }

default system { contact | location }

default
```

Removes the configured `system contact` and `system location` form the system.

```
carrier-id mcc mcc_id mnc mnc_id
```

**Important:** This carrier ID is not used by the GGSN.

Specifies a carrier-id that is a unique identifier for the carrier that has installed the system. When the carrier ID values are set, the carrier-id and gmt_offset attributes are included in access-request and accounting packets when using the following RADIUS dictionaries:

- 3gpp2
- 3gpp2-835
- starent
- starent-835
- starent-vsa1
- starent-vsa1-835
- custom9

**mcc mcc_id:** The mobile country code. This must be specified as a 3-digit string from 001 through 999.

**mnc mnc_id:** The mobile network code. This must be specified as a 2- or 3-digit string from 01 through 999.

```
contact who
```

Default: No contact specified.
contact who: specifies the contact information for the chassis. who must be an alphanumeric string of 0 through 255 characters. The string must be embedded in double quotes () if spaces and special punctuation is to be used.

description string

Allows a user to describe the system for identification purposes. The system description can be comprised of a mix of alphanumeric characters, as follows:

- %version% - software version.
- %build% - software build number
- %chassis% - chassis type (ST16, ASR 5000, or ASR 5500)
- %staros% - OS type
- %hostname% - system name
- %release% - release number
- %kerver% - kernel version
- %machine% - machine hardware name
- string - an alphanumeric string of 1 through 255 characters.

hostname host_name

hostname host_name: configures the chassis host name where host_name must be an alphanumeric string of 1 through 63 characters.

Important: Please note that changing the chassis host name results in the command prompt changing as well to reflect the new name. This may affect any previously scripted interfaces from an OSS or maintenance facility.

location text

Default: No location specified.

location text: specifies the system location expressed as an alphanumeric string of 0 through 255 characters. The text specified must be embedded in double quotes (") if spaces are to be used.

serial-number ser_number

Default: None.

Specifies a system identifier as an alphanumeric string of 1 through 11 characters.

sysdesc-sysoid-style [ default | new ]

Allows the user to select the SNMP return for the objects sysDescr and sysOid.

- default - SNMP returns old style system description and old style system OID string.
- new - SNMP returns Cisco style system description and Cisco style OID string.

Usage

Specify system basic information which is useful back at a network operations center which uses the SNMP interfaces for management.

Example
The following commands configure the contact information, system host name, and location text, or remove configured location and system respectively.

```
  system contact user1@company.com
  system hostname system16
  system location "Clark Street Closet\nBasement Rack 4"
```

The following commands remove the configured contact and location from system respectively

```
  default system contact
  default system location
```
Chapter 142
Global Configuration Mode Commands (T-threshold phspc)

This section includes the commands `tacacs mode` through `threshold phspc-sm-entry-denial`.
The Global Configuration Mode is used to configure basic system-wide parameters.

Mode

Exec > Global Configuration
`configure`

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
tacacs mode

Enters the TACACS+ (Terminal Access Controller Access Control System+) configuration mode. Use this mode to configure up to three TACACS+ servers for use in authenticating administrative users via the TACACS+ protocol.

Product
- All

Privilege
- Security Administrator, Administrator

Mode
- Exec > Global Configuration
  - configure

Entering the above command sequence results in the following prompt:

[local] host_name(config) #

Syntax

tacacs mode

Usage
Enter TACACS Configuration Mode to configure up to three TACACS+ servers for use in authenticating administrative users via the TACACS+ protocol. For additional information, see the TACACS+ Configuration Mode Commands chapter.

Example
Use the following command to enter TACACS mode:

  tacacs mode
task facility acsmgr

This command configures ACSMgr task settings.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure
Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

task facility acsmgr start [ aggressive | normal ]

no task facility acsmgr start

Usage
This command provides option for the resource subsystem to start maximum possible ACSMgr tasks based on the license configured and the available system configuration.

Example
The following command starts the maximum possible ACSMgr tasks:

    task facility acsmgr start aggressive
task facility imsimgr

This command is used to configure the IMSI Manager parameters.

Product
SGSN
MME

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

```
task facility imsimgr { avoid-sessmgr-broadcast | required-sessmgr no_sess_mgrs |
sessmgr-sessions-threshold high-watermark <high_value> low-watermark <low_value> }

no task facility imsimgr [ avoid-sessmgr-broadcast | required-sessmgr ]

default task facility imsimgr sessmgr-sessions-threshold
```

**no**

Disables the selected parameter’s functionality in the configuration.

**default**

This prefix is only used with the `sessmgr-sessions-threshold` parameter. By default, the threshold levels are set to the maximum allowed sessions per Session Manager based on the card type. Both high and low watermarks are set to “100”% by default to ensure backward compatibility.

**avoid-sessmgr-broadcast**

This keyword configures the IMSIMgr to avoid or disable broadcast requests to all SessMgrs when the IMSIMgr finds a particular IMSI is unknown. With this keyword, broadcasting can be disabled ‘on the fly’ if CPU usage is too high due to a large number of broadcast messages.

By default, broadcasting is enabled.

**required-sessmgr**

SGSN only.

This keyword configures the required number of Session Manager instances at the IMSI Manager. By default, this parameter is disabled to ensure backward compatibility.

`no_sess_mgrs`: The number of required Session Managers can be an integer value from “1” through “384”.

Global Configuration Mode Commands (T-threshold phspc)

**sessmgr-sessions-threshold**

This option is used to configure the threshold high and low watermarks, in terms of percentage, for the sessions per Session Manager. The actual session limits are derived based on the card type.

- **high-watermark** `high_value`: The high-watermark value can be a percentage value from “70” through “100”. The default percentage value is “100”.
- **low-watermark** `low_value`: The low-watermark value can be a percentage value from “50” through “100”. The default percentage value is “100”.

**Usage**

For the MME:

Typically, the `avoid-sessmgr-broadcast` and `sessmgr-sessions-threshold` keywords are available for configuration but not used.

For the SGSN:

This command configures the number of Session Manager instances required at the IMSI Manager before forwarding any calls from the Gb Manager or Link Manager, as well, it configures the high watermark and low watermark threshold levels per Session Manager.

If the required number of Session Managers are configured through this command, once the Link Manager or Gb Manager comes up, it sends a query to the IMSI Manager to verify if the IMSI Manager has learnt the configured number of Session Manager instances. IMSI Manager readiness status is determined based on the number of Session Manager instances present in the list maintained. Once the IMSI Manager has completed learning about all the required number Session Manager instances, it informs the Link Manager and Gb Manager. Runtime enabling and modification of Session Manager instance is disabled except disabling this configuration. Disabling of this configuration does not affect the call forwarding to the IMSI Manager as the default behavior is to always forward the calls to the IMSI Manager. This configuration is used to avoid the session imbalance across Session Manager instances due to call forwarding to the same Session Manager instance during or after re-load, if the IMSI Manager has learnt only few Session Manager instances. By default, this feature is disabled and Gb Manager or Link Manager start forwarding calls immediately during or after re-load to the IMSI Manager which in turn forwards the request to the available Session Manager instances. It is recommended to have this configuration before re-load. This option is available only under a SGSN license.

The high and low watermark limits allow the IMSI Manager to decide and select the Session Manager for processing new calls and eliminate the chances of it receiving a “call reject” in instances where the Session Manager has reached its maximum allowed session limits and the IMSI Manager is not aware of the same.

The IMSI Manager converts the high and low watermark percentage to the maximum session allowed for the configured percentage based on the card type. It uses the calculated session values for both high and low watermark to decide and select the Session Manager for processing new calls. Once the Session Manager active session count reaches the calculated high watermark sessions the IMSI Manager stops forwarding the new calls to the Session Manager until the active session count becomes less than the calculated low watermark value. This option is available only under SGSN and MME licenses.

**Example**

Use the following command to configure the required session manager count to be learnt by IMSI Manager for processing new calls to “28”:

```
task facility imsimgr required-sessmgr 28
```

Use the following command to configure the threshold for the sessions per Session Manager:

```
task facility imsimgr sessmgr-sessions-threshold high-watermark 95 low-watermark 85
```
task facility ipsecmgr

Configures IPSec manager settings.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

```
task facility ipsecmgr { ikev1 { task-count { increased | normal } } | task-count { increased | normal } }
```

ikev1 { task-count { increased | normal } }

Default: normal
Adjusts the IPSec manager task count to support EHA for IKEv1. See task-count below.

```
task-count { increased | normal }
```

Default: normal
Adjusts the IPSec manager task count to support EHA.

increased: Starts additional IPSec manager tasks operating on the packet processing cards. In increased mode, they run on all but demux packet processing cards. Also, all the IPSec managers start at the same time when an active non-demux card is detected and IPSec is configured.

normal: Uses the standard algorithm for allocating memory for IPSec manager tasks. In normal mode, IPSec managers do not run on session packet processing cards.

⚠️ Caution: If task-count is set to normal and session recovery is enabled, IPSec manager tasks are not allowed to start on most packet processing cards. Because the resources are not reserved, IPSec managers in normal mode only run on demux packet processing cards.

Usage
Sets IPSec manager parameters for all IPSec managers in the system.

Example
Use the following command to set the IPSec manager task count to increased mode:

```
task facility ipsecmgr task-count increased
```
task facility linkmgr

This command controls the maximum number of Link Managers that can be configured for an SGSN.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator.

**Mode**
Exec > Global Configuration

```configure```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
task facility linkmgr max max_linkmgrs
```

```default```

default task facility linkmgr max

```default```

Resets the value to 4.

```max max_linkmgrs```

Sets the maximum number of LinkMgrs configurable for the SGSN.

`max_linkmgrs` is an integer from 1 to 4. With Release 15.0, the range is from 1 to 12.

**Usage**

By default, 4 LinkMgrs will be started in the system when an SGSN service configuration is present. Use this command to change the maximum number of LinkMgrs to be started in the system.

**Important:** If a change to the default is needed, this command must be used before configuring any SGSN service-related configuration, including SS7 Routing Domain and SCCP Network configurations.

The number of LinkMgrs configurable impacts the following SS7 routing domain components:

- The number of Application Server Process (ASP) instances that can be configured (maximum of 12).
- The number of peer-servers that can be configured across all SS7RDs (maximum of 512).
- The number of peer-servers that can be configured per SS7RD (maximum of 256).
- The number of Peer-Server Process (PSP) instances that can be configured per SS7 Peer (maximum of 12).
**Important:** This command cannot be set dynamically. If the LinkMgr count is modified dynamically, the system must be rebooted for the change to take effect.

**Example**

Change the maximum number of LinkMgrs that can be configured for an SGSN from 4 to 8:

```
task facility linkmgr max 8
```
**task facility mmedemux**

Configures wait-time and percentage parameters related to the MMEDEMUX. The MMEDEMUX distributes the incoming traffic to the associated MMEMGRs based on the percentage value and wait-time configured in this command.

**Product**
MME.

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
task facility mmedemux mmemgr-startup-percentage percent_value [ mmemgr-startup-wait-time wait_time ]
[ default | no ] task facility mmedemux mmemgr-startup-percentage mmemgr-startup-wait-time
```

Either of these command filters disables the operator defined configuration and replaces the configuration with default values.

---

**mmemgr-startup-percentage percent_value**

The percentage parameter allows the operator to configure the percentage of MMEMGRs to be associated with the MMEDEMUX.

*percent_value* must be an integer from 1 to 100. Default is 90%.

---

**mmemgr-startup-wait-time wait_time**

This parameter enables the operator to configure the time (in seconds) that the MMEDEMUX waits for MMEMGRs to start before processing incoming traffic.

*wait_time* must be an integer from 300 to 3600. Default is 600 (10 minutes).

---

**Usage**

This command gives operators some control over the MMEDEMUX system. It allows operators to configure the percentage of MMEMGRs to be associated with the MMEDEMUX. It also assigns the waiting time before processing the incoming traffic. Incoming traffic is distributed to the MMEMGRs based on a combination of the configured values of the two parameters.

By default, the MME waits for ten minutes to check if 90% of the MMEMGRs have started.

---

**Example**

...
The following configures the MMEDEMUX to distribute incoming traffic after a minimum of 5 minutes after the MME starts and as soon as 75% of the MMEMGRs are up and running:

```
task facility mmedemux mmemgr-startup-percentage 75 mmemgr-startup-wait-time 5
```
**task facility sessmgr**

Configures system information which is accessible via SNMP.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

```configure```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config)#
```

**Syntax**

```task { facility sessmgr start { aggressive | normal }```

---

```facility sessmgr start { aggressive | normal }
Default: Normal
Specifies the facility options for the session manager.
aggressive: specifies the maximum number of session manager processes are started immediately.

---

⚠️ **Caution:** The **task facility sessmgr start aggressive** command should only be used if the system will reach capacity (for the existing configuration) during the first few minutes of service.

⚠️ **Caution:** This command must only be executed last during configuration (or appended to the end of the configuration file) to ensure the availability of memory resources to contexts and services.

**Usage**

Set the session manager start policy to aggressive on heavily utilized systems to avoid undue delays in processing subscriber sessions.

**Example**

```task facility sessmgr start aggressive

task facility sessmgr start normal```
task resource cpu-memory-low

Configures the system action for SNMP trap generation and logging whenever CPU memory.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local] host_name(config) #

**Syntax**

```plaintext
task resource cpu-memory-low { kill | warn }
```

Default: kill

Sets the action for the Resource Manager to take when the amount of free memory on a CPU falls below 12MB. An SNMP TRAP and CORBA notification are generated and the event is logged. Once the free memory threshold is crossed, The Resource Manager examines all tasks on that cpu and finds the most over limit task and kills it. If there are no over limit tasks nothing happens. Resource Manager takes preference on killing a non-sessmgr task over a sessmgr task.

**Example**

Set the CPU memory low action to only log CPU low memory events.

```plaintext
task resource cpu-memory-low warn
```
**tech-support test-commands password**

Configures the password that protects access to the `cli test-commands` mode in the Exec mode and Global Configuration mode. This command is only visible to a user logged in as a Security Administrator.

**Product**
All

**Privilege**
Security Administrator

**Caution:** The `cli test-commands` are for use by or under the supervision of Cisco TAC.

**Mode**
Exec > Global Configuration

```
configure
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
tech-support test-commands [encrypted] password password

no tech-support test-commands password
```

- **no**
  Disables the use of a test-commands password. All subsequent attempts to execute `cli test-commands` in Exec or Global Configuration modes will fail.
  Default: no password, access disabled

- **[encrypted]**
  If this optional keyword is specified, the `<password>` argument is interpreted as an encrypted string containing the password value. If the encrypted keyword is not specified, then the `<password>` argument is interpreted as the actual plain text value. In the output of `show configuration` and `save configuration` commands, only the encrypted option of this command syntax appears.

- **password**
  Specifies the password to be used when executing the `cli test-commands` command in Exec or Global Configuration modes. For a plain text password, `password` is an alphanumeric string of 1 through 64 characters. For an encrypted password, `password` is an alphanumeric string of 1 through 524 characters.
  If a password is not entered via this command, the `cli test-commands` command remains disabled in the Exec and Global Configuration modes.
  Default: no password, access disabled

**Important:** An SNMP trap is generated when an administrator enters or edits a password via this command (`starTechSupportPasswordChanged`). Refer to the `SNMP MIB Reference` for additional information.
Usage
Sets the password required to execute the `cli test-commands` command in the Exec and Global Configuration mode.

**Important:** Access to the `cli test-commands` command also requires that a Security Administrator or Administrator enabled the Global Configuration mode `cli hidden` command.

Example
The following command sets the password for `cli test-commands` to `testCommander`.

```
tech-support test-commands password testCommander
```
**terminal**

Configures the console port on the SPIO.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

**configure**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
terminal [ carrierdetect { off | on } | databits { 7 | 8 } | flowcontrol { hardware { off | on } | none } | parity { even | none | odd } | speed { 115200 | 19200 | 38400 | 57600 | 9600 } | stopbits { 1 | 2 } ]
```

- **carrierdetect { off | on }**
  Specifies whether or not the console port is to use Data Carrier Detect (DCD) when connecting to a terminal.
  Default: off
  - off: Do not use DCD.
  - on: Use DCD.

- **databits { 7 | 8 }**
  Specifies the number of data bits used to transmit and receive characters.
  Default: 8
  - 7: Use 7 databits to transmit and receive characters.
  - 8: Use 8 databits to transmit and receive characters.

- **flowcontrol { hardware { off | on } | none }**
  Specifies how the flow of data is controlled between the SPIO and a terminal.
  Default: none
  - hardware: Enables or disables the use of hardware-based flow control
  - off: Disables the use of Ready to Send (RTS) and Clear to Send (CTS).
  - on: Enables the use of Ready to Send (RTS) and Clear to Send (CTS).
  - none: Disables the use of DCD, RTS and CTS.

- **parity { even | none | odd }**
  Specifies the type of error checking used on the port.
  Default: none
  - even: Enables error checking by setting the parity bit to 1 (if needed) making the number of 1s in the data bits even.
  - none: Disables error checking.
**odd** - Enables error checking by setting the parity bit to 1 (if needed) making the number of 1s in the data bits odd.

**speed** { 115200 | 19200 | 38400 | 57600 | 9600 }

Specifies the flow of data in bits per second between the console port and terminal.
Default: 9600

**stopbits** { 1 | 2 }

Specifies the number of stop bits between each transmitted character.
Default: 1
1: Use one stop bit between each transmitted character.
2: Use two stop bits between each transmitted character.

**Usage**

Sets the SPIO’s console port parameters for communication with the terminal device.

**Example**

The following command sets the SPIO’s console port. The terminal must support these values.

```
terminal carrierdetect off databits 7 flowcontrol hardware on parity even speed 115200 stopbits 1
```
threshold 10sec-cpu-utilization

Configures alarm or alert thresholds that measure a 10-second average of CPU utilization. Its polling interval can be set down to 30 seconds.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

```bash
configure
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
threshold 10sec-cpu-utilization percent [ clear percent ]
```

- **percent**
  Default: 0
  Configures Specifies the high threshold for 10-second average cpu-utilization. If the monitored CPU utilization is greater than or equal to the specified percentage an alert is sent. Regardless of the length of the polling interval, only one sample at the end of the polling interval is tested.

- **clear percent**
  Default: 0
  This is a low watermark value that sets the alarm clearing threshold value. If not specified it is taken from the first value.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**

Use this command to set a threshold that sends an alert when CPU utilization over a 10-second average exceeds the limit set.

Alerts or alarms are triggered for 10-second sample of CPU utilization based on the following rules:

- **Enter condition:** 10-second average percentage of CPU utilization is greater than or equal to the high threshold.
- **Clear condition:** 10-second average percentage of CPU utilization is less than the low threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.
Global Configuration Mode Commands (T-threshold phspc)

threshold 10sec-cpu-utilization

**Important:** This command is not supported on all platforms.

Example

The following command generates an alert when the 10-second average CPU utilization reaches 45 percent:

```
threshold 10sec-cpu-utilization 45
```
threshold aaa-acct-archive-queue-size

Configures AAA accounting archive, alarm or alert thresholds based on the maximum values of session manager and ACS manager archive queue size.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold aaa-acct-archive-queue-size1 percent [ clear percent ]
default threshold aaa-acct-archive-queue-size1 percent [ clear percent ]
threshold aaa-acct-archive-queue-size2 percent [ clear percent ]
default threshold aaa-acct-archive-queue-size2 percent [ clear percent ]
threshold aaa-acct-archive-queue-size3 percent [ clear percent ]
default threshold aaa-acct-archive-queue-size3 percent [ clear percent ]

percent

Configures Specifies the high threshold for monitoring the accounting message archive queue length. If the queue length is greater than or equal to the specified percentage an alarm is sent.
Default value for aaa-acct-archive-queue-size1: 25%
Default value for aaa-acct-archive-queue-size2: 50%
Default value for aaa-acct-archive-queue-size3: 90%

clear percent

This is a low watermark value that sets the alarm clearing threshold value. If not specified it is taken from the first value.
Default value for aaa-acct-archive-queue-size1: 25%
Default value for aaa-acct-archive-queue-size2: 50%
Default value for aaa-acct-archive-queue-size3: 90%

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.
Usage

In the event that the system cannot communicate with configured AAA accounting servers (RADIUS or CGFs), either due to the server being busy or loss of network connectivity, the system buffers, or archives, the accounting messages.

Accounting message archive queue size thresholds generate alerts or alarms based on the queue length of AAA accounting messages buffered in the archive during the specified polling interval. Accounting requests are counted for all AAA accounting servers that the system is configured to communicate with.

Alerts or alarms are triggered for accounting message archive queue size thresholds based on the following rules:

- **Enter condition:** Actual number of archived messages is greater than or equal to the high threshold.
- **Clear condition:** Actual number of archived messages less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

Example

The following command generates an alarm when 70% of the AAA accounting message archive buffer is filled, and clears the alarm when the buffer size is reduced to 30%:

```
threshold aaa-acct-archive-queue-size1 70 clear 30
```
threshold aaa-acct-archive-size

Configures accounting message archive size, alarm or alert thresholds.

**Product**
- PDSN
- GGSN
- HA
- ASN-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration
   `configure`

Entering the above command sequence results in the following prompt:
```
[local]host_name(config)#
```

**Syntax**
```
threshold aaa-acct-archive-size high_thresh [ clear low_thresh ]

default threshold aaa-acct-archive-size
```

### high_thresh

Default: 1
Specifies the high threshold number of archived accounting messages that must be met or exceeded within the polling interval to generate an alert or alarm. `high_thresh` is an integer from 0 through 1044000.

### clear low_thresh

Default: 1
Specifies the low threshold number of archived accounting messages that maintains a previously generated alarm condition. If the number of failures falls beneath the low threshold within the polling interval, a clear alarm will be generated. `low_thresh` is an integer from 0 through 1044000.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**
In the event that the system cannot communicate with configured AAA accounting servers (RADIUS or CGFs), either due to the server being busy or loss of network connectivity, the system buffers, or archives, the accounting messages.
Accounting message archive size thresholds generate alerts or alarms based on the number of AAA accounting messages buffered in the archive during the specified polling interval. Accounting requests are counted for all AAA accounting servers that the system is configured to communicate with.
Alerts or alarms are triggered for accounting failures based on the following rules:

- **Enter condition**: Actual number of archived messages that is greater than or equal to the high threshold.

- **Clear condition**: Actual number of archived messages that is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Example**

The following command configures a high threshold count of 250 AAA accounting archived messages and low threshold of 100 for a system using the Alarm thresholding model:

```
threshold aaa-acct-archive-size 250 clear 100
```
threshold aaa-acct-failure

Configures accounting failure, alarm or alert thresholds for the system.

Product

- PDSN
- GGSN
- HA
- ASN-GW

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold aaa-acct-failure high_thres [ clear low_thres ]

default threshold aaa-acct-failure

- **high_thres**
  - Default: 0
  - Specifies the high threshold number of accounting failures that must be met or exceeded within the polling interval to generate an alert or alarm. *high_thres* is an integer from 0 through 10000000. A value of 0 disables the threshold.

- **clear low_thres**
  - Default: 0
  - Specifies the low threshold number of accounting failures that maintains a previously generated alarm condition. If the number of failures falls beneath the low threshold within the polling interval, a clear alarm will be generated. *low_thres* is an integer from 0 through 10000000. A value of 0 disables the threshold.

**Important**: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Accounting failure thresholds generate alerts or alarms based on the number of failed AAA accounting message requests that occur during the specified polling interval. Accounting requests are counted for all AAA accounting servers that the system is configured to communicate with. Alerts or alarms are triggered for accounting failures based on the following rules:

- **Enter condition**: Actual number of failures is greater than or equal to the high threshold.
• **Clear condition:** Actual number of failures is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Example**

The following command configures a high threshold count of 100 AAA accounting failures and low threshold of 25 for a system using the Alarm thresholding model:

```
threshold aaa-acct-failure 100 clear 25
```
threshold aaa-acct-failure-rate

Configures accounting failure rate, alarm or alert thresholds for the system.

Product
PDSN
GGSN
HA
ASN-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold aaa-acct-failure-rate high_thresh [ clear low_thresh ]

default threshold aaa-acct-failure-rate

**high_thresh**

Default: 1
Specifies the high threshold percent of accounting failures that must be met or exceeded within the polling interval to generate an alert or alarm. high_thresh is an integer from 0 and 100.

**clear low_thresh**

Default: 1
Specifies the low threshold percent of accounting failures that maintains a previously generated alarm condition. If the percentage of failures falls beneath the low threshold within the polling interval, a clear alarm will be generated. low_thresh is an integer from 0 through 100.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**

Accounting failure rate thresholds generate alerts or alarms based on the percentage of AAA accounting message requests that failed during the specified polling interval. Accounting requests are counted for all AAA accounting servers that the system is configured to communicate with.

Alerts or alarms are triggered for accounting failure rates based on the following rules:

- **Enter condition:** Actual failure percentage is greater than or equal to the high threshold.
- **Clear condition:** Actual failure percentage is less than the low threshold.
If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

Example

The following command configures a AAA accounting failure rate high threshold percentage of `30` and a low threshold percentage of `10` for a system using the Alarm thresholding model:

```
threshold aaa-acct-failure-rate 30 clear 10
```
threshold aaa-auth-failure

Configures authentication failure, alarm or alert thresholds for the system.

Product
PDSN
GGSN
HA
ASN-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold aaa-auth-failure high_thresh [ clear low_thresh ]

default threshold aaa-auth-failure

<table>
<thead>
<tr>
<th>high_thresh</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default: 0</td>
</tr>
<tr>
<td>Specifies the high threshold number of authentication failures that must be met or exceeded within the polling interval to generate an alert or alarm. high_thresh is an integer from 0 through 10000000. A value of 0 disables the threshold.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>clear low_thresh</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default: 0</td>
</tr>
<tr>
<td>Specifies the low threshold number of authentication failures that maintains a previously generated alarm condition. If the number of failures falls beneath the low threshold within the polling interval, a clear alarm will be generated. low_thresh is an integer from 0 through 10000000. A value of 0 disables the threshold.</td>
</tr>
</tbody>
</table>

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Authentication failure thresholds generate alerts or alarms based on the number of failed AAA authentication message requests that occur during the specified polling interval. Authentication requests are counted for all AAA authentication servers that the system is configured to communicate with. Alerts or alarms are triggered for authentication failures based on the following rules:
- **Enter condition:** Actual number of failures is greater than or equal to the high threshold.
- **Clear condition:** Actual number of failures is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Example**

The following command configures a high threshold count of 100 AAA authentication failures for a system using the Alert thresholding model:

```
threshold aaa-auth-failure 100
```
threshold aaa-auth-failure-rate

Configures authentication failure rate, alarm or alert thresholds for the system.

Product
PDSN
GGSN
HA
ASN-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold aaa-auth-failure-rate high_thresh [ clear low_thresh ]
default threshold aaa-auth-failure-rate

| high_thresh
| Default: 5
| Specifies the high threshold percent of authentication failures that must be met or exceeded within the polling interval to generate an alert or alarm. high_thresh is an integer from 0 through 100.

| clear
| Allows the configuration of Specifies the low threshold.

| low_thresh
| Default: 5
| Specifies the low threshold percent of authentication failures that maintains a previously generated alarm condition. If the percentage of failures falls beneath the low threshold within the polling interval, a clear alarm will be generated. low_thresh is an integer from 0 through 100.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.
Usage

Authentication failure rate thresholds generate alerts or alarms based on the percentage of AAA authentication message requests that failed during the specified polling interval. Authentication requests are counted for all AAA authentication servers that the system is configured to communicate with. Alerts or alarms are triggered for authentication failures based on the following rules:

- **Enter condition**: Actual failure percentage is greater than or equal to the high threshold.
- **Clear condition**: Actual failure percentage is less than the low threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

Example

The following command configures a AAA authentication failure rate high threshold percentage of 30 for a system using the Alert thresholding model:

```
threshold aaa-auth-failure-rate 30
```
threshold aaa-retry-rate

Configures AAA retry rate, alarm or alert thresholds for the system.

Product
PDSN
GGSN
HA
ASN-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold aaa-retry-rate high_thresh [ clear low_thresh ]

default threshold aaa-retry-rate

high_thresh
Default: 5
Specifies the high threshold percent of AAA request message retries that must be met or exceeded within the polling interval to generate an alert or alarm. high_thresh is an integer from 0 through 100.

clear low_thresh
Default: 5
Specifies the low threshold percent of AAA request message retries that maintains a previously generated alarm condition. If the percentage of retries falls beneath the low threshold within the polling interval, a clear alarm will be generated. low_thresh is an integer from 0 through 100.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

AAA request message retry rate thresholds generate alerts or alarms based on the percentage of request messages (both authentication and accounting) that were retried during the specified polling interval. The percentage is based on a message count taken for all AAA authentication and accounting servers that the system is configured to communicate with.
Alerts or alarms are triggered for request message retries based on the following rules:

● Enter condition: Actual retry percentage is greater than or equal to the high threshold.
• **Clear condition:** Actual retry percentage is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Example**

The following command configures a AAA message retry rate high threshold percentage of 25 and a low threshold percentage of 10 for a system using the Alarm thresholding model:

```
threshold aaa-retry-rate 25 clear 10
```
threshold aaamgr-request-queue

Configures the AAA Manager internal request queue, alarm or alert thresholds.

**Product**
- PDSN
- GGSN
- HA
- ASN-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration
configured

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
threshold aaamgr-request-queue high_thresh [ clear low_thresh ]
```

default threshold aaamgr-request-queue

```
high_thresh
Default: 0
Specifies the high threshold number of AAA Manager Requests that must be met or exceeded within the polling interval to generate an alert or alarm. high_thresh is an integer from 1 through 100.
```

```
clear
Allows the configuration of Specifies the low threshold.
```

```
low_thresh
Default: 5
Specifies the low threshold number of AAA Manager Requests that maintains a previously generated alarm condition. If the percentage of failures falls beneath the low threshold within the polling interval, a clear alarm is generated. low_thresh is an integer from 0 through 100.
```

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**

AAA Manager Request thresholds generate alerts or alarms based on the number of AAA Manager Requests for an AAA manager process during the specified polling interval.

Alerts or alarms are triggered for AAA Manager Requests based on the following rules:
- Enter condition: Actual number of AAA Manager Requests per AAA manager is greater than or equal to the high threshold.

- Clear condition: Actual number of AAA Manager Requests per AAA manager process is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm is not generated until the end of the polling interval. Refer to the threshold poll command to configure the polling interval and the threshold monitoring command to enable thresholding for this value.

Example

The following command configures a AAA authentication failure rate high threshold percentage of 30 for a system using the Alert thresholding model:

```
threshold aaamgr-request-queue 30
```
threshold asngw-auth-failure

Configures authentication failure, alarm or alert thresholds for the ASN-GW system.

Product
ASN-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold asngw-auth-failure high_thresh [ clear low_thresh ]

default threshold asngw-auth-failure

| high_thresh  
| Default: 0  
| Specifies the high threshold number of authentication failures that must be met or exceeded within the polling interval to generate an alert or alarm.  
| *high_thresh* is an integer from 0 through 10000000. A value of 0 disables the threshold. |

| clear low_thresh  
| Default: 0  
| Specifies the low threshold number of authentication failures that maintains a previously generated alarm condition. If the number of failures falls beneath the low threshold within the polling interval, a clear alarm will be generated.  
| *low_thresh* is an integer from 0 through 10000000. A value of 0 disables the threshold. |

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Use this command to configure threshold limits to generate alerts or alarms based on the number of failed ASN-GW authentication message requests that occur during the specified polling interval. Authentication requests are counted for all ASN Gateway authentication servers with which the system is configured to communicate. Alerts or alarms are triggered for authentication failures based on the following rules:

- **Enter condition:** Actual number of failures is greater than or equal to the high threshold.
- **Clear condition:** Actual number of failures is less than the low threshold.
If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Example**

The following command configures a high threshold count of 100 authentication failures for an ASN-GW using the Alert thresholding model:

```
  threshold asngw-auth-failure 100
```
threshold asngw-handoff-denial

Configures alarm or alert thresholds for hand-off denials within the ASN-GW service.

Product
ASN-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

```plaintext
threshold asngw-handoff-denial high_thresh [ clear low_thresh ]

default threshold asngw-handoff-denial
```

**high_thresh**

Default: 0
Specifies the high threshold number of hand-off denials that must be met or exceeded within the polling interval to generate an alert or alarm.

*high_thresh* is an integer from 0 through 10000000. A value of 0 disables the threshold.

**clear low_thresh**

Default: 0
Specifies the low threshold number of hand-off denials that maintains a previously generated alarm condition. If the number of hand-off denials falls beneath the low threshold within the polling interval, a clear alarm will be generated.

*low_thresh* is an integer from 0 through 10000000. A value of 0 disables the threshold.

⚠️ Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Use this command to set threshold limits to generate alerts or alarms based on the number of denied hand-off that occurred during the specified polling interval. Hand-off denial messages are counted for all ASN Gateways that the system is configured to communicate with.

Alerts or alarms are triggered for hand-off denials based on the following rules:

- **Enter condition:** Actual number of failures is greater than or equal to the high threshold.
- **Clear condition:** Actual number of failures is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

Example

The following command configures a high threshold count of 100 hand-off denials using the Alert thresholding model:

```
threshold asngw-handoff-denial 100
```
**threshold asngw-max-eap-retry**

Configures alarm or alert thresholds for maximum retries for Extensible Authentication Protocol (EAP) authentication within an ASN-GW service.

**Product**
ASN-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

`configure`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
threshold asngw-max-eap-retry high_thresh [ clear low_thresh ]
```

**default threshold asngw-max-eap-retry**

- `high_thresh`
  Default: 0
  Specifies the high threshold number of retries for EAP authentication that must be met or exceeded within the polling interval to generate an alert or alarm.
  `high_thresh` is an integer from 0 through 10000000. A value of 0 disables the threshold.

- `clear low_thresh`
  Default: 0
  Specifies the low threshold number of retries for EAP authentication that maintains a previously generated alarm condition. If the number of retries falls beneath the low threshold within the polling interval, a clear alarm will be generated.
  `low_thresh` is an integer from 0 through 10000000. A value of 0 disables the threshold.

---

**Important**: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

---

**Usage**

Use this command to set threshold limits to generate alerts or alarms based on the number of retries for EAP authentication that occur during the specified polling interval.

Alerts or alarms are triggered for maximum number of retries for EAP authentication based on the following rules:

- **Enter condition**: Actual number of failures is greater than or equal to the high threshold.
- **Clear condition**: Actual number of failures is less than the low threshold.
If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval. Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Example**

The following command configures a high threshold count of 100 alerts or alarms generated on maximum number of retries for EAP authentication for an ASN Gateway using the Alert thresholding model:

```
threshold asngw-max-eap-retry 100
```
threshold asngw-network-entry-denial

Configures alarm or alert thresholds for denials of network entry to an MS within the ASN-GW service.

Product
ASN-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold asngw-network-entry-denial high_thresh [ clear low_thresh ]

default threshold asngw-network-entry-denial

| high_thresh |
| Default: 0 |
| Specifies the high threshold number of denial of network entry to an MS that must be met or exceeded within the polling interval to generate an alert or alarm. high_thresh is an integer from 0 through 10000000. A value of 0 disables the threshold. |

| clear low_thresh |
| Default: 0 |
| Specifies the low threshold number of denial of network entry to an MS that maintains a previously generated alarm condition. If the number of denials falls beneath the low threshold within the polling interval, a clear alarm will be generated. low_thresh is an integer from 0 through 10000000. A value of 0 disables the threshold. |

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Use this command to set threshold limits to generate alerts or alarms based on the number of network entry denials that occurred during the specified polling interval. Network denial messages are counted for an MS with which the system is configured to communicate. Alerts or alarms are triggered for network entry denials based on the following rules:

- **Enter condition:** Actual number of failures is greater than or equal to the high threshold.
- **Clear condition:** Actual number of failures is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Example**

The following command configures a high threshold count of 100 network entry denials for an MS using the Alert thresholding model:

```
threshold asngw-network-entry-denial 100
```
threshold asngw-session-setup-timeout

Configures alarm or alert thresholds for session setup timeouts in an ASN-GW service.

Product
ASN-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold asngw-session-setup-timeout high_thresh [ clear low_thresh ]

default threshold asngw-session-setup-timeout

<table>
<thead>
<tr>
<th>high_thresh</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default: 0</td>
</tr>
<tr>
<td>Specifies the high threshold number of timeouts during session setup that must be met or exceeded within the polling interval to generate an alert or alarm.</td>
</tr>
<tr>
<td>high_thresh is an integer from 0 through 10000000. A value of 0 disables the threshold.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>clear low_thresh</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default: 0</td>
</tr>
<tr>
<td>Specifies the low threshold number of timeouts during session setup that maintains a previously generated alarm condition. If the number of denials falls beneath the low threshold within the polling interval, a clear alarm will be generated.</td>
</tr>
<tr>
<td>low_thresh is an integer from 0 through 10000000. A value of 0 disables the threshold.</td>
</tr>
</tbody>
</table>

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Use this command to set threshold limits to generate alerts or alarms based on the number of timeouts during session setup that occurred during the specified polling interval.

Alerts or alarms are triggered for session setup timeouts based on the following rules:

- **Enter condition:** Actual number of failures is greater than or equal to the high threshold.
- **Clear condition:** Actual number of failures is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Example**

The following command configures a high threshold count of 100 timeouts during session setup using the Alert thresholding model:

```
threshold asngw-session-setup-timeout 100
```
threshold asngw-session-timeout

Configures alarm or alert thresholds for session timeouts in an ASN-GW service.

Product
ASN-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold asngw-session-timeout high_thresh [ clear low_thresh ]

default threshold asngw-session-timeout

- **high_thresh**
  
  Default: 0
  
  Specifies the high threshold number of timeouts during session that must be met or exceeded within the polling interval to generate an alert or alarm.
  
  **high_thresh** is an integer from 0 through 10000000. A value of 0 disables the threshold.

- **clear low_thresh**
  
  Default: 0
  
  Specifies the low threshold number of timeouts during session that maintains a previously generated alarm condition. If the number of session timeouts falls beneath the low threshold within the polling interval, a clear alarm will be generated.
  
  **low_thresh** is an integer from 0 through 10000000. A value of 0 disables the threshold.

⚠️ **Important**: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Use this command to set threshold limits to generate alerts or alarms based on the number of timeouts during a session that occurred during the specified polling interval.

Alerts or alarms are triggered for session timeouts based on the following rules:

- **Enter condition**: Actual number of failures is greater than or equal to the high threshold.
- **Clear condition**: Actual number of failures is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Example**

The following command configures a high threshold count of 100 timeouts during a session using the Alert thresholding model:

```
threshold asngw-session-timeout 100
```
threshold asnpc-idle-mode-timeout

Configures alarm or alert thresholds for ASNPC Instant Messenger idle mode timeouts.

**Product**
ASN-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
threshold asnpc-idle-mode-timeout high_thresh [ clear low_thresh ]
```

**high_thresh**
Default: 0
Specifies the high threshold number of ASNPC idle mode timeouts that must be met or exceeded within the polling interval to generate an alert or alarm.

**clear low_thresh**
Default: 0
Specifies the low threshold number of ASNPC idle mode timeouts during session that maintains a previously generated alarm condition. If the number of session timeouts falls beneath the low threshold within the polling interval, a clear alarm will be generated.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**
Set the maximum number of idle mode timeouts allowed in the ASNPC service. Alerts or alarms are triggered for session timeouts based on the following rules:

- **Enter condition:** Actual number of timeouts is greater than or equal to the high threshold.
- **Clear condition:** Actual number of timeouts is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.

**Example**
The following command configures the high threshold for ASNPC idle mode timeouts at 10000:

```
threshold asnpc-idle-mode-timeout 10000
```
threshold asnpc-idle-mode-timeout 10000
threshold asnpc-im-entry-denial

Configures the ASNPC Instant Messenger (IM) entry denial, alarm or alert thresholds.

Product
ASN-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:
[local]host_name(config)#

Syntax

```
threshold asnpc-im-entry-denial high_thresh [ clear low_thresh ]
```

- **high_thresh**
  Default: 0
  Specifies the high threshold number of IM entry denials during session that must be met or exceeded within the polling interval to generate an alert or alarm.
  high_thresh is an integer from 0 through 10000000. A value of 0 disables the threshold.

- **clear low_thresh**
  Default: 0
  Specifies the low threshold number of IM entry denials during session that maintains a previously generated alarm condition. If the number of session timeouts falls beneath the low threshold within the polling interval, a clear alarm will be generated.
  low_thresh is an integer from 0 through 10000000. A value of 0 disables the threshold.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Set the maximum number of IM session denials allowed in the ASNPC service. Alerts or alarms are triggered for session timeouts based on the following rules:
- **Enter condition:** Actual number of failures is greater than or equal to the high threshold.
- **Clear condition:** Actual number of failures is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

Example

The following command configures the high threshold for IM session counts at 10000:

```
threshold asnpc-im-entry-denial 10000
```
threshold asnpc -im -entry -denial 10000
threshold asnpc-lu-denial

Configures the alarm or alert thresholds for Location Update (LU) denials.

Product
ASN-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold asnpc-lu-denial high_thresh [ clear low_thresh ]

- **high_thresh**
  - Default: 0
  - Specifies the high threshold number of LU denials during session that must be met or exceeded within the polling interval to generate an alert or alarm.
  - **high_thresh** is an integer from 0 through 10000000. A value of 0 disables the threshold.

- **clear low_thresh**
  - Default: 0
  - Specifies the low threshold number of LU denials during session that maintains a previously generated alarm condition. If the number of session timeouts falls beneath the low threshold within the polling interval, a clear alarm will be generated.
  - **low_thresh** is an integer from 0 through 10000000. A value of 0 disables the threshold.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage
Set the maximum number of Location Update denials allowed in the ASNPC service.

Example
The following command configures high threshold of 10000 LU denials:

threshold asnpc-lu-denial 10000
threshold asnpc-session-setup-timeout

Configures alarm or alert thresholds for ASNPC session setup timeouts in an ASN-GW service.

**Product**
ASN-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

**Syntax**

```plaintext
threshold asnpc-session-setup-timeout value

default threshold asnpc-session-setup-timeout

value

value is an integer from 1 through 1000000.
```

**Usage**

Use this command to set threshold limits to generate alerts or alarms based on the number of timeouts during session setup that occurred during the specified polling interval.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Example**

The following command configures a high threshold count of 100 timeouts during session setup using the Alert thresholding model:

```plaintext
threshold asnpc-session-setup-timeout 100
```
threshold call-reject-no-resource

Configures alarm or alert thresholds on the system for calls rejected due to insufficient resources.

Product  
All

Privilege  
Security Administrator, Administrator

Mode  
Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold call-reject-no-resource high_thresh [ clear low_thresh ]

high_thresh

Default: 0
Specifies the high threshold number of no-resource call rejects issued by the system that must be met or exceeded within the polling interval to generate an alert or alarm.
The number is an integer from 0 through 100000. A value of 0 disables the threshold.

clear low_thresh

Default: 0
Specifies the low threshold number of no-resource call rejects issued by the system that maintains a previously generated alarm condition. If the number of rejections falls beneath the low threshold within the polling interval, a clear alarm will be generated.
The number is an integer from 0 through 100000. A value of 0 disables the threshold.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

No resource call reject thresholds generate alerts or alarms based on the total number of calls that were rejected by the system due to insufficient or no resources (memory and/or session licenses) during the specified polling interval.
Alerts or alarms are triggered for no-resource-rejected calls based on the following rules:

- **Enter condition:** Actual number of calls rejected due to no resources is greater than or equal to the high threshold.

- **Clear condition:** Actual number of calls rejected due to no resources is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

Example

The following command configures a high threshold count for the number of calls rejected by the system due to insufficient or no resources to 100 and allow threshold of 40 for a system using the Alarm thresholding model:

```
threshold call-reject-no-resource 100 clear 40
```
threshold call-setup

Configures call setup, alarm or alert thresholds for the system.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold call-setup high_thresh [ clear low_thresh ]

high_thresh
Default: 0
Specifies the high threshold number of calls setup by the system that must be met or exceeded within the polling interval to generate an alert or alarm.

high_thresh is an integer from 0 through 100000. A value of 0 disables the threshold.

clear low_thresh
Default: 0
Specifies the low threshold number of calls setup by the system that maintains a previously generated alarm condition. If the number of setups falls beneath the low threshold within the polling interval, a clear alarm will be generated.

low_thresh is an integer from 0 through 100000. A value of 0 disables the threshold.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Call setup thresholds generate alerts or alarms based on the total number of calls setup by the system during the specified polling interval.

Alerts or alarms are triggered for call setups based on the following rules:

• Enter condition: Actual number of call setups is greater than or equal to the high threshold.

• Clear condition: Actual number of call setups is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the threshold poll command to configure the polling interval and the threshold monitoring command to enable thresholding for this value.

Example
The following command configures a high threshold count of 100 calls setup for a system using the Alert thresholding model:

```
threshold call-setup 100
```
threshold call-setup-failure

Configures call setup failure, alarm or alert thresholds for the system.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

`configure`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
threshold call-setup-failure high_thresh [ clear low_thresh ]
```

- `high_thresh`
  Default: 0
  Specifies the high threshold number of call setup failures experienced by the system that must be met or exceeded within the polling interval to generate an alert or alarm.
  `high_thresh` is an integer from 0 through 100000. A value of 0 disables the threshold.

- `clear low_thresh`
  Default: 0
  Specifies the low threshold number of call setup failures experienced by the system that maintains a previously generated alarm condition. If the number of setup failures falls beneath the low threshold within the polling interval, a clear alarm will be generated.
  `low_thresh` is an integer from 0 through 100000. A value of 0 disables the threshold.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**

Call setup failure thresholds generate alerts or alarms based on the total number of call setup failures experienced by the system during the specified polling interval.

Alerts or alarms are triggered for call setup failures based on the following rules:

- **Enter condition:** Actual number of call setup failures is greater than or equal to the high threshold.
- **Clear condition:** Actual number of call setup failures is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Example**
The following command configures a high threshold count of 100 call setup failures and a low threshold of 80 for a system using the Alarm thresholding model:

```
threshold call-setup-failure 100 clear 80
```
**threshold card-temperature-near-power-off-limit**

Configures alarm or alert thresholds for triggering and clearing high card temperature alarms.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

```
configure
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
threshold card-temperature-near-power-off-limit high_temp [ clear low_temp ]
```

- **high_thresh**
  Default: 0
  Specifies the high card temperature (in degrees Celsius) that must be met or exceeded within the polling interval to generate an alert or alarm.
  **high_thresh** is an integer from 0 through 100. A value of 0 disables the threshold.

- **clear low_thresh**
  Default: 0
  Specifies the low card temperature (in degrees Celsius) before a high temperature alarm is cleared.
  **low_thresh** is an integer from 0 through 100. A value of 0 disables the threshold.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**
Set the high and low temperatures in degrees Celsius that generate and clear alarms.

**Example**
The following command configures sets the high and low temperatures to 40 and 35 degrees:

```
threshold card-temperature-near-power-off-limit 40 clear 35
```
threshold cdr-file-space

Configures, alarm or alert thresholds for monitoring the percentage of total file space allocated for Charging Data Records (CDRs) used during the polling interval.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local] host_name(config)#
```

**Syntax**

```
threshold cdr-file-space high_thresh [ clear low_thresh ]
```

**default threshold cdr-file-space**

```
default
```

Configures this command with the default threshold settings.

```
high_thresh
```

Specifies the high threshold for percentage of total allocated CDR file space used that must be met or exceeded at the end of the polling interval to generate an alert or alarm.

*high_thresh* is measured in percentage of total allocated CDR file space used and is an integer from 0 through 100. A value of 0 disables the threshold.

Default: 90

```
clear low_thresh
```

Specifies the low threshold for percentage of total allocated CDR file space used that maintains a previously generated alarm condition. If the space usage falls below *low_thresh* within the polling interval, a clear alarm is generated.

*low_thresh* is measured in percentage of total allocated CDR file space used and is an integer from 0 through 100. A value of 0 disables the threshold.

Default: 0

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to *low_thresh*.

**Usage**

CDR file space usage generate alerts or alarms based on the percentage of total allocated CDR file space used during the polling interval.
Alerts or alarms are triggered for CDR file space usage session based on the following rules:

- **Enter condition:** Actual percentage of allocated CDR file space usage is greater than or equal to the specified percentage of total CDR file space.

- **Clear condition:** Actual CDR file space used is less than the specified clear percentage of total allocated CDR file space usage.

If a trigger condition exists at the end of the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Example**

The following command configures a threshold of 65 percent of total allocated CDR file space usage and a clear threshold of 35 percent:

```
threshold cdr-file-space 65 clear 35
```
threshold contfilt-block

Configures, alarm or alert thresholds for Content Filtering rating operations blocked during a polling interval at which the threshold are raised or cleared.

Product
CF

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold contfilt-block high_thresh_value [ clear low_thresh_value ]

default threshold contfilt-block

default
Configures this command with the default threshold settings.

high_thresh
Specifies the high threshold for number of rating operations blocked for content filtering service that must be met or exceeded at the end of the polling interval to generate an alert or alarm.

high_thresh is measured in numbers of total rating operations blocked and is an integer from 0 through 1000000. A value of 0 disables the threshold.

clear low_thresh
Specifies the low threshold for the total number of rating operations blocked for a content filtering service that maintains a previously generated alarm condition. If the threshold falls below specifies the low threshold within the polling interval, a clear alarm is generated.

low_thresh is measured in numbers of total rating operations blocked and is an integer from 0 through 1000000. A value of 0 disables the threshold.
Default: 0

Usage
Use this command to configure the threshold for a content filtering service to generates alerts or alarms based on the number of rating operations blocked for a content filtering service during the polling interval. If a trigger condition exists at the end of the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the threshold poll contfilt-block command to configure the polling interval and the threshold monitoring command to enable thresholding for this value.

Example
The following command configures a threshold of 65000 rating operations blocked and a clear threshold of 35000 operations:

```
threshold contfilt-block 65000 clear 35000
```
threshold contfilt-rating

Configures, alarm or alert thresholds for Content Filtering rating operations performed during a polling interval at which the threshold are raised or cleared.

Product
CF

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold contfilt-rating high_thresh_value [ clear low_thresh_value ]

default threshold contfilt-rating

default

Configures this command with the default threshold settings.

high_thresh

Specifies the high threshold for number of rating operations performed for content filtering service that must be met or exceeded at the end of the polling interval to generate an alert or alarm.

high_thresh is measured in numbers of total rating operations performed and is an integer from 0 through 1000000. A value of 0 disables the threshold.

clear low_thresh

Specifies the low threshold for the total number of rating operations performed for a content filtering service that maintains a previously generated alarm condition. If the threshold falls below

low_thresh is measured in number of total rating operations performed and is an integer from 0 through 1000000. A value of 0 disables the threshold.

Default: 0

Usage

Use this command to configure the threshold for a content filtering service to generates alerts or alarms based on the number of rating operations performed for a content filtering service during the polling interval.

If a trigger condition exists at the end of the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the threshold poll contfilt-rating command to configure the polling interval and the threshold monitoring command to enable thresholding for this value.

Example
The following command configures a threshold of 65000 percent of total rating operations performed and a clear threshold of 35000 percent:

`threshold contfilt-rating 65000 clear 35000`
threshold cpu-available-memory

Configures alarm or alert thresholds for available CPU memory in the system.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config) #

Syntax

threshold cpu-available-memory low_thresh [ clear high_thresh ]

<table>
<thead>
<tr>
<th>low_thresh</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default: 32</td>
</tr>
<tr>
<td>Specifies the low threshold amount of CPU memory that must be met or exceeded at the polling time to generate an alert or alarm.</td>
</tr>
<tr>
<td>low_thresh is measured in megabytes (MB) and is an integer from 0 through 2048.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>clear high_thresh</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default: 32</td>
</tr>
<tr>
<td>Specifies the high threshold amount of CPU memory that maintains a previously generated alarm condition.</td>
</tr>
<tr>
<td>If the memory amount rises above the high threshold within the polling interval, a clear alarm will be generated.</td>
</tr>
<tr>
<td>high_thresh is measured in megabytes (MB) and is an integer from 0 through 2048.</td>
</tr>
</tbody>
</table>

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the low threshold.

Usage

CPU available memory thresholds generate alerts or alarms based on the amount of available memory for each packet processing card CPU at the polling time. Although, a single threshold is configured for all CPUs, separate alerts or alarms can be generated for each CPU.

Alerts or alarms are triggered for available CPU memory based on the following rules:

- **Enter condition**: Average measured amount of memory/CPU for the last 5 minutes is less than or equal to the low threshold.

- **Clear condition**: Average measured amount of memory/CPU for the last 5 minutes is greater than the high threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Important:** This command is not supported on all platforms.

**Example**

The following command configures a low threshold count of 50 MB CPU memory available and a high threshold of 112 MB for a system using the Alarm thresholding model:

```
threshold cpu-available-memory 50 clear 112
```
threshold cpu-load

Configures alarm or alert thresholds for monitoring packet processing card CPU loads using a 5-minute average measurement. The threshold is enabled by enabling CPU resource monitoring.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

```
configure
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config) #
```

**Syntax**

```
threshold cpu-load high_thresh [ clear low_thresh ]
```

* `high_thresh`
  Default: 0
  If the monitored CPU load is greater than or equal to the specified number an alert is sent. `high_thresh` must be an integer from 0 through 15.

* `clear low_thresh`
  Default: 0
  This is a low watermark value that sets the alarm clearing threshold value. If not present it is taken from the first value. `low_thresh` must be an integer from 0 through 15.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to Specifies the low threshold.

**Usage**

Use this command to set an alert when the card’s CPU load is equal to or greater than the number specified. Alerts or alarms are triggered for CPU load based on the following rules:

* **Enter condition:** Actual CPU load is greater than or equal to the high threshold.
* **Clear condition:** Actual CPU load is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Important:** This command is not supported on all platforms.
Example

To set an alert when the packet processing card CPU load is over 10 and set an alert clear when the CPU load drops down equal or less than 7, enter the following command:

```bash
threshold cpu-load 10 clear 7
```
threshold cpu-memory-usage

Configures, alarm or alert thresholds for monitoring the percentage of total CPU memory used during the polling interval.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold cpu-memory-usage high_thresh [ clear low_thresh ]

| high_thresh |
| Default: 0 |
| Specifies the high threshold for percentage of total memory used that must be met or exceeded at the end of the polling interval to generate an alert or alarm. |
| high_thresh is measured as a percentage of total CPU memory used and is an integer from 0 and 100. A value of 0 disables the threshold. |

| clear low_thresh |
| Default: 0 |
| Specifies the low threshold for percentage of total CPU memory used that maintains a previously generated alarm condition. If the memory usage falls below the low threshold within the polling interval, a clear alarm is generated. |
| low_thresh is measured as a percentage of total CPU memory used and is an integer from 0 and 100. A value of 0 disables the threshold. |

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to Specifies the low threshold.

Usage

CPU memory usage generate alerts or alarms based on the percentage of total CPU memory used during the polling interval.

Alerts or alarms are triggered for CPU memory usage session based on the following rules:

- **Enter condition**: Actual percentage of CPU memory usage is greater than or equal to the specified percentage of total CPU memory.

- **Clear condition**: Actual CPU memory usage is less than the specified clear percentage of total CPU memory usage.
If a trigger condition exists at the end of the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the threshold poll command to configure the polling interval and the threshold monitoring command to enable thresholding for this value.

Example

The following command configures a threshold of 65 percent of total packet processing card CPU memory usage and a clear threshold of 35 percent:

```
threshold cpu-memory_usage 65 clear 35
```
threshold cpu-orbs-crit

Configures thresholds for generating critical-level alerts or alarms based on the percentage of CPU utilization by the Object Request Broker System (ORBS) software task.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local] host_name(config) #

Syntax

```
threshold cpu-orbs-crit high_thresh [ clear low_thresh ]
[ default ] threshold cpu-orbs-crit
```

- **default**
  Restores this parameter to its default setting.

- **high_thresh**
  Default: 60
  Specifies the high threshold percent of CPU utilization by the ORB software task that must be exceeded as measured at the time of polling to generate a critical-level alert or alarm. `high_thresh` is measured in percentage of total CPU utilization and is an integer from 0 through 100. A value of 0 disables the threshold.

- **clear low_thresh**
  Default: 60
  Specifies the low threshold percent of CPU utilization by the ORB software task that maintains a previously generated alarm condition. If the percentage is measured as less than or equal to `low_thresh` at the time of polling, a clear alarm will be generated. `low_thresh` is measured in percentage of total CPU utilization and is an integer from 0 through 100. A value of 0 disables the threshold.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to `low_thresh`.

**Usage**

Object Request Broker (ORB) software task CPU utilization thresholds generate critical-level alerts or alarms based on the percentage of packet processing card CPU resources it is consuming at the time of polling.
Critical-level alerts or alarms are triggered for CPU usage by the ORBs software task based on the following rules:

- **Enter condition:** Actual CPU usage percentage is greater than the high threshold.
- **Clear condition:** Actual CPU usage percentage is less than or equal to the low threshold.

Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Example**

The following command configures a critical-level alarm threshold of 35 percent of CPU utilization by the ORBS task and a clear threshold of 30 percent:

```
threshold cpu-orbs-crit 35 clear 30
```
threshold cpu-orbs-warn

Configures thresholds for generating warning-level alerts or alarms based on the percentage of CPU utilization by the Object Request Broker System (ORBS) software task.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold cpu-orbs-warn high_thresh [ clear low_thresh ]
[ default ] threshold cpu-orbs-warn

default
Restores this parameter to its default setting.

high_thresh
Default: 50
Specifies the high threshold percent of CPU utilization by the ORBS software task that must be exceeded as measured at the time of polling to generate a warning-level alert or alarm. high_thresh is measured in percentage of total CPU utilization and is an integer from 0 through 100. A value of 0 disables the threshold.

clear low_thresh
Default: 50
Specifies the low threshold percent of CPU utilization by the ORBS software task that maintains a previously generated alarm condition. If the percentage is measured as less than or equal to low_thresh at the time of polling, a clear alarm will be generated.
low_thresh is measured in percentage of total CPU utilization and is an integer from 0 through 100. A value of 0 disables the threshold.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to Specifies the low threshold.
Usage
Object Request Broker (ORB) software task CPU utilization thresholds generate warning-level alerts or alarms based on the percentage of packet processing card CPU resources it is consuming at the time of polling. Warning-level alerts or alarms are triggered for CPU usage by the ORBS software task based on the following rules:

- **Enter condition:** Actual CPU usage percentage is greater than the high threshold.
- **Clear condition:** Actual CPU usage percentage is less than or equal to the low threshold.

Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

Example
The following command configures a warning-level alarm threshold of 25 percent of CPU utilization by the ORBS task and a clear threshold of 20 percent:

```
threshold cpu-orbs-warn 25 clear 20
```
threshold cpu-session-throughput

Configures alarm or alert thresholds for CPU session throughput within the system.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config) #

Syntax

threshold cpu-session-throughput high_thresh [ clear low_thresh ]

high_thresh
Default: 0
Specifies the high threshold session throughput that must be met or exceeded within the polling interval to generate an alert or alarm.
high_thresh is measured in kilobytes per second (Kbps) and is an integer from 0 through 1000000000. A value of 0 disables the threshold.

clear low_thresh
Default: 0
Specifies the low threshold session thereabout that maintains a previously generated alarm condition. If the throughput falls below Specifies the low threshold within the polling interval, a clear alarm will be generated.
low_thresh is measured in kilobytes per second (Kbps) and is an integer from 0 through 1000000000. A value of 0 disables the threshold.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

CPU session throughput thresholds generate alerts or alarms based on total throughput for all Session Manager tasks running on each packet processing card CPU during the polling interval. Although, a single threshold is configured for all CPUs, separate alerts or alarms can be generated for each CPU. Alerts or alarms are triggered for CPU session throughput based on the following rules:

- Enter condition: Actual CPU session throughput is greater than or equal to the high threshold.

- Clear condition: Actual CPU session throughput is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Important:** This command is not supported on all platforms.

**Example**

The following command configures a high threshold count of 900 Kbps session throughput and a low threshold of 500 KBps for a system using the Alarm thresholding model:

```
threshold cpu-session-throughput 900 clear 500
```
threshold cpu-utilization

Configures alarm or alert thresholds for CPU utilization within the system.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config) #

Syntax

threshold cpu-utilization high_thres [ clear low_thres ]

high_thres
Default: 85
Specifies the high threshold CPU utilization percentage that must be met or exceeded within the polling interval to generate an alert or alarm.
high_thres is an integer from 0 through 100.

clear low_thres
Default: 85
Specifies the low threshold CPU utilization percentage that maintains a previously generated alarm condition. If the utilization percentage falls below the low threshold within the polling interval, a clear alarm will be generated.
low_thres is an integer from 0 through 100.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

CPU utilization thresholds generate alerts or alarms based on the utilization percentage of each packet processing card CPU during the specified polling interval. Although, a single threshold is configured for all CPUs, separate alerts or alarms can be generated for each CPU.

Alerts or alarms are triggered for CPU utilization based on the following rules:

- **Enter condition**: Average measured CPU utilization for the last 5 minutes
- **Clear condition**: Average measured CPU utilization for the last 5 minutes is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Important:** This command is not supported on all platforms.

**Example**

The following command configures a high threshold CPU utilization percentage of 90 for a system using the Alert thresholding model:

```
threshold cpu-utilization 90
```
threshold dcca-bad-answers

Configures alarm or alert thresholds for invalid or bad responses to the system from Diameter servers.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

**Syntax**

```plaintext
threshold dcca-bad-answers high_thresh [ clear low_thresh ]
default threshold dcca-bad-answers
```

**default**
Disables the threshold for configured alarm and sets the `high_thresh` and `low_thresh` values to 0.

**high_thresh**
Default: 0
Specifies the high threshold number of invalid messages or responses that must be met or exceeded within the polling interval to generate an alert or alarm.

`high_thresh` is an integer from 0 through 1000000.

**clear low_thresh**
Default: 0
Specifies the low threshold number of invalid messages/responses that maintains a previously generated alarm condition. If the number of failures falls beneath the low threshold within the polling interval, a clear alarm will be generated.

`low_thresh` is an integer from 0 through 1000000.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**

In the event that the system receives invalid message or response from Diameter server `dcca-bad-answers` is generated.
DCCA bad answer messages size threshold generates alerts or alarms based on the number of invalid response or messages received during the specified polling interval.
Alerts or alarms are triggered for DCCA bad answers based on the following rules:
• **Enter condition:** Actual number of DCCA bad answer messages is greater than or equal to the high threshold.

• **Clear condition:** Actual number of DCCA bad answer messages is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

**Example**

The following command configures a high threshold count of 250 DCCA bad answer messages and low threshold of 100 for a system using the Alarm thresholding model:

```
threshold dcca-bad-answers 250 clear 100
```
threshold dcca-protocol-error

Configures alarm or alert thresholds for Diameter Credit Control Application (DCCA) protocol errors from the Diameter server.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold dcca-protocol-error high_thresh [ clear low_thresh ]

default threshold dcca-protocol-error

<table>
<thead>
<tr>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disables the threshold for configured alarm and sets the high_thresh and low_thresh values to 0.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>high_thresh</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default: 0</td>
</tr>
<tr>
<td>Specifies the high threshold number of protocol error received from Diameter server that must be met or exceeded within the polling interval to generate an alert or alarm.</td>
</tr>
<tr>
<td>high_thresh is an integer from 0 through 1000000.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>clear low_thresh</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default: 0</td>
</tr>
<tr>
<td>Specifies the low threshold number of protocol error received from Diameter server that maintains a previously generated alarm condition. If the number of errors falls beneath the low threshold within the polling interval, a clear alarm will be generated.</td>
</tr>
<tr>
<td>low_thresh is an integer from 0 through 1000000.</td>
</tr>
</tbody>
</table>

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

In the event that the system receives the protocol errors from Diameter server, dcca-protocol-error is generated.

DCCA protocol error threshold generates alerts or alarms based on the number of protocol error messages received from Diameter server during the specified polling interval.
Alerts or alarms are triggered for DCCA protocol error based on the following rules:

- **Enter condition:** Actual number of DCCA protocol error is greater than or equal to the high threshold.
- **Clear condition:** Actual number of DCCA protocol errors is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

**Example**

The following command configures a high threshold count of 250 protocol errors and low threshold of 100 for a system using the Alarm thresholding model:

```
threshold dcca-protocol-error 250 clear 100
```
threshold dcca-rating-failed

Configures Diameter Credit Control Application (DCCA) Rating Group (content-id) request reject, alarm or alert thresholds.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config) #

Syntax

threshold dcca-rating-failed high_thresh [ clear low_thresh ]

default threshold dcca-rating-failed

default

Disables the threshold for configured alarm and sets the high_thresh and low_thresh values to 0.

high_thresh

Default: 0
Specifies the high threshold number of requests for a block of credits due to invalid Rating Group (content-id), rejected from the Diameter server that must be met or exceeded within the polling interval to generate an alert or alarm.

high_thresh is an integer from 0 through 1000000.

clear low_thresh

Default: 0
Specifies the low threshold number of requests for a block of credits due to invalid Rating Group (content-id), rejected from the Diameter server that maintains a previously generated alarm condition. If the number of errors falls beneath the low threshold within the polling interval, a clear alarm will be generated.

low_thresh is an integer from 0 through 1000000.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

In the event that the Diameter server rejects the system request for a block of credits due to invalid Rating Group, defined as content-id, dcca-rating-failed message is generated.
Rating Group failed threshold generates alerts or alarms based on the number of requests rejected from Diameter server during the specified polling interval. Alerts or alarms are triggered for Rating Group failed based on the following rules:

- **Enter condition:** Actual number of DCCA Rating Group failed is greater than or equal to the high threshold.

- **Clear condition:** Actual number of DCCA Rating Group failed is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

**Example**

The following command configures a high threshold count of 250 requests rejected and low threshold of 100 for a system using the Alarm thresholding model:

```
threshold dcca-rating-failed 250 clear 100
```
threshold dcca-unknown-rating-group

Configures alarm or alert thresholds for the unknown Diameter Credit Control Application (DCCA) Rating Group (content-id) messages returned by Diameter servers.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

```
[local] host_name(config) #
```

**Syntax**

threshold dcca-unknown-rating-group high_thresh [ clear low_thresh ]

default threshold dcca-unknown-rating-group

**default**

Disables the threshold for configured alarm and sets the high_thresh and low_thresh values to 0.

**high_thresh**

Default: 0
Specifies the high threshold number of unknown Rating Group (content-id) messages sent by the Diameter server that must be met or exceeded within the polling interval to generate an alert or alarm. 
high_thresh is an integer from 0 through 1000000.

**clear low_thresh**

Default: 0
Specifies the low threshold number of unknown Rating Group (content-id) sent by Diameter server and received by system that maintains a previously generated alarm condition. If the number of errors falls beneath the low threshold within the polling interval, a clear alarm will be generated.
low_thresh is an integer from 0 through 1000000.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**

In the event that the Diameter server sends invalid Rating Groups, content-ids to the system, dcca-unk-
rating-group message is generated.
Unknown Rating Group threshold generates alerts or alarms based on the number of unknown Rating Groups received by the system from Diameter server during the specified polling interval.
Alerts or alarms are triggered for unknown rating groups based on the following rules:

- **Enter condition**: Actual number of unknown rating groups is greater than or equal to the high threshold.
- **Clear condition**: Actual number of unknown rating groups is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

**Example**

The following command configures a high threshold count of 250 unknown rating groups and low threshold of 100 for a system using the Alarm thresholding model:

```bash
threshold dcca-unknown-rating-group 250 clear 100
```
threshold diameter diameter-retry-rate

Configures Diameter Retry Rate, alarm or alert thresholds based on the percentage of Diameter requests that were retried during the polling interval.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration
`configure`

Entering the above command sequence results in the following prompt:

```
[local] host_name(config)#
```

**Syntax**

```
threshold diameter diameter-retry-rate high_thresh [ clear low_thresh ]
```

**default**

```
threshold diameter diameter-retry-rate
```

- **default**
  Configures this command with the default threshold settings.
  Default: 0—disabled

- **high_thresh**
  Specifies the high threshold. If, within the polling interval, the percentage of Diameter requests retried equals or exceeds `high_thresh` an alert or alarm is generated. `high_thresh` is an integer from 0 through 100.
  Default: 0

- **clear low_thresh**
  Specifies the low threshold. If, within the polling interval, the percentage of Diameter requests retried falls below `low_thresh`, a clear alarm is generated. `low_thresh` is an integer from 0 through 100.
  Default: 0

**Important:** This value is applicable for the Alarm mode, and ignored for the Alert mode. In addition, if this value is not configured for the Alarm mode, the system assumes it is identical to the high threshold.

**Usage**

Diameter Retry Rate threshold generates alerts or alarms based on the percentage of Diameter requests that were retried during the specified polling interval.
Alerts or alarms are triggered based on the following rules:
- **Enter condition:** Percentage of Diameter requests retried is greater than or equal to the high threshold.
- **Clear condition:** Percentage of Diameter requests retried is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

**Example**

The following command configures a high threshold of 75 percent, and a low threshold of 50 percent for a system using the Alarm thresholding model:

```
threshold diameter diameter-retry-rate 75 clear 50
```
threshold dns-learnt-ip-max-entries

Configures alarm or alert thresholds for the percentage of total DNS-learnt IP entries in relation to the ACS DNS Snooping feature.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local] host_name(config)#

Syntax

threshold dns-learnt-ip-max-entries high_thresh [ clear low_thresh ]

default threshold dns-learnt-ip-max-entries

default

Configures this command with the default threshold setting.
Default: 90 percent. It is the same for both high and low thresholds.

high_thresh

Default: 90 percent

Specifies the high threshold for percentage of total DNS-learnt IP entries. When the percentage of total DNS-learnt IP entries meets or exceeds the high threshold at the end of the polling interval, an alert or alarm is generated.

When the percentage of total DNS-learnt IPv4 entries meets or exceeds the high threshold, the ECSTotalDNSLearntIPv4Threshold trap is generated.
When the percentage of total DNS-learnt IPv6 entries meets or exceeds the high threshold, the ECSTotalDNSLearntIPv6Threshold trap is generated.

high thresh is an integer value from 0 through 100. When configured to 0 the threshold is disabled.

clear low_thresh

Default: 90 percent

 Specifies the low threshold for percentage of total DNS-learnt IP entries. When the percentage of total DNS-learnt IP entries goes below the low threshold within the polling interval, a clear alarm is generated.
When the percentage of total DNS-learnt IPv4 entries goes below the low threshold, the ECSTotalDNSLearntIPv4ThresholdClear trap is generated.
When the percentage of total DNS-learnt IPv6 entries goes below the low threshold, the ECSTotalDNSLearntIPv6ThresholdClear trap is generated.

low_thresh is an integer value from 0 through 100. When configured to 0 the threshold is disabled.
Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the low threshold.

Usage
Use this command to configure thresholds for the percentage of total DNS-learnt IP entries in relation to the ACS DNS Snooping feature. Note that this threshold applies to both IPv4 and IPv6 DNS entries. Alerts or alarms are triggered based on the following rules:

- **Enter condition:** Actual percentage of total DNS-learnt IP entries is greater than or equal to the specified percentage of total DNS-learnt IP entries.

- **Clear condition:** Actual of total DNS-learnt IP entries is less than the specified clear percentage of total DNS-learnt IP entries.

If a trigger condition exists at the end of the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the `threshold poll` command to configure the polling interval, and the `threshold monitoring` command to enable thresholding for this value.

Example
The following command configures a high threshold of 65 percent and a clear threshold of 35 percent for total DNS-learnt IP entries:

```
threshold dns-learnt-ip-max-entries 65 clear 35
```
threshold dns-lookup-failure

Configures alarm or alert thresholds based on the percentage of total DNS lookup failures.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

**Syntax**

\[threshold dns-lookup-failure\]

**default**

Configures this command with the default threshold setting.
Default: 90 percent. It is the same for both high and low thresholds.

**high_thresh**

Default: 90 percent
Specifies the high threshold for percentage of total DNS lookup failures. When the percentage of total failures meets or exceeds the high threshold at the end of the polling interval, an alert or alarm is generated.
\[high_thresh\] is an integer value from 0 through 100. When configured to 0 the threshold is disabled.

**clear low_thresh**

Default: 90 percent
Specifies the low threshold for percentage of total DNS lookup failures. When the percentage of total failures goes below the low threshold within the polling interval, a clear alarm is generated.
\[low_thresh\] is an integer value from 0 through 100. When configured to 0 the threshold is disabled.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the low threshold.

**Usage**

Use this command to configure thresholds for the percentage of total DNS lookup failures. Note that this threshold applies to both IPv4 and IPv6 DNS entries.
Alerts or alarms are triggered based on the following rules:

- **Enter condition:** Actual percentage of total DNS lookup failures is greater than or equal to the specified percentage of total DNS lookup failures.
• **Clear condition**: Actual of total DNS lookup failures is less than the specified clear percentage of total DNS lookup failures.

If a trigger condition exists at the end of the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the `threshold poll` command to configure the polling interval, and the `threshold monitoring` command to enable thresholding for this value.

**Example**

The following command configures a high threshold of 65 percent and a clear threshold of 35 percent for total DNS lookup failures:

```
threshold dns-lookup-failure 65 clear 35
```
threshold edr-file-space

Configures alarm or alert thresholds for monitoring the percentage of total file space allocated for Event Data Records (EDRs) used during the polling interval.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

**Syntax**

```
[ default ] threshold edr-file-space high_thresh [ clear low_thresh ]
```

**high_thresh**

Default: 90
Specifies the high threshold for percentage of total allocated EDR file space used that must be met or exceeded at the end of the polling interval to generate an alert or alarm.

*high_thresh* is measured in percentage of total allocated EDR file space used and is an integer from 0 through 100. A value of 0 disables the threshold.

**clear low_thresh**

Default: 0
Specifies the low threshold for percentage of total allocated EDR file space used that maintains a previously generated alarm condition. If the space usage falls below the low threshold within the polling interval, a clear alarm is generated.

*low_thresh* is measured in percentage of total allocated EDR file space used and is an integer from 0 through 100. A value of 0 disables the threshold.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the low threshold.

**Usage**

EDR file space usage generate alerts or alarms based on the percentage of total allocated EDR file space used during the polling interval.

Alerts or alarms are triggered for EDR file space usage session based on the following rules:

- **Enter condition:** Actual percentage of allocated EDR file space usage is greater than or equal to the specified percentage of total EDR file space.

- **Clear condition:** Actual EDR file space used is less than the specified clear percentage of total allocated EDR file space usage.
If a trigger condition exists at the end of the polling interval, the alert or alarm will not be generated until the end of the polling interval. Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Example**

The following command configures a high threshold of 65 percent and a clear threshold of 35 percent for total allocated EDR file space usage:

```
threshold edr-file-space 65 clear 35
```
threshold edr-udr-dropped flow control

Configures alarm or alert thresholds to monitor the total number of Event Data Records (EDRs) and Usage Data Records (UDRs) discarded due to flow control.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

```
[local] host_name(config) #
```

**Syntax**

```
threshold edr-udr-dropped-flow-control high_thresh [ clear low_thresh ]

default threshold edr-udr-dropped-flow-control

  default
  Configures this command with the default threshold settings.
  Default: High threshold: 90; Low threshold: 10

  high_thresh
  Specifies the high threshold for total number of EDRs + UDRs dropped due to flow control, which must be
  met or exceeded within the polling interval to generate an alert or alarm.
  high_thresh must be an integer from 0 through 100000.
  A value of 0 disables the threshold.
  Default: 90

  clear low_thresh
  Specifies the low threshold for total number of EDRs + UDRs dropped that maintains a previously generated
  alarm condition. If the total number of EDRs + UDRs dropped falls below Specifies the low threshold within
  the polling interval, a clear alarm is generated.
  low_thresh must be an integer from 0 through 100000 that must be lower than high_thresh.
  A value of 0 disables the threshold.
  Default: 10

**Usage**

Use this command to configure thresholds to monitor the total number of EDRs + UDRs discarded due to
flow control. Alerts or alarms are generated based on the total number of EDRs + UDRs dropped during
polling interval.

Alerts or alarms are triggered for EDR file space usage session based on the following rules:
• **Enter condition:** Actual number of EDRs + UDRs dropped greater than or equal to the specified number of EDRs + UDRs dropped.

• **Clear condition:** Actual number of EDR + UDRs dropped is less than the specified clear number of EDRs + UDRs dropped.

If a trigger condition exists at the end of the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Example**

The following command configures a high threshold of **90** and a clear threshold of **45** to monitor EDRs + UDRs dropped due to flow control:

```
threshold edr-udr-dropped-flow-control 90 clear 45
```
threshold epdg-current-sessions

Configures alarm or alert thresholds for the number of subscribers currently in Evolved Packet Date Gateway (ePDG) sessions.

**Product**
ePDG

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
threshold epdg-current-sessions

default threshold epdg-current-sessions
```

**default**

Disables the threshold for configured alarm and sets the `high_thresh` and `low_thresh` values to 0.

```
high_thresh
```

Default: 0
Specifies the high threshold number of the total number of ePDG subscriber sessions that must be met or exceeded within the polling interval to generate an alert or alarm. `high_thresh` is an integer from 0 through 1000000.

```
clear low_thresh
```

Default: 0
Specifies the low threshold number of the total number of ePDG subscriber sessions that maintains a previously generated alarm condition. If the number of errors falls beneath the low threshold within the polling interval, a clear alarm will be generated. `low_thresh` is an integer from 0 through 1000000.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**

Sets the upper and power thresholds for the total number of ePDG subscriber sessions that will generate and clear alerts or alarms. Alerts or alarms are triggered based on the following rules:
Global Configuration Mode Commands (T-threshold phspc)

threshold epdg-current-sessions

- **Enter condition:** Actual number of ePDG subscriber sessions is greater than or equal to the high threshold.
- **Clear condition:** Actual number of ePDG subscriber sessions is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

**Example**

The following command configures sets the upper threshold of ePDG subscriber sessions at 100000 and the lower threshold at 90000:

```
threshold epdg-current-sessions 100000 clear 90000
```
threshold fng-current-active-sessions

Configures alarm or alert thresholds for the number of subscribers currently active Femto Network Gateway (FNG) sessions.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold fng-current-active-sessions

default threshold fng-current-active-sessions

default
Disables the threshold for configured alarm and sets the high_thresh and low_thresh values to 0.

high_thresh
Default: 0
Specifies the high threshold number of the total number of active FNG subscriber sessions that must be met or exceeded within the polling interval to generate an alert or alarm. high_thresh is an integer from 0 through 1000000.

clear low_thresh
Default: 0
Specifies the low threshold number of the total number of active FNG subscriber sessions that maintains a previously generated alarm condition. If the number of errors falls beneath the low threshold within the polling interval, a clear alarm will be generated. low_thresh is an integer from 0 through 1000000.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage
Sets the upper and power thresholds for the total number of active FNG subscriber sessions that will generate and clear alerts or alarms.
Alerts or alarms are triggered based on the following rules:
• **Enter condition**: Actual number of active FNG subscriber sessions is greater than or equal to the high threshold.

• **Clear condition**: Actual number of active FNG subscriber sessions is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

**Example**

The following command configures sets the upper threshold of active FNG subscriber sessions at 100000 and the lower threshold at 90000:

```
threshold fng-current-active-sessions 100000 clear 90000
```
threshold fng-current-sessions

Configures alarm or alert thresholds for the number of subscribers currently in Femto Network Gateway (FNG) sessions, including inactive sessions.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold fng-current-sessions

default threshold fng-current-sessions

default

Configures this command with the default threshold settings.
Default: High threshold: 90; Low threshold: 10

high_thresh

Default: 0
Specifies the high threshold number of the total number of FNG subscriber sessions that must be met or exceeded within the polling interval to generate an alert or alarm.
high_thresh is an integer from 0 through 1000000.

clear low_thresh

Default: 0
Specifies the low threshold number of the total number of FNG subscriber sessions that maintains a previously generated alarm condition. If the number of errors falls beneath the low threshold within the polling interval, a clear alarm will be generated.
low_thresh is an integer from 0 through 1000000.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Sets the upper and power thresholds for the total number of FNG subscriber sessions that will generate and clear alerts or alarms.
Alerts or alarms are triggered based on the following rules:
- **Enter condition**: Actual number of FNG subscriber sessions is greater than or equal to the high threshold.
- **Clear condition**: Actual number of FNG subscriber sessions is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

**Example** The following command configures sets the upper threshold of FNG subscriber sessions at 200000 and the lower threshold at 190000:

```
threshold fng-current-sessions 200000 clear 190000
```
threshold fw-deny-rule

Configures alarm or alert thresholds for the Stateful Firewall Deny Rule.

**Product**
PSF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

```
configure
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config) #
```

**Syntax**

```
threshold fw-deny-rule high_thresh [ clear low_thresh ]
default threshold fw-deny-rule
```

**default threshold fw-deny-rule**

```
default
Confides this command with the default threshold settings.
Default: 0—disabled
```

```
high_thresh
Specifies the Stateful Firewall Deny-Rule threshold value, which if met or exceeded generates an alert or alarm.
high_thresh must be an integer from 0 through 1000000.
Default: 0
```

```
clear low_thresh
Specifies the Stateful Firewall Deny-Rule alarm clear threshold value. If, in the same polling interval, the threshold falls below low_thresh a clear alarm is generated.
low_thresh must be an integer from 0 through 1000000.
Default: 0
```

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the low threshold.

**Usage**

When the number of Deny-Rule instances exceeds a given value, an alarm or alert is raised; it is cleared when the number of Deny-Rule instances falls below a value within the polling interval.

Refer to the **threshold poll** command to configure the polling interval, and the **threshold monitoring** command to enable thresholding for this value.

**Example**
The following command configures a Stateful Firewall Deny Rule high threshold of 1000 and a low threshold of 900 for a system using the Alarm Thresholding model:

```
threshold fw-deny-rule 1000 clear 900
```
threshold fw-dos-attack

Configures alarm or alert thresholds for Stateful Firewall Denial-of-Service (DoS) attacks.

Product
PSF

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local] host_name(config) #

text

Syntax

threshold fw-dos-attack high_thresh [ clear low_thresh ]

default threshold fw-dos-attack

  default
  Configures this command with the default threshold settings.
  Default: 0—disabled

  high_thresh
  Specifies the Stateful Firewall DoS attacks threshold value, which if met or exceeded generates an alert or
  alarm.
  high_thresh must be an integer from 0 through 1000000.
  Default: 0

  clear low_thresh
  Specifies the Stateful Firewall DoS attacks clear threshold value. If, in the same polling interval, the threshold
  falls below low_thresh a clear alarm is generated.
  low_thresh must be an integer from 0 through 1000000.
  Default: 0

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm
model, the system assumes it is identical to the low threshold.

Usage

When the number of DoS attacks exceed a given value, a threshold is raised and it is cleared when the
number of DoS attacks fall below a value within the polling interval.
Refer to the threshold poll command to configure the polling interval and the threshold monitoring
command to enable thresholding for this value.

Example
The following command configures a Stateful Firewall DoS attacks high threshold of 1000 and a low threshold of 100 for a system using the Alarm Thresholding model:

```
threshold fw-dos-attack 1000 clear 100
```
**threshold fw-drop-packet**

Configures alarm or alert thresholds for Stateful Firewall dropped packets.

**Product**
PSF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
threshold fw-drop-packet high_thresh [ clear low_thresh ]
default threshold fw-drop-packet
```

**default threshold fw-drop-packet**

```
default
Configures this command with the default threshold settings.
Default: 0—disabled
```

```
high_thresh
Specifies the Stateful Firewall dropped packets threshold value, which if met or exceeded generates an alert
or alarm.
high_thresh must be an integer from 0 through 1000000.
Default: 0
```

```
clear low_thresh
Specifies the Stateful Firewall dropped packets clear threshold value. If, in the same polling interval, the
threshold falls below low_thresh a clear alarm is generated.
low_thresh must be an integer from 0 through 1000000.
Default: 0
```

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm
model, the system assumes it is identical to the low threshold.

**Usage**

When the number of dropped packets exceed a given value, a threshold is raised and it is cleared when the
number of dropped packets fall below a value within the polling interval.
Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring`
command to enable thresholding for this value.

**Example**
The following command configures a Stateful Firewall dropped packets high threshold of 1000 and a low threshold of 900 for a system using the Alarm thresholding model:

```
threshold fw-drop-packet 1000 clear 900
```
threshold fw-no-rule

Configures alarm or alert thresholds for Stateful Firewall no rule occurrences.

Product
PSF

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration

configure
Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold fw-no-rule high_thresh [ clear low_thresh ]

default threshold fw-no-rule

---

default

Configures this command with the default threshold settings.
Default: 0—disabled

high_thresh

Specifies the Stateful Firewall no rules threshold value, which if met or exceeded generates an alert or alarm.
high_thresh must be an integer from 0 through 1000000.
Default: 0

clear low_thresh

Specifies the Stateful Firewall no rules clear threshold value. If, in the same polling interval, the threshold falls below low_thresh a clear alarm is generated.
low_thresh must be an integer from 0 through 1000000.
Default: 0

---

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the low threshold.

---

Usage

When the number of no rule occurrences exceeds a given value, a threshold is raised and it is cleared when the number of no rules fall below a value within the polling interval.
Refer to the threshold poll command to configure the polling interval and the threshold monitoring command to enable thresholding for this value.

---

Example
The following command configures a Stateful Firewall no rule high threshold of 1000 and a low threshold of 900 for a system using the Alarm Thresholding model:

```
threshold fw-no-rule 1000 clear 900
```
threshold license remaining-sessions

Configures alarm or alert thresholds for the percentage of session license utilization by the system.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

[ no ] threshold license remaining-sessions low_thresh clear high_thresh

no low_thresh
Disables threshold session license utilization alerts or alarms.

remaining-sessions low_thresh
Default: 10
Specifies the low threshold session license utilization percentage that must be met or exceeded within the polling interval to generate an alert or alarm.
low_thresh is an integer from 0 through 100.

clear high_thresh
Default: 10
Specifies the high threshold session license utilization percentage that maintains a previously generated alarm condition. If the utilization percentage rises above the high threshold within the polling interval, a clear alarm will be generated.
high_thresh is an integer from 0 through 100.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to Specifies the low threshold.

Usage
Session license utilization thresholds generate alerts or alarms based on the utilization percentage of all session capacity licenses during the specified polling interval.
The system uses session capacity license to dictate the maximum number of simultaneous sessions that can be supported. There are multiple session types that require licenses. Although, a single threshold is configured for all session types, alerts or alarms can be generated for each type.
Alerts or alarms are triggered for session license utilization based on the following rules:
**Enter condition:** Actual session license utilization percentage per session type is greater than or equal to the low threshold.

**Clear condition:** Actual session license utilization percentage per session type is greater than the high threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval. Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Example**

The following command configures a session license low threshold percentage of 10 and a high threshold of 35 for a system using the Alarm thresholding model:

```
threshold license remaining-sessions 10 clear 35
```
threshold mgmt-cpu-memory-usage

Configures alarm or alert thresholds for the percentage of CPU memory usage on management cards.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local] host_name(config) #

Syntax

threshold mgmt-cpu-memory-usage high_thresh [ clear low_thresh ]

**high_thresh**

Default: 0
Specifies the high threshold percent of CPU memory usage that must be met or exceeded within the polling interval to generate an alert or alarm.

high_thresh is measured in percentage of total memory used and can be configured to an integer from 0 through 100. A value of 0 disables the threshold.

**clear low_thresh**

Specifies the low threshold percent of CPU memory usage that maintains a previously generated alarm condition. If the percentage falls beneath the low threshold within the polling interval, a clear alarm will be generated.

low_thresh is measured in percentage of total memory used and can be configured to an integer from 0 through 100. A value of 0 disables the threshold.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**

CPU memory usage thresholds generate alerts or alarms based on memory usage for the SPC, SMC, or MIO CPU during the polling interval. A single threshold enables CPU monitoring for both the active and standby SPCs, SMCs, or MIOs allowing for alerts or alarms to be generated for each CPU.

Alerts or alarms are triggered for SPC, SMC, or MIO CPU memory usage based on the following rules:

- **Enter condition:** Actual CPU memory usage is greater than or equal to the high threshold
  - **Clear condition:** Actual CPU memory usage is less than the low threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Important:** This command is not supported on all platforms.

**Example**

The following command configures a threshold of 65 percent of total SPC, SMC, or MIO CPU memory usage and a clear threshold of 35 percent:

```
threshold mgmt-cpu-memory-usage 65 clear 35
```
threshold mgmt-cpu-utilization

Configures alarm or alert thresholds for the percentage of CPU utilization on management cards.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

*configure*

Entering the above command sequence results in the following prompt:

```
threshold mgmt-cpu-utilization
```

**Syntax**

```
threshold mgmt-cpu-utilization high_thresh [ clear low_thresh ]
```

**high_thresh**

Default: 0

Specifies the high threshold CPU utilization percentage that must be met or exceeded within the polling interval to generate an alert or alarm.

*high_thresh* is an integer from 0 through 100.

**clear low_thresh**

Specifies the low threshold CPU utilization percentage that maintains a previously generated alarm condition. If the utilization percentage falls beneath the low threshold within the polling interval, a clear alarm will be generated.

*low_thresh* is an integer from 0 through 100.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**

CPU utilization thresholds generate alerts or alarms based on the utilization percentage of each SPC, SMC, or MIOCPU during the specified polling interval. Although, a single threshold is configured for both SPC, SMC, or MIO CPUs, separate alerts or alarms can be generated for each CPU.

Alerts or alarms are triggered for SPC, SMC, or MIO CPU utilization based on the following rules:

- **Enter condition:** Average measured CPU utilization for the last 5 minutes is greater than or equal to the high threshold.

- **Clear condition:** Average measured CPU utilization for the last 5 minutes is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Important:** This command is not supported on all platforms.

**Example**

The following command configures a high threshold SPC, SMC, or MIO CPU utilization percentage of 90 for a system using the Alert thresholding model:

```
threshold mgmt-cpu-utilization 90
```
threshold mme-attach-failure

Configures alarm or alert thresholds for the total number of MME Attach Failure messages across all the MME services in the system.

**Product**
MME

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

**Syntax**

```
threshold total-mme-attach-failure high_thresh [ clear low_thresh ]
```

**high_thresh**
Default: 0 (Disabled)
Specifies the high threshold number of total MME Attach Failure messages across all services on a system that must be met or exceeded within the polling interval to generate an alert or alarm.
*high_thresh* can be configured to an integer from 0 through 100000. A value of 0 disables the threshold.

**clear low_thresh**
Default: 0 (Disabled)
Specifies the low threshold number of total MME Attach Failure messages across all services on a system that maintains a previously generated alarm condition. If the number of MME Attach Failure messages across all the services in a system, falls beneath the low threshold within the polling interval, a clear alarm will be generated.
*low_thresh* is an integer from 0 through 100000. A value of 0 disables the threshold.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**

Use this command to monitor and set alarms or alerts when the total number of MME Attach Failure message across all the MME services in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for the total number of MME Attach Failure message based on the following rules:

- **Enter condition:** Actual total number of MME Attach Failure messages is greater than or equal to the high threshold.
- **Clear condition:** Actual total number of MME Attach Failure messages is less than the low threshold.
If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval. Refer to the `threshold poll mme-attach-failure` command to configure the polling interval and the `threshold monitoring mme-service` command to enable thresholding for this value.

**Example**

The following command configures the limit of MME Attach Failure high threshold count of 10000 for a system using the Alert thresholding model:

```
threshold mme-attach-failure 10000
```
threshold mme-auth-failure

Configures alarm or alert thresholds for the total number of MME Auth Failure messages across all the MME services.

Product
MME

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

\texttt{threshold total-mme-auth-failure \texttt{high\_thresh} [ \texttt{clear \ low\_thresh} ]}

\texttt{high\_thresh}

Default: 0 (Disabled)
Specifies the high threshold number of total MME Auth Failure messages across all MMM services on a system that must be met or exceeded within the polling interval to generate an alert or alarm.

\texttt{high\_thresh} can be configured to an integer from 0 through 100000. A value of 0 disables the threshold.

\texttt{clear \ low\_thresh}

Default: 0 (Disabled)
Specifies the low threshold number of total MME Auth Failure messages across all services on a system that maintains a previously generated alarm condition. If the number of MME Attach Failure messages across all the services in a system, falls beneath the low threshold within the polling interval, a clear alarm will be generated.

\texttt{low\_thresh} is an integer from 0 through 100000. A value of 0 disables the threshold.

\textbf{Important:} This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Use this command to monitor and set alarms or alerts when the total number of MME Auth Failure messages across all the MME services in the system is equal to or greater than the set limit. Alerts or alarms are triggered for the total number of MME Auth Failure messages based on the following rules:

\begin{itemize}
  \item \textbf{Enter condition:} Actual total number of MME Auth Failure messages is greater than or equal to the high threshold.
  \item \textbf{Clear condition:} Actual total number of MME Auth Failure messages is less than the low threshold.
\end{itemize}

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the `threshold poll mme-auth-failure` command to configure the polling interval and the `threshold monitoring mme-service` command to enable thresholding for this value.

**Example**

The following command configures a total MME Auth Failure high threshold count of 10000 for a system using the Alert thresholding model:

```
threshold mme-auth-failure 10000
```
threshold model

Configures the thresholding model, alarm or alert, for the system to use.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

**Syntax**

```plaintext
threshold model { alarm | alert }
```

**alarm**
Selects the alarm thresholding model as described in the *Usage* section for this command.

**alert**
Selects the alert thresholding model as described in the *Usage* section for this command.

**Usage**
The system supports the following thresholding models:

- **Alert**: A value is monitored and an alert condition occurs when the value reaches or exceeds the configured high threshold within the specified polling interval. The alert is generated then generated and/or sent at the end of the polling interval.

In the example shown in the figure below, this model generates alerts during period 2, 3, and 5 at the point where the count exceeded the high threshold.

- **Alarm**: Both high and low threshold are defined for a value. An alarm condition occurs when the value reaches or exceeds the configured high threshold within the specified polling interval. The alert is generated then generated and/or sent at the end of the polling interval.

The alarm is cleared at the end of the first interval where the measured value is below the low threshold. In the example shown in the figure below, this model generates an alarm during period 2 when the count exceeds the high threshold. A second alarm is generated in period 6 when the count falls beneath low threshold. The second alarm indicates a “clear” condition.
**Important:** For certain values the alert or alarm serves to warn of low quantities (such as, memory, session licenses, etc.). In these cases, the low threshold is the condition that must be met or exceeded within the polling interval to generate the alert or alarm. When the high threshold is exceeded during an interval, the low quantity condition is cleared.

Refer to the `threshold monitoring` command for additional information on thresholding.

**Example**

The following command configures the system to support the Alarm thresholding model:

```
threshold model alarm
```
threshold monitoring

Enables threshold monitoring for the selected value.

**Product**
All

**Privilege**
Administrator

**Mode**
Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

**Syntax**

```
```

- **no**
  Disables threshold monitoring for the specified value.

- **default**
  Sets or restores the default value assigned to the specified parameter.

- **aaa-acct-archive-queue**
  Enables threshold monitoring for the AAA accounting archive message queue size.
  Refer to the `threshold aaa-acct-archive-queue-size` command for additional information on these values.

- **aaa-acct-archive-size**
  Enables threshold monitoring for the size of the AAA accounting record archive.

- **aaa-acct-failure**
  Enables threshold monitoring for AAA accounting failures and AAA accounting failure rate values.
  Refer to the `threshold aaa-acct-failure` and `threshold aaa-acct-failure-rate` commands for additional information on these values.

- **aaa-auth-failure**
  Enables threshold monitoring for AAA authentication failures and AAA authentication failure rate values.
Refer to the `threshold aaa-auth-failure` and `threshold aaa-auth-failure-rate` commands for additional information on these values.

aaa-retry-rate
Enables threshold monitoring for the AAA retry rate value.
Refer to the `threshold aaa-retry-rate` command for additional information on this value.

aaamgr-request-queue
Enables threshold monitoring for AAA Manager Requests for each AAA manager process. Refer to the `threshold aaamgr-request-queue` command for additional information on these values.

asngw
Enables the threshold monitoring for ASN-GW services.

call-setup
Enables threshold monitoring for the call setup, call setup failures, and no-resource rejected call values.
Refer to the `threshold call-setup`, `threshold call-setup-failure`, `threshold ppp-setup-fail-rate`, `threshold rp-setup-fail-rate`, and `threshold call-reject-no-resource` commands for additional information on these values.

cpu-resource
Enables threshold monitoring for CPU thresholds.

cpu-session-throughput
Enables threshold monitoring for the CPU session throughput value.
Refer to the `threshold cpu-session-throughput` command for additional information on this value.

content-filtering
Enables threshold monitoring for the Content Filtering in-line service.

diameter
Enables threshold monitoring for Diameter.

ecs
Enables threshold monitoring for the Active Charging Service (ACS)/Enhanced Charging Service (ECS).

epdg-service
Enables threshold monitoring for Evolved Packet Data Gateway (ePDG) service.
Refer to the `threshold epdg-current-sessions` command for additional information on this value.
fa-service
Enables threshold monitoring for Registration Reply errors for each FA service.
Refer to the threshold reg-reply-error FA Service Configuration Mode command for additional information on this value.

fw-and-nat
Enables threshold monitoring for the Firewall and NAT in-line service.
Default: Disabled
Refer to the threshold fw-deny-rule, threshold fw-dos-attack, threshold fw-drop
packet, threshold fw-no-rule, threshold nat-pkt-drop, and threshold nat-port
chunks-usage commands for additional information on this value.

ha-service
Enables threshold monitoring for Registration Reply errors, re-registration reply errors, deregistration reply errors, and average calls setup per second for each HA service and average calls setup per second at the context level.
Refer to the threshold init-rrq-rcvd-rate, threshold reg-reply-error, threshold
rereg-reply-error, and threshold dereg-reply-error HA Service Configuration Mode commands and the threshold ha-service init-rrq-rcvd-rate Context Configuration mode command for additional information on this value.

hnbgw-service
Enables threshold monitoring for HeNB-GW service.

Important: This keyword is required to activate the threshold alarm/alert for HeNB-GW service to use
threshold hnbgw-paging-messages, threshold total-hnbgw-hnb-sessions, and threshold
total-hnbgw-ue-sessions commands for threshold values.

hnbgw-service
Enables threshold monitoring for HNB-GW sessions including Iu-CS and Iu-PS sessions for HNB-GW services on a system at the system level.

Important: This keyword is required to activate the threshold alarm/alert for HNB-GW service to use
threshold total-hnbgw-hnb-sessions, threshold total-hnbgw-ue-sessions, and threshold
total-hnbgw-ue-sessions command for threshold values.

hsgw-service
Enables threshold monitoring for HSGW services.
Refer to the threshold total-hsgw-sessions for more information on HSGW thresholds.

ipsec
Enables monitoring of IPSec thresholds.
Refer to the HA-Service Configuration Mode chapter of the Command Line Interface Reference for information on the IPSec thresholds.
license
Enables threshold monitoring for the session license value.
Refer to the threshold license command for additional information on this value.

lma-service
Enables threshold monitoring for LMA services.
Refer to the threshold total-lma-sessions command for more information on LMA thresholds.

mme-service
Default: Disabled.
Enables threshold monitoring for the MME services.
Refer to the threshold total-mme-sessions command for additional information on this value.

npu-resource
Enables threshold monitoring for the Network Processor Unit (NPU) resources, including NPU utilization.
Refer to the threshold npu-utilization command for additional information on this value.

packets-filtered-dropped
Enables threshold monitoring for the filtered/dropped packet value.
Refer to the threshold packets-filtered-dropped command for additional information on this value.

packets-forwarded-to-cpu
Enables threshold monitoring for the forwarded packet value.
Refer to the threshold packets-forwarded-to-cpu command for additional information on this value.

pdg-service
Enables threshold monitoring for PDG service.
Threshold monitoring for PDG service is disabled by default.

pdif-service
Enables threshold monitoring for PDIF service.

pdsn-service
Enables threshold monitoring for average calls setup per second for contexts and for PDSN services, A11 Request.
Refer to the threshold packets-forwarded-to-cpu command for additional information on this value.

pgw-service
Enables threshold monitoring for P-GW services.
Refer to the threshold total-pgw-sessions for more information on P-GW thresholds.

route-service
Enables threshold monitoring for BGP/VRF route services.
Refer to the ip maximum-routes command in Context configuration mode and threshold route-service bgp-routes in this mode for more information on route thresholds.
**saegw-service**

Enables threshold monitoring for SAEGW services.
Refer to the `threshold total-saegw-sessions` for more information on SAEGW thresholds.

**sess-flow-count**

Enables threshold monitoring for Session Flow Count.
Default: 90%
Refer to the `threshold sess-flow-count` for more information on Session Flow Count Thresholds

**sgw-service**

Enables threshold monitoring for S-GW services.
Refer to the `threshold total-sgw-sessions` for more information on S-GW thresholds.

**subscriber**

Enables threshold monitoring for the subscriber and session values.
Refer to the `threshold subscriber active, threshold subscriber total, threshold total-ggsn-sessions, threshold total-gprs-sessions, threshold total-gprs-pdp-sessions, threshold total-ha-sessions, threshold total-lns-sessions, threshold total-pdsn-sessions, threshold total-pgw-sessions, threshold total-sgw-sessions, threshold total-saegw-sessions, threshold total-sgsn-sessions, threshold total-sgsn-pdp-sessions, threshold per-service-ggsn-sessions, threshold per-service-ha-sessions, threshold per-service-lns-sessions, and threshold per-service-pdsn-sessions` commands for additional information on these values.

**system**

Enables system (chassis) thresholds monitoring.

**tpo**

**Important:** The Traffic Performance Optimization (TPO) in-line service is not supported in this release.

**Usage**

Thresholding on the system is used to monitor the system for conditions that could potentially cause errors or outage. Typically, these conditions are temporary (i.e. high CPU utilization, or packet collisions on a network) and are quickly resolved. However, continuous or large numbers of these error conditions within a specific time interval may be indicative of larger, more severe issues. The purpose of thresholding is to help identify potentially severe conditions so that immediate action can be taken to minimize and/or avoid system downtime.

Thresholding reports conditions using one of the following mechanisms:

- **SNMP traps:** SNMP traps have been created that indicate the condition (high threshold crossing and/or clear) of each of the monitored values. Complete descriptions and other information pertaining to these traps is located in the starentMIB(8164).starentTraps(2) section of the SNMP MIB Reference.

The generation of specific traps can be enabled or disabled on the system allowing you to view only those traps that are most important to you.
• **Logs:** The system provides a facility called threshold for which active and event logs can be generated. As with other system facilities, logs are generated Log messages pertaining to the condition of a monitored value are generated with a severity level of WARNING.

• **Alarm System:** High threshold alarms generated within the specified polling interval are considered “outstanding” until the condition no longer exists and/or a condition clear alarm is generated. “Outstanding” alarms are reported to through the system’s alarm subsystem and are viewable through the CLI.

The following table indicates the reporting mechanisms supported by each of the above models.

**Table 29. ASR 5000 Thresholding Reporting Mechanisms by Model**

<table>
<thead>
<tr>
<th>Model</th>
<th>SNMP Traps</th>
<th>Logs</th>
<th>Alarm System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Alarm</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

**Table 30. ASR 5500 Thresholding Reporting Mechanisms by Model**

<table>
<thead>
<tr>
<th>Model</th>
<th>Logs</th>
<th>Alarm System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Alarm</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

In addition to the values that can be enabled by this command, the system supports the enabling of threshold monitoring for IP pool address availability (refer to the `ip pool` and `threshold` commands in this reference) and port utilization (refer to the `threshold` commands in this chapter).

**Example**

The following command enables thresholding for subscriber totals:

```
threshold monitoring subscriber
```
threshold nat-port-chunks-usage

Configures alarm or alert thresholds for the percentage of Network Address Translation (NAT) port chunk utilization.

**Important:** This command is only available in 8.3 and later releases.

**Product**
NAT

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

```
[local] host_name(config) #
```

**Syntax**

```
threshold nat-port-chunks-usage high_thresh [ clear low_thresh ]

default threshold nat-port-chunks-usage
```

**default**

Configures this command with the default threshold settings.

Default: 0—disabled

**high_thresh**

Specifies the high NAT-port-chunks-usage percentage threshold that must be met or exceeded within the polling interval to generate an alert or alarm.

*high_thresh* must be an integer from 0 through 100. A value of 0 disables the threshold.

Default: 0

**clear low_thresh**

Specifies the low nat-port-chunks-usage percentage threshold that must be met within the polling interval for a clear alarm to be generated.

*low_thresh* must be an integer from 0 through 100. A value of 0 disables the threshold. If not set, the *high_thresh* will be the high and low threshold setting.

Default: 0

**Usage**

Use this command to configure the NAT port chunk utilization threshold settings.

**Example**

The following command sets the NAT port chunk utilization threshold settings to a high of 75% and a low of 15%:

```
threshold nat-port-chunks-usage 75 clear 15
threshold npu-utilization

Configures alarm or alert thresholds for the percentage of network processing unit (NPU) utilization.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

**configure**
Entering the above command sequence results in the following prompt:

```
[local] host_name(config) #
```

**Syntax**

```plaintext
threshold npu-utilization high_thresh clear low_thresh
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>default</strong></td>
<td>Configures this command with the default threshold settings. Default: 0—disabled</td>
</tr>
<tr>
<td><strong>high_thresh</strong></td>
<td>Specifies the high percentage threshold for NPU utilization that must be met or exceeded within the polling interval to generate an alert or alarm. <code>high_thresh</code> must be an integer from 0 through 100. A value of 0 disables the threshold. Default: 0</td>
</tr>
<tr>
<td><strong>clear low_thresh</strong></td>
<td>Specifies the low percentage threshold for NPU utilization that must be met within the polling interval for a clear alarm to be generated. <code>low_thresh</code> must be an integer from 0 through 100. A value of 0 disables the threshold. If not set, the <code>high_thresh</code> will be the high and low threshold setting. Default: 0</td>
</tr>
</tbody>
</table>

**Usage**
Use this command to configure the NPU utilization threshold settings.

**Example**
The following command sets the NPU utilization threshold settings to a high of 90% and a low of 75%:

```
threshold npu-utilization 90 clear 75
```
**threshold packets-filtered-dropped**

Configures alarm or alert thresholds for filtered or dropped packets within the system.

**Product**
- PDSN
- GGSN
- HA
- P-GW
- SAEGW
- SGSN
- ASN-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

**Syntax**

```
threshold packets-filtered-dropped high_thresh [ clear low_thresh ]
```

- `high_thresh`
  - Default: 0
  - Specifies the high threshold number of filtered/dropped packets experienced by the system resulting from access control list (ACL) rules that must be met or exceeded within the polling interval to generate an alert or alarm.
  - `high_thresh` is an integer from 0 through 100000000. A value of 0 disables the threshold.

- `clear low_thresh`
  - Default: 0
  - Specifies the low threshold number of filtered/dropped packets experienced by the system resulting from ACL rules that maintains a previously generated alarm condition. If the number of packets falls beneath the low threshold within the polling interval, a clear alarm will be generated.
  - `low_thresh` is an integer from 0 through 100000000. A value of 0 disables the threshold.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.
Filtered/dropped packet thresholds generate alerts or alarms based on the total number of packets that were filtered or dropped by the system as a result of ACL rules during the specified polling interval. Alerts or alarms are triggered for filtered/dropped packets based on the following rules:

- **Enter condition:** Actual number of filtered/dropped packets is greater than or equal to the high threshold.
- **Clear condition:** Actual number of filtered/dropped packets is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value. In addition, refer to information on ACLs in this reference.

**Example**

The following command configures a filtered/dropped packet high threshold count of 150000 for a system using the Alert thresholding model:

```
threshold packets-filtered-dropped 150000
```
threshold packets-forwarded-to-cpu

Configures alarm or alert thresholds for packets forwarded to active system CPUs in the system.

**Product**
- PDSN
- GGSN
- HA
- P-GW
- SAEGW
- SGSN
- ASN-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

```
configure
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
threshold packets-forwarded-to-cpu high_thresh  [ clear low_thresh ]
```

**high_thresh**

Default: 0
Specifies the high threshold number of packets forwarded to CPUs that must be met or exceeded within the polling interval to generate an alert or alarm.
`high_thresh` is an integer from 0 through 1000000000. A value of 0 disables the threshold.

**clear low_thresh**

Default: 0
Specifies the low threshold number of packets forwarded to CPUs that maintains a previously generated alarm condition. If the number of packets falls beneath the low threshold within the polling interval, a clear alarm will be generated.
`low_thresh` is an integer from 0 through 1000000000. A value of 0 disables the threshold.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.
Global Configuration Mode Commands (T-threshold phspc)

Usage

Forwarded packet thresholds generate alerts or alarms based on the total number of packets that were forwarded to active system CPU(s) during the specified polling interval. Packets are forwarded to active system CPUs when the NPUs do not have adequate information to properly route them.

**Important:** Ping and/or traceroute packets are intentionally forwarded to system CPUs for processing. These packet types are included in the packet count for this threshold.

Alerts or alarms are triggered for forwarded packets based on the following rules:

- **Enter condition:** Actual number of forwarded packets is greater than or equal to the high threshold
- **Clear condition:** Actual number of forwarded packets is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

Example

The following command configures a forwarded packet high threshold count of **100000** for a system using the Alert thresholding model:

```
threshold packets-forwarded-to-cpu 100000
```
threshold pdg-current-active-sessions

Configures alarm or alert thresholds for monitoring the total number of currently active Packet Data Gateway/Tunnel Termination Gateway (PDG/TTG) sessions.

Product
PDG/TTG

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold pdg-current-active-sessions high_thresh [ clear low_thresh ]

/configure

high_thresh

Configures the total number of active PDG sessions to be monitored on a chassis. high_thresh is an integer from 0 through 1000000. There is no default, but 0 means that there is no threshold monitoring.

clear low_thresh

Clears the number of sessions being monitored using the high_thresh variable defined above. low_thresh is an integer from 0 through 1000000.

Usage

Thresholds are provided for monitoring the overall PDG usage on a chassis. This command is used to monitor the total number of active PDG sessions for an entire chassis.

Example

The following command configures a monitoring threshold of 300000 and a clearing threshold of 100000 active PDG sessions on a chassis:

threshold pdg-current-active-sessions 300000 clear 100000
threshold pdg-current-sessions

Configures alarm or alert thresholds for monitoring the total number of current Packet Data Gateway/Tunnel Termination Gateway (PDG/TTG) sessions, including inactive sessions.

Product
PDG/TTG

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold pdg-current-sessions high_thresh [ clear low_thresh ]

*high_thresh*

Configures the total number of PDG sessions on a chassis, both active and inactive. *high_thresh* is any integer from 0 through 1000000. There is no default, but 0 means that there is no threshold monitoring.

*clear low_thresh*

Clears any number of sessions being monitored using the *high_thresh* variable defined above. *low_thresh* is any integer from 0 through 1000000.

Usage

Thresholds are provided for monitoring the overall PDG usage on a chassis. This command is used to monitor the total number of PDG sessions, both active and inactive, for an entire chassis.

Example

The following command configures a monitoring threshold of 300000 and a clearing threshold of 100000 active and inactive PDG sessions on a chassis:

```
threshold pdg-current-sessions 300000 clear 100000
```
threshold pdif-current-active-sessions

Configures alarm or alert thresholds for monitoring the total number of currently active Packet Data Interworking Function (PDIF) sessions.

Product
PDIF

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold pdif-current-active sessions high_thresh [ clear low_thresh ]

**high_thresh**

Configures the total number of active PDIF sessions to be monitored on a chassis. *high_thresh* is any integer from 0 through 1000000. There is no default, but 0 means that there is no threshold monitoring.

**clear low_thresh**

Clears the specified number of sessions being monitored using the *high_thresh* variable defined above. *low_thresh* is any integer from 0 through 1000000.

Usage

Thresholds are provided for monitoring the overall PDIF usage on a chassis. This command is used to monitor the total number of active PDIF sessions for an entire chassis.

Example

The following command configures a monitoring threshold of 300000 and a clearing threshold of 100000 active PDIF sessions on a chassis:

```
threshold pdif-current-active-sessions 300000 clear 100000
```
threshold pdif-current-sessions

Configures alarm or alert thresholds for monitoring the total number of current Packet Data Interworking Function (PDIF) sessions, including inactive sessions.

**Product**
PDIF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

```
[local] host_name(config) #
```

**Syntax**

```
threshold pdif-current-sessions high_thresh [ clear low_thresh ]
```

- **high_thresh**
  Configures the total number of PDIF sessions on a chassis, both active and inactive. `high_thresh` is an integer from 0 through 1000000. There is no default, but 0 means that there is no threshold monitoring.

- **clear low_thresh**
  Clears the specified number of sessions being monitored using the `high_thresh` variable defined above. `low_thresh` is an integer from 0 through 1000000.

**Usage**

Thresholds are provided for monitoring the overall PDIF usage on a chassis. This command is used to monitor the total number of PDIF sessions, both active and inactive, for an entire chassis.

**Example**

The following command configures a monitoring threshold of 300000 and a clearing threshold of 100000 active and inactive PDIF sessions on a chassis:

```
threshold pdif-current-sessions 300000 clear 100000
```
threshold per-service-asngw-sessions

Configures alarm or alert thresholds for the number of sessions per ASN-GW service in the system.

Product
ASN-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold per-service-asngw-sessions high_thresh [ clear low_thresh ]

| **high_thresh**
Default: 0
Specifies the high threshold number of PDP contexts for any one ASN-GW service that must be met or exceeded within the polling interval to generate an alert or alarm.
| **low_thresh** is an integer from 0 through 2500000. A value of 0 disables the threshold.

| **clear low_thresh**
Default: 0
Specifies the low threshold number of PDP contexts for any one ASN-GW service that maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.
| **low_thresh** is an integer from 0 through 2500000. A value of 0 disables the threshold.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Monitor and set alarms or alerts when the number of PDP contexts for any ASN-GW service in the system is equal to or greater than the set limit.

Alerts or alarms are triggered for PDP contexts based on the following rules:

- **Enter condition:** Actual number of PDP contexts for any ASN-GW service is greater than or equal to the high threshold
- **Clear condition:** Actual number of PDP contexts is less than the low threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the threshold poll command to configure the polling interval and the threshold monitoring command to enable thresholding for this value.
Example

The following command configures a high threshold count of 10000 subscriber attaches per GGSN service for the Alert thresholding model:

```
threshold per-service-asngw-sessions 10000
```
threshold per-service-ggsn-sessions

Configures alarm or alert thresholds for the number of PDP contexts per GGSN service in the system.

Product
GGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

```
threshold per-service-ggsn-sessions high_thresh [ clear low_thresh ]
```

- **high_thresh**
  - Default: 0
  - Specifies the high threshold number of PDP contexts for any one GGSN service that must be met or exceeded within the polling interval to generate an alert or alarm.
  - `high_thresh` is an integer from 0 through 4000000. A value of 0 disables the threshold.

- **clear low_thresh**
  - Default: 0
  - Specifies the low threshold number of PDP contexts for any one GGSN service that maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.
  - `low_thresh` is an integer from 0 through 4000000. A value of 0 disables the threshold.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Monitor and set alarms or alerts when the number of PDP contexts for any GGSN service in the system is equal to or greater than the set limit.

Alerts or alarms are triggered for PDP contexts based on the following rules:

- **Enter condition:** Actual number of PDP contexts for any GGSN service is greater than or equal to the high threshold
- **Clear condition:** Actual number of PDP contexts is less than the low threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.
Example

The following command configures a high threshold count of 10000 subscriber attaches per GGSN service for the Alert thresholding model:

```
threshold per-service-ggsn-sessions 10000
```
threshold per-service-gprs-pdp-sessions

Configures alarm or alert thresholds for the number of 2G-activated PDP contexts per GPRS service.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration
   configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

**Syntax**

```
threshold per-service-gprs-pdp-sessions high_thresh [ clear low_thresh ]
```

---

### high_thresh

Default: 0
Specifies the high threshold number of 2G-activated PDP contexts for any one GPRS service. This number must be met or exceeded within the polling interval to generate an alert or alarm.

*high_thresh* is an integer from 0 through 4000000. A value of 0 disables the threshold.

---

### clear low_thresh

Default: 0
Specifies the low threshold number of 2G-activated PDP contexts for any one GPRS service. This number or higher maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, then a clear alarm will be generated.

*low_thresh* is an integer from 0 through 4000000. A value of 0 disables the threshold.

---

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

---

**Usage**

Monitor and set alarms or alerts when the number of 2G-activated PDP contexts for any GPRS service in the system is equal to or greater than the set limit.

Alerts or alarms are triggered for PDP contexts based on the following rules:

- **Enter condition:** Actual number of PDP contexts for any GPRS service is greater than or equal to the high threshold.

- **Clear condition:** Actual number of PDP contexts is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.
Example

The following command configures a high threshold count of 10000 2G-activated PDP contexts per GPRS service for the Alert thresholding model:

```
threshold per-service-gprs-sessions 10000
```
threshold per-service-gprs-sessions

Configures alarm or alert thresholds for the number of 2G-attached subscribers per GPRS service.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold per-service-gprs-sessions high_thresh [ clear low_thresh ]

high_thresh

Default: 0

Specifies the high threshold number of 2G-attached subscribers for any one GPRS service. This threshold number must be met or exceeded within the polling interval to generate an alert or alarm.

high_thresh is an integer from 0 through 2000000. A value of 0 disables the threshold.

clear low_thresh

Default: 0

Specifies the low threshold number of 2G-attached subscribers for any one GPRS service. The number of subscribers must remain above this threshold in order to maintain a previously generated alarm condition. If the number of 2G subscribers falls beneath the low threshold within the polling interval, then a clear alarm will be generated.

low_thresh is an integer from 0 through 2000000. A value of 0 disables the threshold.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Monitor and set alarms or alerts when the number of 2G-attached subscribers for any GPRS service in the system is equal to or greater than the set limit.

Alerts or alarms are triggered for PDP contexts based on the following rules:

• Enter condition: Actual number of 2G-attached subscribers for any GPRS service is greater than or equal to the high threshold.

• Clear condition: Actual number of 2G-attached subscribers is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Example**

The following command configures a high threshold count of **10000** 2G-attaches per GPRS service for the Alert thresholding model:

```
threshold per-service-gprs-sessions 10000
```
threshold per-service-ha-sessions

Configures alarm or alert thresholds for the number of HA sessions per Home Agent (HA) service in the system.

Product

HA

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold per-service-ha-sessions high_thresh [ clear low_thresh ]

- **high_thresh**
  - Default: 0
  - Specifies the high threshold number of HA sessions for any one HA service that must be met or exceeded within the polling interval to generate an alert or alarm.
  - *high_thresh* is an integer from 0 through 4000000. A value of 0 disables the threshold.

- **clear low_thresh**
  - Default: 0
  - Specifies the low threshold number of HA sessions for any one HA service that maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.
  - *low_thresh* is an integer from 0 through 4000000. A value of 0 disables the threshold.

- **Important**: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Monitor and set alarms or alerts when the number of HA sessions for any HA service in the system is equal to or greater than the set limit.

Alerts or alarms are triggered for HA sessions based on the following rules:

- **Enter condition**: Actual number of HA sessions for any HA service is greater than or equal to the high threshold.

- **Clear condition**: Actual number of HA sessions is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the **threshold poll** command to configure the polling interval and the **threshold monitoring** command to enable thresholding for this value.
Example

The following command configures a HA session per service high threshold count of 10000 for a system using the Alert thresholding model:

```
threshold per-service-ha-sessions 10000
```
threshold per-service-lns-sessions

Configures alarm or alert thresholds for the number of L2TP Network Server (LNS) sessions per LNS service in the system.

Product
PDSN
GGSN
HA
ASN-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

```
threshold per-service-lns-sessions high_thresh [ clear low_thresh ]
```

high_thresh
Default: 0
Specifies the high threshold number of LNS sessions for any one LNS service that must be met or exceeded within the polling interval to generate an alert or alarm.

high_thresh is an integer from 0 through 2500000. A value of 0 disables the threshold.

clear low_thresh
Default: 0
Specifies the low threshold number of LNS sessions for any one LNS service that maintains a previously generated alarm condition. If the number of LNS sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.

low_thresh is an integer from 0 through 2500000. A value of 0 disables the threshold.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage
Monitor and set alarms or alerts when the number of LNS sessions for any LNS service in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for LNS sessions based on the following rules:

- **Enter condition:** Actual number of LNS sessions for any LNS service is greater than or equal to the high threshold.
**Clear condition:** Actual number of LNS sessions is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Example**

The following command configures a LNS session per service high threshold count of **10000** for a system using the Alert thresholding model:

```
threshold per-service-Ins-sessions 10000
```
threshold per-service-pdg-sessions

Configures alarm or alert thresholds for the number of Packet Data Gateway (PDG) sessions per PDG service in the system.

**Product**
PDG/TTG

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
threshold per-service-pdg-sessions high_thresh [ clear low_thresh ]
```

**high_thresh**
Default: 0
Specifies the high threshold number of PDG sessions for any one PDG service that must be met or exceeded within the polling interval to generate an alert or alarm.

*high_thresh* is an integer from 0 through 1000000. A value of 0 disables the threshold.

**clear low_thresh**
Default: 0
Specifies the low threshold number of PDG sessions for any one PDG service that maintains a previously generated alarm condition. If the number of PDG sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.

*low_thresh* is an integer from 0 through 1000000. A value of 0 disables the threshold.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**
Monitor and set alarms or alerts when the number of PDG sessions for any PDG service in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for PDSN sessions based on the following rules:

- **Enter condition:** Actual number of PDG sessions for any PDG service is greater than or equal to the high threshold.

- **Clear condition:** Actual number of PDSN sessions is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

Example

The following command configures a PDG session per service high threshold count of 10000 for a system using the Alert thresholding model:

```
threshold per-service-pdg-sessions 10000
```
threshold per-service-pdsn-sessions

Configures alarm or alert thresholds for the number of Packet Data Serving Node (PDSN) sessions per PDSN service in the system.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
threshold per-service-pdsn-sessions high_thresh [ clear low_thresh ]
```

**high_thresh**

Default: 0
Specifies the high threshold number of PDSN sessions for any one PDSN service that must be met or exceeded within the polling interval to generate an alert or alarm.

*high_thresh* is an integer from 0 through 2500000. A value of 0 disables the threshold.

**clear low_thresh**

Default: 0
Specifies the low threshold number of PDSN sessions for any one PDSN service that maintains a previously generated alarm condition. If the number of PDSN sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.

*low_thresh* is an integer from 0 through 2500000. A value of 0 disables the threshold.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**

Monitor and set alarms or alerts when the number of PDSN sessions for any PDSN service in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for PDSN sessions based on the following rules:

- **Enter condition:** Actual number of PDSN sessions for any PDSN service is greater than or equal to the high threshold.
- **Clear condition:** Actual number of PDSN sessions is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Example**

The following command configures a PDSN session per service high threshold count of 10000 for a system using the Alert thresholding model:

```
threshold per-service-pdsn-sessions 10000
```
threshold per-service-sgsn-pdp-sessions

Configures alarm or alert thresholds for the number of 3G-activated PDP contexts per SGSN service on the system.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

**Syntax**
```plaintext
threshold per-service-sgsn-pdp-sessions high_thresh [ clear low_thresh ]
```

| high_thresh |
| Default: 0 |
| Specifies the high threshold number of 3G-activated PDP contexts for any one SGSN service. This number must be met or exceeded within the polling interval to generate an alert or alarm. |
| high_thresh is an integer from 0 through 4000000. A value of 0 disables the threshold. |

| clear low_thresh |
| Default: 0 |
| Specifies the low threshold number of 3G-activated PDP contexts for any one SGSN service. This number or higher maintains a previously generated alarm condition. If the number of 3G-activated PDP contexts falls beneath the low threshold within the polling interval, a clear alarm will be generated. |
| low_thresh is an integer from 0 through 2400000. A value of 0 disables the threshold. |

---

**Important**: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**
Monitor and set alarms or alerts when the number of 3G-activated PDP contexts for any SGSN service in the system is equal to or greater than the set limit.

Alerts or alarms are triggered for PDP contexts based on the following rules:

- **Enter condition**: Actual number of 3G-activated PDP contexts for any SGSN service is greater than or equal to the high threshold.

- **Clear condition**: Actual number of 3G-activated PDP contexts is less than the low threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.
Example

The following command configures a high threshold count of 10000 3G-activated PDP contexts per SGSN service for the system’s Alert thresholding model:

```
threshold per-service-sgsn-sessions 10000
```
threshold per-service-sgsn-sessions

Configures alarm or alert thresholds for the number of 3G-attached subscribers per SGSN service in the system.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:
[local]host_name(config)#

Syntax

threshold per-service-sgsn-sessions high_thresh [ clear low_thresh ]

high_thresh
Default: 0
Specifies the high threshold number of 3G-attached subscribers for any one SGSN service. This number must be met or exceeded within the polling interval to generate an alert or alarm.
high_thresh is an integer from 0 through 2000000. A value of 0 disables the threshold.

clear low_thresh
Default: 0
Specifies the low threshold number of 3G-attached subscribers for any one SGSN service. This number must be met or exceeded to maintain a previously generated alarm condition. If the number of subscribers falls beneath the low threshold within the polling interval, a clear alarm will be generated.
low_thresh is an integer from 0 through 2000000. A value of 0 disables the threshold.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage
Monitor and set alarms or alerts when the number of 3G-attached subscribers for any one SGSN service in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for PDP contexts based on the following rules:

- **Enter condition**: Actual number of 3G-attached subscribers for any single SGSN service is greater than or equal to the high threshold.
- **Clear condition**: Actual number of 3G-attached subscribers for any single SGSN service is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Example**

The following command configures a high threshold count of 10000 3G-attached subscribers per SGSN service for a system using the Alert thresholding model:

```
threshold per-service-sgsn-sessions 10000
```
threshold phsgw-auth-failure

Configures alarm or alert thresholds for the number of authentication failures in Personal Handyphone Service Gateway (PHSGW) service.

Product
PHSGW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold phsgw-auth-failure high_thresh [ clear low_thresh ]

#### high_thresh

Default: 0
Specifies the high threshold number for PHSGW authentication failures in any one PHSGW service. This number must be met or exceeded within the polling interval to generate an alert or alarm.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

#### clear low_thresh

Default: 0
Specifies the low threshold number of PHSGW authentication failures in any one PHSGW service. This number must be met or exceeded to maintain a previously generated alarm condition. If the number of subscribers falls beneath the low threshold within the polling interval, a clear alarm will be generated.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Set the monitoring and clearing thresholds for PHSGW authentication failures.

Alerts or alarms are triggered for authentication failures based on the following rules:

- **Enter condition:** Actual number of PHSGW authentication failures in any one PHSGW service is greater than or equal to the high threshold.

- **Clear condition:** Actual number of PHSGW authentication failures in any one PHSGW service is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the *threshold poll* command to configure the polling interval and the *threshold monitoring* command to enable thresholding for this value.

**Example**

The following command configures a monitoring threshold of 100000 and a clearing threshold of 50000 for PHSGW auth failures:

```
threshold phsgw-auth-failure 100000 clear 50000
```
threshold phsgw-eapol-auth-failure

Configures alarm or alert thresholds for authentication failures for a PHSGW service using Extensible Authentication Protocol Over LAN (EAPOL).

Product
PHSGW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold phsgw-eapol-auth-failure high_thresh [ clear low_thresh ]

- **high_thresh**
  Default: 0
  Specifies the high threshold number for PHSGW EAPOL failures in any one PHSGW service. This number must be met or exceeded within the polling interval to generate an alert or alarm.
  **high_thresh** is an integer from 0 through 1000000. A value of 0 disables the threshold.

- **clear low_thresh**
  Default: 0
  Specifies the low threshold number of PHSGW EAPOL failures in any one PHSGW service. This number must be met or exceeded to maintain a previously generated alarm condition. If the number of subscribers falls beneath the low threshold within the polling interval, a clear alarm will be generated.
  **low_thresh** is an integer from 0 through 1000000. A value of 0 disables the threshold.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Set the monitoring and clearing thresholds for PHSGW EAPOL failures. Alerts or alarms are triggered for EAPOL failures based on the following rules:

- **Enter condition:** Actual number of PHSGW EAPOL failures in any one PHSGW service is greater than or equal to the high threshold.
- **Clear condition:** Actual number of PHSGW EAPOL failures in any one PHSGW service is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Example**

The following command configures a monitoring threshold of 100000 and a clearing threshold of 50000 for PHSGW EAPOL failures:

```
threshold phsgw-eapol-auth-failure 100000 clear 50000
```
**threshold phsgw-handoff-denial**

Configures alarm or alert thresholds for handoff denials in PHSGW.

**Product**
PHSGW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

```
configure
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
threshold phsgw-handoff-denial high_thresh [ clear low_thresh ]
```

```
high_thresh
Default: 0
Specifies the high threshold number of handoff denials for any one PHSGW service. This number must be met or exceeded within the polling interval to generate an alert or alarm.
`high_thresh` is an integer from 0 through 1000000. A value of 0 disables the threshold.
```

```
clear low_thresh
Default: 0
Specifies the low threshold number of handoff denials for any one PHSGW service. This number must be met or exceeded to maintain a previously generated alarm condition. If the number of subscribers falls beneath the low threshold within the polling interval, a clear alarm will be generated.
`low_thresh` is an integer from 0 through 1000000. A value of 0 disables the threshold.
```

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**

Set the monitoring and clearing thresholds for PHSGW handoff denials.

Alerts or alarms are triggered for handoff denials based on the following rules:

- **Enter condition:** Actual number of PHSGW handoff denials in any one PHSGW service is greater than or equal to the high threshold.
- **Clear condition:** Actual number of PHSGW handoff denials in any one PHSGW service is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.
Example

The following command configures a monitoring threshold of 100000 and a clearing threshold of 50000 for PHSGW handoff denials:

```
threshold phsgw-handoff-denial 100000 clear 50000
```
threshold phsgw-max-eap-retry

Configures alarm or alert thresholds for the maximum number of Extensible Authentication Protocol (EAP) retries in PHSGW.

Product

PHSGW

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold phsgw-max-eap-retry high_thresh [ clear low_thresh ]

| high_thresh

Default: 0
Specifies the high threshold number of EAP retries for any one PHSGW service. This number must be met or exceeded within the polling interval to generate an alert or alarm.

| low_thresh

Default: 0
Specifies the low threshold number of EAP retries for any one PHSGW service. This number must be met or exceeded to maintain a previously generated alarm condition. If the number of subscribers falls beneath the low threshold within the polling interval, a clear alarm will be generated.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Set the monitoring and clearing thresholds for PHSGW EAP retries.
Alerts or alarms are triggered for handoff denials based on the following rules:

- **Enter condition:** Actual number of PHSGW EAP retries in any one PHSGW service is greater than or equal to the high threshold.

- **Clear condition:** Actual number of PHSGW EAP retries in any one PHSGW service is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Example**

The following command configures a monitoring threshold of 100000 and a clearing threshold of 50000 for PHSGW EAP retries:

```
threshold phsgw-max-eap-retry 100000 clear 50000
```
threshold phsgw-max-eapol-retry

Configures alarm or alert thresholds for the maximum number of Extensible Authentication Protocol over LAN (EAPOL) retries in PHSGW.

Product
PHSGW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold phsgw-max-eapol-retry high_thresh [ clear low_thresh ]

- **high_thresh**
  - Default: 0
  - Specifies the high threshold number of EAPOL retries for any one PHSGW service. This number must be met or exceeded within the polling interval to generate an alert or alarm.
  - *high_thresh* is an integer from 0 through 1000000. A value of 0 disables the threshold.

- **clear low_thresh**
  - Default: 0
  - Specifies the low threshold number of EAPOL retries for any one PHSGW service. This number must be met or exceeded to maintain a previously generated alarm condition. If the number of subscribers falls beneath the low threshold within the polling interval, a clear alarm will be generated.
  - *low_thresh* is an integer from 0 through 1000000. A value of 0 disables the threshold.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Set the monitoring and clearing thresholds for PHSGW EAPOL retries.
Alerts or alarms are triggered for handoff denials based on the following rules:

- **Enter condition:** Actual number of PHSGW EAPOL retries in any one PHSGW service is greater than or equal to the high threshold.

- **Clear condition:** Actual number of PHSGW EAPOL retries in any one PHSGW service is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Example**

The following command configures a monitoring threshold of 100000 and a clearing threshold of 50000 for PHSGW EAPOL retries:

```
threshold phsgw-max-eapol-retry 100000 clear 50000
```
threshold phsgw-network-entry-denial

Configures, alarm or alert thresholds for the number of network entry denials in PHSGW.

Product
PHSGW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

```
threshold phsgw-max-network-entry-denial high_thresh [ clear low_thresh ]
```

**high_thresh**

Default: 0

Specifies the high threshold number of network entry denials for any one PHSGW service. This number must be met or exceeded within the polling interval to generate an alert or alarm.

*high_thresh* is an integer from 0 through 1000000. A value of 0 disables the threshold.

**clear low_thresh**

Default: 0

Specifies the low threshold number of network entry denials for any one PHSGW service. This number must be met or exceeded to maintain a previously generated alarm condition. If the number of subscribers falls beneath the low threshold within the polling interval, a clear alarm will be generated.

*low_thresh* is an integer from 0 through 1000000. A value of 0 disables the threshold.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Set the monitoring and clearing thresholds for PHSGW network entry denials. Alerts or alarms are triggered for handoff denials based on the following rules:

- **Enter condition:** Actual number of PHSGW network entry denials in any one PHSGW service is greater than or equal to the high threshold.

- **Clear condition:** Actual number of PHSGW network entry denials in any one PHSGW service is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.
Example

The following command configures a monitoring threshold of 100000 and a clearing threshold of 50000 for PHSGW network entry denials:

```
threshold phsgw-network-entry-denial 100000 clear 50000
```
threshold phsgw-session-setup-timeout

Configures alarm or alert thresholds for the number of PHSGW sessions that timed out during setup.

**Product**
PHSGW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
threshold phsgw-session-setup-timeout high_thresh [ clear low_thresh ]
```

- **high_thresh**
  Default: 0
  Specifies the high threshold number of session setup timeouts for any one PHSGW service. This number must be met or exceeded within the polling interval to generate an alert or alarm.
  `high_thresh` is an integer from 0 through 1000000. A value of 0 disables the threshold.

- **clear low_thresh**
  Default: 0
  Specifies the low threshold number of session setup timeouts for any one PHSGW service. This number must be met or exceeded to maintain a previously generated alarm condition. If the number of subscribers falls beneath the low threshold within the polling interval, a clear alarm will be generated.
  `low_thresh` is an integer from 0 through 1000000. A value of 0 disables the threshold.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**

Set the monitoring and clearing thresholds for PHSGW session setup timeouts.
Alerts or alarms are triggered for handoff denials based on the following rules:

- **Enter condition:** Actual number of PHSGW session setup timeouts in any one PHSGW service is greater than or equal to the high threshold.
- **Clear condition:** Actual number of PHSGW session setup timeouts in any one PHSGW service is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.
Example

The following command configures a monitoring threshold of 100000 and a clearing threshold of 50000 for PHSGW session setup timeouts:

```
threshold phsgw-session-setup-timeout 100000 clear 50000
```
threshold phsgw-session-timeout

Configures alarm or alert thresholds for the number of PHSGW sessions that timed out.

**Product**
PHSGW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration
*configure*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
threshold phsgw-session-timeout high_thresh [ clear low_thresh ]
```

- **high_thresh**
  
  Default: 0
  
  Specifies the high threshold number of session timeouts for any one PHSGW service. This number must be met or exceeded within the polling interval to generate an alert or alarm.
  
  high_thresh is an integer from 0 through 1000000. A value of 0 disables the threshold.

- **clear low_thresh**

  Default: 0
  
  Specifies the low threshold number of session timeouts for any one PHSGW service. This number must be met or exceeded to maintain a previously generated alarm condition. If the number of subscribers falls beneath the low threshold within the polling interval, a clear alarm will be generated.
  
  low_thresh is an integer from 0 through 1000000. A value of 0 disables the threshold.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**

Set the monitoring and clearing thresholds for PHSGW session timeouts.

Alerts or alarms are triggered for handoff denials based on the following rules:

- **Enter condition:** Actual number of PHSGW session timeouts in any one PHSGW service is greater than or equal to the high threshold.

- **Clear condition:** Actual number of PHSGW session timeouts in any one PHSGW service is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the threshold poll command to configure the polling interval and the threshold monitoring command to enable thresholding for this value.
Example

The following command configures a monitoring threshold of 100000 and a clearing threshold of 50000 for PHSGW session timeouts:

```
threshold phsgw-session-timeout 100000 clear 50000
```
### threshold phspc-session-setup-timeout

Configures alarm or alert thresholds for the number of Personal Handyphone System - Personal Computer (PHSPC) sessions that timed out during setup.

**Product**
- PHSGW

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration
  ```
  configure
  ```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config)#
```

**Syntax**

```
threshold phspc-session-setup-timeout high_thresh  [ clear low_thresh ]
```

- **high_thresh**
  
  Default: 0
  
  Specifies the high threshold number of session setup timeouts for any one PHSPC service. This number must be met or exceeded within the polling interval to generate an alert or alarm.
  
  `high_thresh` is an integer from 0 through 1000000. A value of 0 disables the threshold.

- **clear low_thresh**
  
  Default: 0
  
  Specifies the low threshold number of session setup timeouts for any one PHSPC service. This number must be met or exceeded to maintain a previously generated alarm condition. If the number of subscribers falls beneath the low threshold within the polling interval, a clear alarm will be generated.
  
  `low_thresh` is an integer from 0 through 1000000. A value of 0 disables the threshold.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**

Set the monitoring and clearing thresholds for PHSPC session setup timeouts.

Alerts or alarms are triggered for handoff denials based on the following rules:

- **Enter condition:** Actual number of PHSPC session setup timeouts in any one PHSGW service is greater than or equal to the high threshold.
  
  - **Clear condition:** Actual number of PHSPC session setup timeouts in any one PHSGW service is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

Example

The following command configures a monitoring threshold of 100000 and a clearing threshold of 50000 for PHSPC session setup timeouts:

```
threshold phspc-session-setup-timeout 100000 clear 50000
```
threshold phspc-sleep-mode-timeout

Configures alarm or alert thresholds for the number of PHSPC sessions that timed out when the personal computer went into sleep mode.

**Product**

PHSGW

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration

**Syntax**

```
threshold phspc-sleep-mode-timeout high_thresh [ clear low_thresh ]
```

- **high_thresh**
  
  Default: 0
  
  Specifies the high threshold number of sleep mode timeouts for any one PHSPC service. This number must be met or exceeded within the polling interval to generate an alert or alarm. `high_thresh` is an integer from 0 through 1000000. A value of 0 disables the threshold.

- **clear low_thresh**
  
  Default: 0
  
  Specifies the low threshold number of sleep mode timeouts for any one PHSPC service. This number must be met or exceeded to maintain a previously generated alarm condition. If the number of subscribers falls beneath the low threshold within the polling interval, a clear alarm will be generated. `low_thresh` is an integer from 0 through 1000000. A value of 0 disables the threshold.

- **Important**: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**

Set the monitoring and clearing thresholds for PHSPC sleep mode timeouts. Alerts or alarms are triggered for handoff denials based on the following rules:

- **Enter condition**: Actual number of PHSPC sleep mode timeouts in any one PHSGW service is greater than or equal to the high threshold.

- **Clear condition**: Actual number of PHSPC sleep mode timeouts in any one PHSGW service is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Example**

The following command configures a monitoring threshold of 100000 and a clearing threshold of 50000 for PHSPC sleep mode timeouts:

```
threshold phspc-sleep-mode-timeout 100000 clear 50000
```
threshold phspc-sm-entry-denial

Configures alarm or alert thresholds for the number of denied PHSPC short message (SM) sessions.

**Product**
PHSGW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration
configure
Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
threshold phspc-sm-entry-denial high_thresh [ clear low_thresh ]
```

- **high_thresh**
  - Default: 0
  - Specifies the high threshold number of SM entry denials for any one PHSPC service. This number must be met or exceeded within the polling interval to generate an alert or alarm.
  - *high_thresh* is an integer from 0 through 1000000. A value of 0 disables the threshold.

- **clear low_thresh**
  - Default: 0
  - Specifies the low threshold number of SM entry denials for any one PHSPC service. This number must be met or exceeded to maintain a previously generated alarm condition. If the number of subscribers falls beneath the low threshold within the polling interval, a clear alarm will be generated.
  - *low_thresh* is an integer from 0 through 1000000. A value of 0 disables the threshold.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**
Set the monitoring and clearing thresholds for PHSPC SM entry denials.
Alerts or alarms are triggered for handoff denials based on the following rules:

- **Enter condition:** Actual number of PHSPC SM entry denials in any one PHSPC service is greater than or equal to the high threshold.
- **Clear condition:** Actual number of PHSPC SM entry denials in any one PHSPC service is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the *threshold poll* command to configure the polling interval and the *threshold monitoring* command to enable thresholding for this value.
Example

The following command configures a monitoring threshold of 100000 and a clearing threshold of 50000 for PHSPC SM entry denials:

```
threshold phsgw-sm-entry-denial 100000 clear 50000
```
Chapter 143
Global Configuration Mode Commands (threshold poll commands A - N)

This section includes the commands threshold poll 10sec-cpu-utilization interval through threshold poll npu-utilization interval.

The Global Configuration Mode is used to configure basic system-wide parameters.

Mode

Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
threshold poll 10sec-cpu-utilization interval

Configures the polling interval over which to measure a 10-second average of CPU utilization.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local]host_name(config) #

Syntax

threshold poll 10sec-cpu-utilization interval duration

default threshold poll 10sec-cpu-utilization interval

default
Restores the specified parameter to its default value 300 seconds.

interval duration
Default: 300 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
duration is an integer from 30 through 60000 in multiples of 30.

Usage

This command sets the time period over which to monitor the specified value for threshold crossing.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system’s support for thresholds in this chapter.

Important: To enable an SNMP trap for monitoring this threshold use the snmp trap enable ThreshCPUUtilization10Sec command in this mode.

Example

The following command configures the polling interval to 600 seconds for the 10-second CPU utilization threshold:

threshold poll 10sec-cpu-utilization 600
threshold poll a11-ppp-send-discard interval

Configures the polling interval for PDSN service over which to count the number of packets that the PPP protocol processing layer internally discarded on transmit for any reason.

Product
PDSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

```
threshold poll a11-ppp-send-discard interval duration
```

default threshold poll a11-ppp-send-discard interval

default
Restores the specified parameter to its default value 0 seconds.

```
interval duration
```
Default: 0 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
`duration` is an integer from 60 through 900 in multiples of 30.

Usage
This command sets the time period over which to monitor the specified value for threshold crossing.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the `threshold monitoring` and other threshold commands for additional information on the system’s support for thresholds in this chapter.

Important: To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshPDSNSvcA11PPPSendDiscard` command in this mode.

Example
The following command configures the polling interval to 600 seconds for the A11 PPP send discard threshold:
threshold poll all-ppp-send-discard interval 600
threshold poll a11-rac-msg-discard interval

Configures the polling interval for PDSN service over which to count the number of Discarded A11 Registration Acknowledgements.

**Product**

PDSN

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration

**Syntax**

```
threshold poll a11-rac-msg-discard interval duration
default threshold poll a11-rac-msg-discard interval
```

**Default**

Restores the specified parameter to its default value 0 seconds.

```
default
```

**interval duration**

Default: 0 seconds.

Specifies the amount of time (in seconds) that comprises the polling interval. duration is an integer from 60 through 900 in multiples of 30.

**Usage**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system’s support for thresholds in this chapter.

**Important:** To enable an SNMP trap for monitoring this threshold use the **snmp trap enable** **ThreshPDSNSvcA11RACMsgDiscard** command in this mode.

**Example**

The following command configures the polling interval to 600 seconds for the A11 RAC message discard threshold:
threshold poll all-rac-msg-discard interval 600
threshold poll aa11-rrp-failure interval

Configures the polling interval for PDSN service over which to count A11 Registration Response failures.

**Product**  
PDSN

**Privilege**  
Security Administrator, Administrator

**Mode**  
Exec > Global Configuration  
```bash
configure
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
threshold poll all-rrp-failure interval duration

default threshold poll all-rrp-failure interval
```

**Usage**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system’s support for thresholds in this chapter.

**Important:** To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshPDSNSvcAllRRPFailure` command in this mode.

**Example**

The following command configures the polling interval to 600 seconds for the A11 RRP failure threshold:

```
threshold poll all-rrp-failure interval 600
```
threshold poll a11-rrq-msg-discard interval

Configures the polling interval for PDSN service over which to count how many A11 Registration Request messages are discarded.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
threshold poll a11-rrq-msg-discard interval duration

default threshold poll a11-rrq-msg-discard interval

default

Restores the specified parameter to its default value 0 seconds.

interval duration

Default: 0 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
duration is an integer from 60 through 900 in multiples of 30.
```

**Usage**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system’s support for thresholds in this chapter.

**Important:** To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshPDSNSvcAllRRQMsgDiscard` command in this mode.

**Example**

The following command configures the polling interval to 600 seconds for the A11 RRQ message discard threshold:
threshold poll all-rrq-msg-discard interval 600
threshold poll aaa-acct-archive-queue-size interval

Configures the polling interval over which to measure AAA accounting archive message queue size.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local] host_name(config) #

Syntax

threshold poll aaa-acct-archive-queue-size1 interval duration
default threshold poll aaa-acct-archive-queue-size1 interval
threshold poll aaa-acct-archive-queue-size2 interval duration
default threshold poll aaa-acct-archive-queue-size2 interval
threshold poll aaa-acct-archive-queue-size3 interval duration
default threshold poll aaa-acct-archive-queue-size3 interval

default
Restores the specified parameter to its default value 900 seconds.

interval duration
Default: 900 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
duration is an integer from 60 through 60000 in multiples of 30.

Usage

This command sets the time period over which to monitor the specified value for threshold crossing.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system’s support for thresholds in this chapter.
**Important:** To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshAAAAcctArchiveQueue-<1-3>` command in this mode.

**Example**

The following command configures the polling interval to 600 seconds for the AAA accounting archive queue size 1 threshold:

```
threshold poll aaa-acct-archive-queue-size1 interval 600
```
threshold poll aaa-acct-archive-size interval

Configures the polling interval over which to count archived AAA accounting messages.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold poll aaa-acct-archive-size interval duration

default threshold poll aaa-acct-archive-size interval

default
Restores the specified parameter to its default value 300 seconds.

interval duration
Default: 300 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
duration is an integer from 60 through 60000 in multiples of 30.

Usage
This command sets the time period over which to monitor the specified value for threshold crossing.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system’s support for thresholds in this chapter.

Example

The following command configures the polling interval to 600 seconds for the AAA accounting archive size threshold:

threshold poll aaa-acct-archive-size interval 600
threshold poll aaa-acct-failure interval

Configures the polling interval over which to count failed AAA accounting requests.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
threshold poll aaa-acct-failure interval duration

default threshold poll aaa-acct-failure interval
```

**Usage**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the `threshold monitoring` and other threshold commands for additional information on the system’s support for thresholds in this chapter.

**Important:** To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshAAAACacctFail` command in this mode.

**Example**

The following command configures the polling interval to 600 seconds for the AAA accounting failure threshold:

```
threshold poll aaa-acct-failure interval 600
```
threshold poll aaa-acct-failure-rate interval

Configures the polling interval over which to measure the percentage of AAA accounting failures.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold poll aaa-acct-failure-rate interval duration

default threshold poll aaa-acct-failure-rate interval

default

Restores the specified parameter to its default value 300 seconds.

interval duration

Default: 300 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
duration is an integer from 60 through 60000 in multiples of 30.

Usage

This command sets the time period over which to monitor the specified value for threshold crossing.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system’s support for thresholds in this chapter.

Important: To enable an SNMP trap for monitoring this threshold use the snmp trap enable ThreshAAAAcctFailRate command in this mode.

Example

The following command configures the polling interval to 600 seconds for the AAA accounting failure rate threshold:

threshold poll aaa-acct-failure-rate interval 600
threshold poll aaa-auth-failure interval

Configures the polling interval over which to count failed authentication requests.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold poll aaa-auth-failure interval duration

default threshold poll aaa-auth-failure interval

default
Restores the specified parameter to its default value 300 seconds.

interval duration
Default: 300 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
duration is an integer from 60 through 60000 in multiples of 30.

Usage
This command sets the time period over which to monitor the specified value for threshold crossing.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system’s support for thresholds in this chapter.

Important: To enable an SNMP trap for monitoring this threshold use the snmp trap enable ThreshAAAAuthFail command in this mode.

Example
The following command configures the polling interval to 600 seconds for the AAA authentication failure threshold:

threshold poll aaa-auth-failure interval 600
threshold poll aaa-auth-failure-rate interval

Configures the polling interval over which to measure the percentage of AAA authentication failures.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local] host_name(config) #

**Syntax**

`threshold poll aaa-auth-failure-rate interval duration`

`default threshold poll aaa-auth-failure-rate interval`

**default**

Restores the specified parameter to its default value 300 seconds.

`interval duration`

Default: 300 seconds.

Specifies the amount of time (in seconds) that comprises the polling interval.

`duration` is an integer from 60 through 60000 in multiples of 30.

**Usage**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the `threshold monitoring` and other threshold commands for additional information on the system’s support for thresholds in this chapter.

**Important:** To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshAAAAuthFailRate` command in this mode.

**Example**

The following command configures the polling interval to 600 seconds for the AAA authentication failure rate threshold:

`threshold poll aaa-auth-failure-rate interval 600`
threshold poll aaa-retry-rate interval

Configures the polling interval over which to measure the percent of AAA request message retries.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local] host_name(config) #

Syntax

threshold poll aaa-retry-rate interval duration

default threshold poll aaa-retry-rate interval

default
Restores the specified parameter to its default value 300 seconds.

interval duration
Default: 300 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
duration is an integer from 60 through 60000 in multiples of 30.

Usage
This command sets the time period over which to monitor the specified value for threshold crossing.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system’s support for thresholds in this chapter.

Important: To enable an SNMP trap for monitoring this threshold use the snmp trap enable ThreshAAARetryRate command in this mode.

Example

The following command configures the polling interval to 600 seconds for the AAA retry rate threshold:

threshold poll aaa-retry-rate interval 600
threshold poll aaamgr-request-queue interval

Configures the polling interval over which to count the number of AAA Manager Requests for each AAA manager process.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure
Entering the above command sequence results in the following prompt:

[local]host_name(config) #

Syntax

threshold poll aaamgr-request-queue interval duration

default threshold poll aaamgr-request-queue interval

default
Restores the specified parameter to its default value 0 seconds.

interval duration
Default: 0 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
duration is an integer from 60 through 60000 in multiples of 30.

Usage
This command sets the time period over which to monitor the specified value for threshold crossing.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system’s support for thresholds in this chapter.

Important: To enable an SNMP trap for monitoring this threshold use the snmp trap enable ThreshAAAMgrQueue command in this mode.

Example
The following command configures the polling interval to 600 seconds for the AAA manager request queue threshold:
threshold poll aaamgr-request-queue interval 600
threshold poll active-subscriber interval

Configures the polling interval over which to count the total number of active subscriber sessions.

**Product**
- All

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration
  ```
  configure
  ```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
threshold poll active-subscriber interval duration

default threshold poll active-subscriber interval
```

```
default
Restores the specified parameter to its default value 300 seconds.
```

```
interval duration
Default: 300 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
duration is an integer from 60 through 60000 in multiples of 30.
```

**Usage**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system’s support for thresholds in this chapter.

**Important:** To enable an SNMP trap for monitoring this threshold use the **snmp trap enable ThreshSubscriberActive** command in this mode.

**Example**

The following command configures the polling interval to 600 seconds for the active subscriber threshold:

```
threshold poll active-subscriber interval 600
```
threshold poll asngw-auth-failure interval

Configures the polling interval over which to count or measure the thresholding value for ASN Gateway authentication failure.

**Product**
ASN-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

**Syntax**

```
threshold poll asngw-auth-failure interval dur
```

**Usage**

This command sets the time period over which to monitor the specified value for threshold crossing.

---
**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the *threshold monitoring* and other threshold commands for additional information on the system’s support for thresholds in this chapter.

---
**Important:** To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThresholdASNGWAuthFail` command in this mode.

**Example**

The following command configures the polling interval to 600 seconds for the ASN Gateway authentication failure threshold:
threshold poll asngw-auth-failure interval 600
threshold poll asngw-handoff-denial interval

Configures the polling interval over which to count or measure the thresholding value for ASN Gateway hand-off denial.

Product
ASN-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold poll asngw-handoff-denial interval  dur

default threshold poll asngw-handoff-denial interval

default
Restores the specified parameter to its default value 300 seconds.

interval  dur
Default: 300 seconds.
Specifies the polling interval time in seconds.
dur is an integer from 30 through 60000 in multiples of 30.

Usage

This command sets the time period over which to monitor the specified value for threshold crossing.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system’s support for thresholds in this chapter.

Important: To enable an SNMP trap for monitoring this threshold use the snmp trap enable ThreshASNGWHandoffDenial command in this mode.

Example

The following command configures the polling interval to 600 seconds for the hand-off denial threshold:

threshold poll asngw-handoff-denial interval 600
threshold poll asngw-max-eap-retry interval

Configures the polling interval over which to count or measure the thresholding value for maximum Extensible Authentication Protocol (EAP) authentication retries.

**Product**
ASN-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

```
[local] host_name(config) #
```

**Syntax**

```
threshold poll asngw-max-eap-retry interval dur

default threshold poll asngw-max-eap-retry interval
```

**default threshold poll asngw-max-eap-retry interval**

- **default**
  Restores the specified parameter to its default value 300 seconds.

- **interval dur**
  Default: 300 seconds.
  Specifies the amount of time (in seconds) that comprises the polling interval.
  *dur* is an integer from 30 through 60000 in multiples of 30.

**Usage**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system’s support for thresholds in this chapter.

**Important:** To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThresholdASNGWMaxEAPretry` command in this mode.

**Example**

The following command configures the polling interval to 600 seconds for the maximum EAP authentication retry threshold:
threshold poll asngw-max-eap-retry interval 600
threshold poll asngw-network-entry-denial interval

Configures the polling interval over which to count or measure the thresholding value for network entry denial to an MS.

Product
ASN-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config) #

Syntax

threshold poll asngw-network-entry-denial interval  dur

default threshold poll asngw-network-entry-denial interval

default
Restores the specified parameter to its default value 300 seconds.

interval  dur
Default: 300 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
dur is an integer from 30 through 60000 in multiples of 30.

Usage

This command sets the time period over which to monitor the specified value for threshold crossing.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system’s support for thresholds in this chapter.

Important: To enable an SNMP trap for monitoring this threshold use the snmp trap enable ThreshASNGWNNWEntryDenial command in this mode.

Example

The following command configures the polling interval to 600 seconds for the network entry denial threshold:
threshold poll asngw-network-entry-denial interval 600
threshold poll asngw-session-setup-timeout interval

Configures the polling interval over which to count or measure the thresholding value for session setup timeout.

Product
ASN-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config) #

Syntax

threshold poll asngw-session-setup-timeout interval dur

default threshold poll asngw-session-setup-timeout interval

default
Restores the specified parameter to its default value 300 seconds.

interval dur
Default: 300 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
dur is an integer from 30 through 60000 in multiples of 30.

Usage
This command sets the time period over which to monitor the specified value for threshold crossing.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system’s support for thresholds in this chapter.

Important: To enable an SNMP trap for monitoring this threshold use the snmp trap enable ThreshASNGWSessSetupTimeout command in this mode.

Example

The following command configures the polling interval to 600 seconds for the session setup timeout threshold:

threshold poll asngw-session-setup-timeout interval 600
threshold poll asngw-session-timeout interval

Configures the polling interval over which to count or measure the thresholding value for session timeout.

Product
ASN-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold poll asngw-session-timeout interval  
dur

default threshold poll asngw-session-timeout interval

  default
  Restores the specified parameter to its default value (300 seconds).

  interval  
dur
  Default: 300 seconds.
  Specifies the amount of time (in seconds) that comprises the polling interval.
  
dur  is an integer from 30 through 60000 in multiples of 30.

Usage

This command sets the time period over which to monitor the specified value for threshold crossing.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system’s support for thresholds in this chapter.

Important: To enable an SNMP trap for monitoring this threshold use the 

| snmp trap enable ThreshASNGWSessTimeout |

Example

The following command configures the polling interval to 600 seconds for the session timeout threshold:

threshold poll asngw-session-timeout interval 600
threshold poll asnpc-idle-mode-timeout interval

Configures the polling interval over which to count the number of ASNPC Instant Messenger idle mode timeouts.

**Product**
ASN-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

```
configure
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
threshold poll asnpc-idle-mode-timeout interval dur
```

```
default threshold poll asnpc-idle-mode-timeout interval
```

```
default
```

Restores the specified parameter to its default value (300 seconds).

```
interval dur
```

Default: 300 seconds.

Specifies the amount of time (in seconds) that comprises the polling interval.

`dur` is an integer from 30 through 60000 in multiples of 30.

**Usage**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system’s support for thresholds in this chapter.

**Important:** To enable an SNMP trap for monitoring this threshold use the `snmp trap enable` `ThreshASNPCIdleModeTimeout` command in this mode.

**Example**

The following command configures the polling interval to 600 seconds for the idle mode timeout threshold:

```
threshold poll asnpc-idle-mode-timeout interval 600
```
threshold poll asnpc-im-entry-denial interval

Configures the polling interval over which to count the number of ASNPC Instant Messenger entry denials.

Product
ASN-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold poll asnpc-im-entry-denial interval dur

default threshold poll asnpc-im-entry-denial interval

| default
| Restores the specified parameter to its default value (300 seconds).

| interval dur
| Default: 300 seconds.
| Specifies the amount of time (in seconds) that comprises the polling interval.
| dur is an integer from 30 through 60000 in multiples of 30.

Usage
This command sets the time period over which to monitor the specified value for threshold crossing.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system’s support for thresholds in this chapter.

Important: To enable an SNMP trap for monitoring this threshold use the snmp trap enable ThreshASNPCImEntryDenial command in this mode.

Example
The following command configures the polling interval to 600 seconds for the IM entry denial threshold:

threshold poll asnpc-im-entry-denial interval 600
threshold poll asnpc-lu-denial interval

Configures the polling interval over which to count the number of ASNPC Location Update (LU) denials.

Product
ASN-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold poll asnpc-lu-denial interval dur

default threshold poll asnpc-lu-denial interval interval

default
Restores the specified parameter to its default value (300 seconds).

interval dur
Default: 300 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
dur is an integer from 30 through 60000 in multiples of 30.

Usage

This command sets the time period over which to monitor the specified value for threshold crossing.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system’s support for thresholds in this chapter.

Important: To enable an SNMP trap for monitoring this threshold use the snmp trap enable ThreshASNPCLuDenial command in this mode.

Example

The following command configures the polling interval to 600 seconds for the LU denial threshold:

threshold poll asnpc-lu-denial interval 600
**threshold poll asnpc-session-setup-timeout interval**

Configures the polling interval over which to count the number of times an ASNPC session timed out before setup completion.

**Product**
ASN-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration
**configure**

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
threshold poll asnpc-session-setup-timeout interval dur

default threshold poll asnpc-session-setup-timeout interval
```

**Syntax**

```
default
```

Restores the specified parameter to its default value (300 seconds).

```
interval dur
```

Default: 300 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
`dur` is an integer from 30 through 60000 in multiples of 30.

**Usage**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the `threshold monitoring` and other threshold commands for additional information on the system’s support for thresholds in this chapter.

**Important:** To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshASNPCSessSetupTimeout` command in this mode.

**Example**

The following command configures the polling interval to 600 seconds for the session setup timeout threshold:
threshold poll asnpc-session-setup-timeout interval 600
threshold poll available-ip-pool-group interval

Configures the polling interval over which to measure IP pool utilization.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

**Syntax**

```
threshold poll available-ip-pool-group interval dur
```

**default threshold poll available-ip-pool-group interval**

```
default
Restores the specified parameter to its default value (300 seconds).
```

```
interval dur
Default: 300 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
dur is an integer from 30 through 60000 in multiples of 30.
```

**Usage**
This command sets the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system’s support for thresholds in this chapter.

**Important:** To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshIPPoolAvail` command in this mode.

**Example**
The following command configures the polling interval to 600 seconds for available IP pool threshold:

```
threshold poll available-ip-pool-group interval 600
```
threshold poll call-reject-no-resource interval

Configures the polling interval over which to measure IP pool utilization.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure
Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold poll call-reject-no-resource interval dur

default threshold poll call-reject-no-resource interval

default
Restores the specified parameter to its default value (900 seconds).

interval dur
Default: 900 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
dur is an integer from 30 through 60000 in multiples of 30.

Usage
This command sets the time period over which to monitor the specified value for threshold crossing.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system’s support for thresholds in this chapter.

Important: To enable an SNMP trap for monitoring this threshold use the snmp trap enable ThreshCallRejectNoResource command in this mode.

Example
The following command configures the polling interval to 600 seconds for call reject no-resource threshold:

threshold poll call-reject-no-resource interval 600
threshold poll call-setup interval

Configures the polling interval over which to count the number of calls that were setup.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold poll call-setup interval dur

default threshold poll call-setup interval

  default
  Restores the specified parameter to its default value (900 seconds).

  interval dur
  Default: 900 seconds.
  Specifies the amount of time (in seconds) that comprises the polling interval.
  dur is an integer from 30 through 60000 in multiples of 30.

Usage

This command sets the time period over which to monitor the specified value for threshold crossing.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system’s support for thresholds in this chapter.

Important: To enable an SNMP trap for monitoring this threshold use the snmp trap enable ThreshCallSetup command in this mode.

Example

The following command configures the polling interval to 600 seconds for the call setup threshold:

threshold poll call-setup interval 600
threshold poll call-setup-failure interval

Configures the polling interval over which to count the number of calls that failed to setup.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold poll call-setup-failure interval dur

default threshold poll call-setup-failure interval

default

Restores the specified parameter to its default value (900 seconds).

interval dur

Default: 900 seconds.

Specifies the amount of time (in seconds) that comprises the polling interval.

dur is an integer from 30 through 60000 in multiples of 30.

Usage

This command sets the time period over which to monitor the specified value for threshold crossing.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system’s support for thresholds in this chapter.

Important: To enable an SNMP trap for monitoring this threshold use the snmp trap enable ThreshCallSetupFailure command in this mode.

Example

The following command configures the polling interval to 600 seconds for call setup failure threshold:

threshold poll call-setup-failure interval 600
threshold poll call-setup-fails interval

Configures the polling interval over which to count the number of CSCF call setup failures.

**Product**
SCM

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

**Syntax**

```
threshold poll call-setup-failures interval \[\text{dur}\]
```

default threshold poll call-setup-failures interval

**Usage**
This command sets the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system’s support for thresholds in this chapter.

**Important:** To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshCSCFSvcTotalCallFailure` command in this mode.

**Example**
The following command configures the polling interval to **600** seconds for CSCF session timeout threshold:

```
threshold poll call-setup-failures interval 600
```
threshold poll call-total-active interval

Configures the polling interval over which to count the total number of CSCF active calls.

**Product**
SCM

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

*configure*

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

**Syntax**

```
threshold poll call-total-active interval dur
```

**default threshold poll call-total-active interval**

```
default
Restores the specified parameter to its default value (300 seconds).
```

```
interval dur
Default: 300 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
dur is an integer from 60 through 60000 in multiples of 30.
```

**Usage**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system’s support for thresholds in this chapter.

**Important:** To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshCSCFSvcTotalActiveCalls` command in this mode.

**Example**

The following command configures the polling interval to 600 seconds for session timeout threshold:

```
threshold poll call-total-active interval 600
```
threshold poll card-temperature-near-power-off-limit interval

Configures the polling interval over which to count the number of times card temperatures reached the power-off limit.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

**Syntax**

threshold poll card-temperature-near-power-off-limit interval \texttt{dur}

default threshold poll card-temperature-near-power-off-limit interval

\texttt{default}

Restores the specified parameter to its default value (300 seconds).

\texttt{interval \texttt{dur}}

Default: 300 seconds.

Specifies the amount of time (in seconds) that comprises the polling interval.

\texttt{dur} is an integer from 60 through 60000 in multiples of 30.

**Usage**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system’s support for thresholds in this chapter.

**Important:** To enable an SNMP trap for monitoring this threshold use the \texttt{snmp trap enable ThreshCardTemperatureNearPowerOffLimit} command in this mode.

**Example**

The following command configures the polling interval to 600 seconds for session timeout threshold:

threshold poll card-temperature-near-power-off-limit interval 600
threshold poll cdr-file-space interval

Configures the polling interval for Charging Data Record (CDR) File Space Usage threshold.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold poll cdr-file-space interval duration

default threshold poll cdr-file-space interval

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Uses the default polling interval. Default: 300 seconds</td>
</tr>
<tr>
<td>interval duration</td>
<td>Specifies the polling interval (in seconds) for the CDR File Space Usage threshold. duration must be an integer from 60 through 60000.</td>
</tr>
</tbody>
</table>

Usage

This command configures the polling interval for CDR File Space Usage threshold.

⚠️ Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system’s support for thresholds in this chapter.

⚠️ Important: To enable an SNMP trap for monitoring this threshold use the snmp trap enable ThreshCDRFileSpace command in this mode.

Example

The following command configures the polling interval to 600 seconds for the CDR file space usage threshold:

threshold poll cdr-file-space interval 600
threshold poll contfilt-block interval

Configures the polling interval Content Filtering Block threshold.

**Product**
CF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration
`configure`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
threshold poll contfilt-block interval duration
default threshold poll contfilt-block interval
```

- `default`
  Uses the default threshold polling interval.
  Default: 300 seconds

```
interval duration
```

- Specifies the polling interval (in seconds) for the Content Filtering Block threshold.
- `duration` must be an integer from 60 through 60000.

**Usage**

This command configures the polling interval Content Filtering Block threshold.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system’s support for thresholds in this chapter.

**Important:** To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshContFiltBlock` command in this mode.

**Example**

The following command configures the polling interval to **600** seconds for the content filtering blocking threshold:

```
threshold poll contfilt-block interval 600
```
threshold poll contfilt-rating interval

Configures the polling interval for the Content Filtering Rating threshold.

Product
    CF

Privilege
    Security Administrator, Administrator

Mode
    Exec > Global Configuration
    configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold poll contfilt-rating interval duration

default threshold poll contfilt-rating interval

<table>
<thead>
<tr>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uses the default threshold polling interval.</td>
</tr>
<tr>
<td>Default: 300 seconds</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>interval dur</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the polling interval (in seconds) for the Content Filtering Rating threshold.</td>
</tr>
<tr>
<td>duration must be an integer from 60 through 60000.</td>
</tr>
</tbody>
</table>

Usage

This command configures the polling interval for the Content Filtering Rating threshold.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system’s support for thresholds in this chapter.

**Important:** To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshContFiltRating` command in this mode.

Example

The following command configures the polling interval to 600 seconds for the content filtering rating processing threshold:

```
threshold poll contfilt-rating interval 600
```
threshold poll cpu-available-memory interval

Configures the polling interval over which to measure the percentage of total packet processing card CPU memory used.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

```
[local] host_name(config)#
```

**Syntax**

```
threshold poll cpu-available-memory interval duration
```

```
default threshold poll cpu-available-memory interval
```

<table>
<thead>
<tr>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uses the default threshold polling interval.</td>
</tr>
<tr>
<td>Default: 300 seconds</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>interval duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the amount of time (in seconds) that comprises the polling interval.</td>
</tr>
<tr>
<td>duration must be an integer from 30 through 60000.</td>
</tr>
</tbody>
</table>

**Usage**
This command sets the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system’s support for thresholds in this chapter.

**Important:** To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshCPU Memory` command in this mode.

**Example**
The following command configures the polling interval to 600 seconds for the CPU available memory threshold:

```
threshold poll cpu-available-memory interval 600
```
threshold poll cpu-load interval

Configures the polling interval over which to monitor packet processing card CPU loads using a 5-minute average measurement.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold poll cpu-load interval duration

default threshold poll cpu-load interval

default

Uses the default threshold polling interval.
Default: 300 seconds

interval dur

Specifies the amount of time (in seconds) that comprises the polling interval.
duration must be an integer from 30 through 60000.

Usage

This command sets the time period over which to monitor the specified value for threshold crossing.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system’s support for thresholds in this chapter.

Important: To enable an SNMP trap for monitoring this threshold use the snmp trap enable ThreshCPULoad command in this mode.

Example

The following command configures the polling interval to 600 seconds for the CPU load threshold:

threshold poll cpu-load interval 600
threshold poll cpu-memory-usage interval

Configures the polling interval over which to measure the percentage of total packet processing card CPU memory used.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold poll cpu-memory-usage interval duration

default threshold poll cpu-memory-usage interval

default
Uses the default threshold polling interval.
Default: 300 seconds

interval dur
Specifies the amount of time (in seconds) that comprises the polling interval.
duration must be an integer from 30 through 60000.

Usage

This command sets the time period over which to monitor the specified value for threshold crossing.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system’s support for thresholds in this chapter.

Important: To enable an SNMP trap for monitoring this threshold use the snmp trap enable ThreshCPUMemUsage command in this mode.

Example

The following command configures the polling interval to 600 seconds for the CPU memory usage threshold:

threshold poll cpu-memory-usage interval 600
threshold poll cpu-orbs-crit interval

Configures the polling interval over which to measure the percentage of CPU utilization by the ORBS software task for critical-level alerts.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration
`configure`

Entering the above command sequence results in the following prompt:

```
[local] host_name(config)#
```

**Syntax**

```
threshold poll cpu-orbs-crit interval duration
```

**default threshold poll cpu-orbs-crit interval**

```
default

Uses the default threshold polling interval.
Default: 300 seconds
```

```
interval dur

Specifies the amount of time (in seconds) that comprises the polling interval.
`duration` must be an integer from 60 through 60000.
```

**Usage**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the `threshold monitoring` and other threshold commands for additional information on the system’s support for thresholds in this chapter.

**Important:** To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshCPUOrbsCritical` command in this mode.

**Example**

The following command configures the polling interval to 600 seconds for the CPU ORBS critical threshold:

```
threshold poll cpu-orbs-crit interval 600
```
threshold poll cpu-orbs-warn interval

Configures the polling interval over which to measure the percentage of CPU utilization by the ORBS software task for warning-level alerts.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

```bash
configure
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config)#
```

**Syntax**

```bash
threshold poll cpu-orbs-warn interval duration
```

```bash
default threshold poll cpu-orbs-warn interval
```

`default`

Uses the default threshold polling interval.
Default: 300 seconds

```bash
interval dur
```

Specifies the amount of time (in seconds) that comprises the polling interval.
`duration` must be an integer from 60 through 60000.

**Usage**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the `threshold monitoring` and other threshold commands for additional information on the system’s support for thresholds in this chapter.

**Important:** To enable an SNMP trap for monitoring this threshold use the `snmp trap enable` `ThreshCPUOrbsWarn` command in this mode.

**Example**

The following command configures the polling interval to `600` seconds for the CPU ORBS warning threshold:
threshold poll cpu-orbs-warn interval 600
threshold poll cpu-session-throughput interval

Configures the polling interval over which to measure total throughput for all Session Manager tasks running on each packet processing card CPU.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold poll cpu-session-throughput interval duration

default threshold poll cpu-session-throughput interval

default

Uses the default threshold polling interval.
Default: 300 seconds

interval dur

Specifies the amount of time (in seconds) that comprises the polling interval.
duration must be an integer from 60 through 60000.

Usage

This command sets the time period over which to monitor the specified value for threshold crossing.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system’s support for thresholds in this chapter.

Important: To enable an SNMP trap for monitoring this threshold use the \texttt{snmp trap enable ThreshSessCPUThroughput} command in this mode.

Example

The following command configures the polling interval to 600 seconds for the CPU session throughput threshold:
threshold poll cpu-session-throughput interval

threshold poll cpu-session-throughput interval 600
**threshold poll cpu-utilization interval**

Configures the polling interval over which to measure the percentage of CPU utilization.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
threshold poll cpu-utilization interval duration

default threshold poll cpu-utilization interval
```

```
default
Uses the default threshold polling interval.
Default: 300 seconds
```

```
interval dur
Specifies the amount of time (in seconds) that comprises the polling interval.
duration must be an integer from 60 through 60000.
```

**Usage**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system’s support for thresholds in this chapter.

**Important:** To enable an SNMP trap for monitoring this threshold use the `snmp trap enable` ThreshCPUUtilization command in this mode.

**Example**

The following command configures the polling interval to 600 seconds for the CPU utilization threshold:

```
threshold poll cpu-utilization interval 600
```
threshold poll cscf-invite-rcvd interval

Configures the polling interval in seconds over which to count the invitations received for Call State Control Function (CSCF) calls.

**Product**

SCM

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

**Syntax**

threshold poll cscf-invite-rcvd interval duration

default threshold poll cscf-invite-rcvd interval

<table>
<thead>
<tr>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uses the default threshold polling interval. Default: 300 seconds</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>interval dur</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the amount of time (in seconds) that comprises the polling interval. duration must be an integer from 60 through 60000.</td>
</tr>
</tbody>
</table>

**Usage**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system’s support for thresholds in this chapter.

**Important:** To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshCSCFSvcCallsPerInterval` command in this mode.

**Example**

The following command configures the polling interval to 600 seconds for the CSCF call invite threshold:

```
threshold poll cscf-invite-rcvd interval 600
```
threshold poll cscf-reg-rcvd interval

Configures the polling interval in seconds over which to count the registrations received for Call State Control Function (CSCF) calls.

Product
SCM

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold poll cscf-reg-rcvd interval duration

default threshold poll cscf-reg-rcvd interval

default
Uses the default threshold polling interval.
Default: 300 seconds

interval dur
Specifies the amount of time (in seconds) that comprises the polling interval.
duration must be an integer from 60 through 60000.

Usage

This command sets the time period over which to monitor the specified value for threshold crossing.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system’s support for thresholds in this chapter.

Important: To enable an SNMP trap for monitoring this threshold use the snmp trap enable ThreshCSCFSvcRegPerInterval command in this mode.

Example

The following command configures the polling interval to 600 seconds for the CSCF call registrations threshold:
threshold poll cscf-reg-rcvd interval 600
threshold poll cscf-service-route-failures interval

Configures the polling interval in seconds over which to count the CSCF service route failures.

**Product**
SCM

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

**Syntax**

```
threshold poll cscf-service-route-failures interval duration
```

default threshold poll cscf-service-route-failures interval

**Usage**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system’s support for thresholds in this chapter.

**Important:** To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshCSCFSvcRouteFailures` command in this mode.

**Example**

The following command configures the polling interval to 600 seconds for the CSCF service route failures threshold:

```
threshold poll cscf-service-route-failures interval 600
```
threshold poll dcca-bad-answers interval

Configures the polling interval for DCCA Bad Answers threshold—invalid or bad response to the system from the Diameter server.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

**Syntax**

```plaintext
threshold poll dcca-bad-answers interval duration

default threshold poll dcca-bad-answers interval
```

- **default**
  
  Uses the default threshold polling interval.
  
  Default: 900 seconds

- **interval duration**
  
  Specifies the polling interval (in seconds) for the DCCA Bad Answers threshold.
  
  `duration` must be an integer from 60 through 60000.

**Usage**

This command configures the polling interval for DCCA Bad Answers threshold.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system’s support for thresholding in this chapter.

**Important:** To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshDCCABadAnswers` command in this mode.

**Example**

The following command configures the polling interval to **600** seconds for invalid or bad response threshold to the system from Diameter server:
threshold poll dcca-bad-answers interval

threshold poll dcca-rating-failed interval 600
threshold poll dcca-protocol-error interval

Configures the polling interval for Diameter Credit-Control Application (DCCA) Protocol Error threshold.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure
Entering the above command sequence results in the following prompt:

[local] host_name(config) #

Syntax

threshold poll dcca-protocol-error interval duration

default threshold poll dcca-protocol-error interval

- **default**
  - Uses the default threshold polling interval.
  - Default: 900 seconds

- **interval duration**
  - Specifies the polling interval (in seconds) for the DCCA Protocol Error threshold.
  - duration must be an integer from 60 through 60000.

Usage

Use this the polling interval for DCCA Protocol Error threshold.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system’s support for thresholding in this chapter.

**Important:** To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThresholdDCCAProtocolError` command in this mode.

Example

The following command configures the polling interval to 600 seconds for the DCCA protocol error threshold:

```
threshold poll dcca-protocol-error interval 600
```
threshold poll dccarating-failed interval

This command configures the polling interval for Diameter Credit-Control Application (DCCA) Rating Failed threshold.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

```
[local] host_name(config)#
```

**Syntax**

```
threshold poll dccarating-failed interval duration

default threshold poll dccarating-failed interval
```

**Usage**

This command configures the polling interval for DCCA Rating Failed threshold.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system’s support for thresholding in this chapter.

**Important:** To enable an SNMP trap for monitoring this threshold use the **snmp trap enable ThreshDCCARatingFailed** command in this mode.

**Example**

The following command configures the polling interval to **600 seconds** for the Diameter Credit Control Application (DCCA) Rating Group (content-id) request reject thresholds:

```
threshold poll dccarating-failed interval 600
```
threshold poll dcca-unknown-rating-group interval

Configures the polling interval for Diameter Credit-Control Application (DCCA) Unknown Rating Group threshold.

**Product**

ACS

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration

command

Entering the above command sequence results in the following prompt:

[local]host_name(config) #

**Syntax**

```
threshold poll dcca-unknown-rating-group interval duration
```

```
default threshold poll dcca-unknown-rating-group interval
```

```
default
```

Uses the default polling interval.
Default: 900 seconds

```
interval duration
```

Specifies the polling interval (in seconds) for the DCCA Unknown Rating Group threshold.

`duration` must be an integer from 60 through 60000.

**Usage**

This command configures the polling interval for DCCA Unknown Rating Group threshold.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the `threshold monitoring` and other threshold commands for additional information on the system’s support for thresholding in this chapter.

**Important:** To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshDCCAUnknownRatingGroup` command in this mode.

**Example**

The following command configures the polling interval to 600 seconds to threshold for the unknown DCCA Rating Group (content-id) returned by Diameter to system:

```
threshold poll dcca-unknown-rating-group interval 600
```
threshold poll dereg-reply-error interval

Configures the polling interval to count the number of de-registration reply errors per HA service.

**Product**
HA

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
threshold poll dereg-reply-error interval duration

default threshold poll dereg-reply-error interval
```

**default**

Uses the default polling interval.
Default: 300 seconds

```
interval duration
```

Specifies the amount of time (in seconds) that comprises the polling interval.
`duration` must be an integer from 60 through 60000. The input will be rounded up to the closest multiple of 30.

**Usage**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the `threshold monitoring` and other threshold commands in this chapter for additional information on the system’s support for thresholding.

**Important:** To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshHASvcDeregReplyError` command in this mode.

**Example**

The following command configures the HA de-registration reply error threshold polling interval to 600 seconds:

```
```
threshold poll dereg-reply-error interval 600
threshold poll diameter-retry-rate interval

Configures the polling interval for the Diameter Credit-Control Application (DCCA) Diameter Retry Rate threshold.

Usage
This command specifies the polling interval for Diameter Retry Rate threshold.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands in this chapter for additional information on the system’s support for thresholding.

Important: To enable an SNMP trap for monitoring this threshold use the **snmp trap enable** command in this mode.

Example
The following command configures the Diameter Retry Rate threshold polling interval to 600 seconds:

```
threshold poll diameter-retry-rate interval 600
```
threshold poll edr-file-space interval

Command configures the polling interval for Event Data Record (EDR) File Space Usage threshold.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

```
configure
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config) #
```

**Syntax**

```
threshold poll edr-file-space interval duration
```

### interval duration

Default: 300 seconds.

Specifies the polling interval (in seconds) for the EDR File Space Usage threshold.

*duration* must be an integer from 60 through 60000.

**Usage**

This command configures the polling interval for EDR File Space Usage threshold.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system’s support for thresholds in this chapter.

**Important:** To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshEDRFileSpace` command in this mode.

**Example**

The following command configures the polling interval to 600 seconds for the EDR file space usage threshold:

```
threshold poll edr-file-space interval 600
```
threshold poll edr-udr-dropped-flow-control interval

Configures the polling interval to count the total number of Event Data Records (EDRs) and Usage Data Records (UDRs) discarded due to ACSMGR flow control.

Product
ACS

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold poll edr-udr-dropped-flow-control interval duration

interval duration

Default: 300 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
duration must be an integer from 60 through 60000.

Usage

This command sets the time period over which to monitor the specified value for threshold crossing.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system’s support for thresholds in this chapter.

Example

The following command configures the polling interval to 600 seconds for the EDR/UDR drops due to flow control threshold:

threshold poll edr-udr-dropped-flow-control interval 600
threshold poll epdg-current-sessions interval

Configures the polling interval to count the total number of subscribers currently in Evolved Packet Date Gateway (ePDG) sessions.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration
configure
Entering the above command sequence results in the following prompt:

```
[local] host_name(config)#
```

**Syntax**

```
threshold poll epdg-current-sessions interval duration
```

**interval duration**

Default: 300 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
```
duration
```
must be an integer from 60 through 60000.

**Usage**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system’s support for thresholds in this chapter.

**Important:** To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThresholdEPDGCurrSess` command in this mode.

**Example**

The following command configures the polling interval to 600 seconds for the ePDG sessions threshold:

```
threshold poll epdg-current-sessions interval 600
```
threshold poll error-no-resource interval

Configures the polling interval in seconds over which to count CSCF No Resource Errors.

**Product**
SCM

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

```conf
configure
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
threshold poll error-no-resource interval duration
```

- `interval duration`
  - Default: 300 seconds.
  - Specifies the amount of time (in seconds) that comprises the polling interval.
  - `duration` must be an integer from 60 through 60000.

**Usage**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the `threshold monitoring` and other threshold commands for additional information on the system’s support for thresholds in this chapter.

**Important:** To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshCSCFSvcErrorNoResource` command in this mode.

**Example**

The following command configures the polling interval to 600 seconds for the CSCF No Resource Errors threshold:

```
threshold poll error-no-resource interval 600
```
threshold poll error-presence interval

Configures the polling interval in seconds over which to count CSCF Presence Errors.

**Product**
SCM

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config) #

**Syntax**

```
threshold poll error-presence interval duration
```

**Usage**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system’s support for thresholds in this chapter.

**Important:** To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshCSCFSvcErrorPresence` command in this mode.

**Example**

The following command configures the polling interval to 600 seconds for the CSCF Presence Errors threshold:

```
threshold poll error-presence interval 600
```
threshold poll error-reg-auth interval

Configures the polling interval in seconds over which to count CSCF Reg-Auth Errors.

Product
SCM

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold poll error-reg-auth interval duration

interval duration

Default: 300 seconds.

Specifies the amount of time (in seconds) that comprises the polling interval.

duration must be an integer from 60 through 60000.

Usage

This command sets the time period over which to monitor the specified value for threshold crossing.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system’s support for thresholds in this chapter.

Important: To enable an SNMP trap for monitoring this threshold use the snmp trap enable ThreshCSCFSvcErrorRegAuth command in this mode.

Example

The following command configures the polling interval to 600 seconds for the CSCF Reg-Auth Errors threshold:

threshold poll error-reg-auth interval 600
threshold poll error-tcp interval

Configures the polling interval in seconds over which to count CSCF TCP Errors.

Product
SCM

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration

configure
Entering the above command sequence results in the following prompt:

[local] host_name(config) #

Syntax

threshold poll error-tcp interval duration

interval duration
Default: 300 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
duration must be an integer from 60 through 60000.

Usage
This command sets the time period over which to monitor the specified value for threshold crossing.

⚠️ Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system’s support for thresholds in this chapter.

⚠️ Important: To enable an SNMP trap for monitoring this threshold use the snmp trap enable ThreshCSCFSvcErrorTcp command in this mode.

Example

The following command configures the polling interval to 600 seconds for the CSCF TCP Errors threshold:

threshold poll error-tcp interval 600
threshold poll fa-reg-reply-error interval

Configures the polling interval over which to measure the number of registration reply errors for Foreign Agent (FA) services.

Product
FA

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold poll fa-reg-reply-error interval duration

interval duration
Default: 0 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
duration must be an integer from 60 through 60000.

Usage

This command sets the time period over which to monitor the specified value for threshold crossing.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system’s support for thresholds in this chapter.

Important: To enable an SNMP trap for monitoring this threshold use the snmp trap enable ThreshFASvcRegReplyError command in this mode.

Example

The following command configures the polling interval to 600 seconds for the FA registration reply errors threshold:

threshold poll fa-reg-reply-error interval 600
threshold poll fng-current-active-sessions interval

Configures the polling interval in seconds over which to count Femto Network Gateway (FNG) current active sessions.

**Product**
FNG

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

*configure*

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
threshold poll fng-current-active-sessions interval duration
```

*interval duration*

Default: 0 seconds.

Specifies the amount of time (in seconds) that comprises the polling interval.

*duration* must be an integer from 60 through 60000.

**Usage**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system’s support for thresholds in this chapter.

**Important:** To enable an SNMP trap for monitoring this threshold use the *snmp trap enable ThreshFNGCurrActSess* command in this mode.

**Example**

The following command configures the polling interval to 600 seconds for the FNG current active sessions threshold:

```
threshold poll fng-current-active-sessions interval 600
```
threshold poll fng-current-sessions interval

Configures the polling interval in seconds over which to count Femto Network Gateway (FNG) current sessions, including inactive sessions.

**Product**
FNG

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
threshold poll fng-current-sessions interval duration
```

```
interval duration
```
Default: 0 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
duration must be an integer from 60 through 60000.

**Usage**
This command sets the time period over which to monitor the specified value for threshold crossing.

⚠️ **Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system’s support for thresholds in this chapter.

⚠️ **Important:** To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshFNGCurrSess` command in this mode.

**Example**
The following command configures the polling interval to 600 seconds for the FNG current sessions threshold:

```
threshold poll fng-current-sessions interval 600
```
threshold poll fw-deny-rule interval

Configures the Stateful Firewall Deny Rule threshold polling interval.

Product
PSF

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

`threshold poll fw-deny-rule interval duration`

`interval duration`

Default: 900 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
`duration` must be an integer from 60 through 900.

Usage
This command sets the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the `threshold monitoring` and other threshold commands for additional information on the system’s support for thresholds in this chapter.

**Important:** To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshFWDenyRule` command in this mode.

Example
The following command configures the polling interval to 600 seconds for the Stateful Firewall Deny Rule threshold:

`threshold poll fw-deny-rule interval 600`
threshold poll fw-dos-attack interval

Configures the Stateful Firewall Denial of Service (DoS) Attacks threshold polling interval.

Product
PSF

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold poll fw-dos-attack interval duration

- interval duration
  Default: 900 seconds.
  Specifies the amount of time (in seconds) that comprises the polling interval.
  duration must be an integer from 60 through 900.

Usage

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system’s support for thresholds in this chapter.

**Important:** To enable an SNMP trap for monitoring this threshold use the snmp trap enable ThreshFWDosAttack command in this mode.

Example

The following command configures the polling interval to 600 seconds for the Stateful Firewall DoS Attacks threshold:

threshold poll fw-dos-attack interval 600
threshold poll fw-drop-packet interval

Configures the Stateful Firewall Drop-Packet threshold polling interval.

**Product**
PSF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local]host_name(config) #

**Syntax**

```
threshold poll fw-drop-packet interval duration
```

---

**Usage**

This command sets the time period over which to monitor the specified value for threshold crossing.

---

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system’s support for thresholds in this chapter.

---

**Important:** To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshFWDropPacket` command in this mode.

**Example**

The following command configures the polling interval to 600 seconds for the Stateful Firewall Drop-Packet threshold:

```
threshold poll fw-drop-packet interval 600
```
threshold poll fw-no-rule interval

Configures the Stateful Firewall No-Rule threshold polling interval.

**Product**
PSF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

```console
configure
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
threshold poll fw-no-rule interval duration
```

- `interval duration`
  - Default: 900 seconds.
  - Specifies the amount of time (in seconds) that comprises the polling interval.
  - `duration` must be an integer from 60 through 900.

**Usage**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system’s support for thresholds in this chapter.

**Important:** To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshFWNoRule` command in this mode.

**Example**

The following command configures the polling interval to 600 seconds for the Stateful Firewall No-Rule threshold:

```
threshold poll fw-no-rule interval 600
```
threshold poll ha-init-rrq-rcvd-rate interval

Configures the polling interval for Home Agent (HA) service over which to measure the average number of calls setup per minute.

**Product**
HA

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local] host_name(config) #

**Syntax**

```plaintext
threshold poll ha-init-rrq-rcvd-rate interval duration
```

**interval duration**
Default: 0 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
`duration` must be an integer from 60 through 900.

**Usage**
This command sets the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the `threshold monitoring` and other threshold commands for additional information on the system’s support for thresholds in this chapter.

**Important:** To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshHACallSetupRate` command in this mode.

**Example**
The following command configures the polling interval to 600 seconds for the average number of HA calls setup per minute:

```plaintext
threshold poll ha-init-rrq-rcvd-rate interval 600
```
Global Configuration Mode Commands (threshold poll commands A - N)

threshold poll ha-svc-init-rrq-rcvd-rate interval

Configures the polling interval over which to measure the average number of calls setup per minute for HA services.

Product
HA

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold poll ha-svc-init-rrq-rcvd-rate interval duration

interval duration
Default: 0 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
duration must be an integer from 60 through 900.

Usage
This command sets the time period over which to monitor the specified value for threshold crossing.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system’s support for thresholds in this chapter.

Important: To enable an SNMP trap for monitoring this threshold use the snmp trap enable ThreshHASvcCallSetupRate command in this mode.

Example

The following command configures the polling interval to 600 seconds for the average number of calls setup per minute for HA services:

threshold poll ha-svc-init-rrq-rcvd-rate interval 600
**threshold poll henbgw-paging-messages interval**

Configures how frequently the HeNB-GW paging messages are polled.

**Product**
HeNB-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

    configure

Entering the above command sequence results in the following prompt:

    [local]host_name(config)#

**Syntax**

```plaintext
threshold poll henbgw-paging-messages interval duration
```

**Usage**

This command configures how frequently the HeNB-GW paging messages are polled.

**Important:**
All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system’s support for thresholds in this chapter.

**Important:**
To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshHeNBGW PagingMessages` command in this mode.

**Example**

The following command configures the polling interval to **6000** seconds for the HeNB-GW service:

```plaintext
threshold poll henbgw-paging-messages interval 6000
```
threshold poll ip-pool-free interval

Configures the polling interval over which to measure the percentage of the IP pool addresses that are in the Free state.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

`configure`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
threshold poll ip-pool-free interval duration
```

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>threshold poll ip-pool-free interval duration</td>
<td>Specifies the amount of time (in seconds) that comprises the polling interval. duration must be an integer from 30 through 60000.</td>
</tr>
</tbody>
</table>

**Usage**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system’s support for thresholds in this chapter.

**Important:** To enable an SNMP trap for monitoring this threshold use the `snmp trap enable` ThreshIPPoolFree command in this mode.

**Example**

The following command configures the polling interval to 600 seconds for the average number of Free IP pools:

```
threshold poll ip-pool-free interval interval 600
```
threshold poll ip-pool-hold interval

Configures the polling interval over which to measure the percentage of the IP pool addresses that are in the Hold state.

**Product**  
All

**Privilege**  
Security Administrator, Administrator

**Mode**  
Exec > Global Configuration  
configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
threshold poll ip-pool-hold interval duration
```

<table>
<thead>
<tr>
<th>Syntax</th>
<th>interval duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>duration</td>
<td>Must be an integer from 30 through 60000.</td>
</tr>
</tbody>
</table>

**Usage**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system’s support for thresholds in this chapter.

**Important:** To enable an SNMP trap for monitoring this threshold use the **snmp trap enable** ThreshIPPoolHold command in this mode.

**Example**

The following command configures the polling interval to 600 seconds for the average number of IP pool addresses in Hold state:

```
threshold poll ip-pool-hold interval 600
```
threshold poll ip-pool-release interval

Configures the polling interval over which to measure the percentage of IP pool addresses that are in the Release state.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

```
configure
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
threshold poll ip-pool-release interval duration
```

**interval duration**

Default: 300 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
`duration` must be an integer from 30 through 60000.

**Usage**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system’s support for thresholds in this chapter.

**Important:** To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshIPPoolRelease` command in this mode.

**Example**

The following command configures the polling interval to 600 seconds for the average number of IP pool addresses in Release state:

```
threshold poll ip-pool-release interval 600
```
threshold poll ip-pool-used interval

Configures the polling interval over which to measure the percentage of the IP pool addresses that are used.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

`configure`
Entering the above command sequence results in the following prompt:

```
[local] host_name(config)#
```

**Syntax**

```
threshold poll ip-pool-used interval duration
```

**interval duration**
Default: 300 seconds. Specifies the amount of time (in seconds) that comprises the polling interval. `duration` must be an integer from 30 through 60000.

**Usage**
This command sets the time period over which to monitor the specified value for threshold crossing.

⚠️ **Important**: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system’s support for thresholds in this chapter.

⚠️ **Important**: To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshIPPoolUsed` command in this mode.

**Example**
The following command configures the polling interval to 600 seconds for the average number of used IP pool addresses:

```
threshold poll ip-pool-used interval 600
```
threshold poll ipsec-call-req-rej interval

Configures the polling interval over which to count the IPSec call requests that are rejected.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
threshold poll ipsec-call-req-rej interval duration
```

- `interval duration`
  - Default: 900 seconds.
  - Specifies the amount of time (in seconds) that comprises the polling interval.
  - `duration` must be an integer from 30 through 60000.

**Usage**
This command sets the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system’s support for thresholds in this chapter.

**Important:** To enable an SNMP trap for monitoring this threshold use the **snmp trap enable ThreshIPSECCallReqRej** command in this mode.

**Example**

The following command configures the polling interval to 600 seconds for the average number of rejected IPSec IKE calls:

```
threshold poll ipsec-call-req-rej interval 600
```
threshold poll ipsec-ike-failrate interval

Configures the polling interval over which to count the IPSec IKE failure rate.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold poll ipsec-ike-failrate interval duration

interval duration
Default: 900 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.

duration must be an integer from 30 through 60000.

Usage
This command sets the time period over which to monitor the specified value for threshold crossing.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system’s support for thresholds in this chapter.

Important: To enable an SNMP trap for monitoring this threshold use the snmp trap enable ThreshIPSECIKEFailRate command in this mode.

Example
The following command configures the polling interval to 600 seconds for the average rate for IPSec IKE failures:

threshold poll ipsec-ike-failrate interval 600
threshold poll ipsec-ike-failures interval

Configures the polling interval over which to count the number of IPSec IKE failures.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

```
threshold poll ipsec-ike-failures interval duration
```

```
interval duration
Default: 900 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
duration must be an integer from 30 through 60000.
```

Usage

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system’s support for thresholds in this chapter.

**Important:** To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshIPSECIKEFailures` command in this mode.

Example

The following command configures the polling interval to 600 seconds for the average number of IPSec IKE failures:

```
threshold poll ipsec-ike-failures interval 600
```
threshold poll ipsec-ike-requests interval

Configures the polling interval over which to count the number of IPSec IKE requests.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration

configure
Entering the above command sequence results in the following prompt:

[local] host_name(config) #

Syntax

threshold poll ipsec-ike-requests interval duration

interval duration

Default: 900 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
duration must be an integer from 30 through 60000.

Usage
This command sets the time period over which to monitor the specified value for threshold crossing.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system’s support for thresholds in this chapter.

Important: To enable an SNMP trap for monitoring this threshold use the snmp trap enable ThreshIPSECIKERequests command in this mode.

Example

The following command configures the polling interval to 600 seconds for the average number of IPSec call requests:

threshold poll ipsec-ike-requests interval 600
threshold poll ipsec-tunnels-established interval

Configures the polling interval over which to count the number of IPSec tunnels that have been established.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold poll ipsec-tunnels-established interval duration

interval duration

Default: 900 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
duration must be an integer from 30 through 60000.

Usage

This command sets the time period over which to monitor the specified value for threshold crossing.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system’s support for thresholds in this chapter.

Important: To enable an SNMP trap for monitoring this threshold use the snmp trap enable ThreshIPSECTunEstab1 command in this mode.

Example

The following command configures the polling interval to 600 seconds for the number of established IPSec tunnels:

threshold poll ipsec-tunnels-established interval 600
threshold poll ipsec-tunnels-setup interval

Configures the polling interval over which to count the number of IPSec tunnels that have been setup.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config) #

Syntax

```
threshold poll ipsec-tunnels-setup interval duration
```

- **interval**
  - duration: Specifies the amount of time (in seconds) that comprises the polling interval.
  - **duration** must be an integer from 30 through 60000.

Usage

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system’s support for thresholds in this chapter.

**Important:** To enable an SNMP trap for monitoring this threshold use the `snmp trap enable` ThreshIPSECTunSetup command in this mode.

Example

The following command configures the polling interval to 600 seconds for the number of IPSec tunnels that have been setup:

```
threshold poll ipsec-tunnels-setup interval 600
```
threshold poll license-remaining-session interval

Configures the polling interval over which to measure session license utilization.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
threshold poll license-remaining-session interval  duration
```

```
interval duration
Default: 900 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
duration must be an integer from 30 through 60000.
```

**Usage**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system’s support for thresholds in this chapter.

**Important:** To enable an SNMP trap for monitoring this threshold use the **snmp trap enable ThreshLicense** command in this mode.

**Example**

The following command configures the polling interval to 600 seconds for the utilization of session licenses:

```
threshold poll license-remaining-session interval 600
```
threshold poll mgmt-cpu-memory-usage interval

Configures the polling interval over which to measure management card CPU memory usage.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold poll mgmt-cpu-memory-usage interval duration

interval duration
Default: 300 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
duration must be an integer from 30 through 60000.

Usage
This command sets the time period over which to monitor the specified value for threshold crossing.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system’s support for thresholds in this chapter.

Example
The following command configures the polling interval to 600 seconds for management card CPU memory usage:

threshold poll mgmt-cpu-memory-usage interval 600
threshold poll mgmt-cpu-utilization interval

Configures the polling interval over which to measure management card CPU utilization.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
threshold poll mgmt-cpu-utilization interval duration
```

**interval duration**

Default: 300 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
*duration* must be an integer from 30 through 60000.

**Usage**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the *threshold monitoring* and other threshold commands for additional information on the system’s support for thresholds in this chapter.

**Example**

The following command configures the polling interval to 600 seconds for management card CPU memory usage:

```
threshold poll mgmt-cpu-utilization interval 600
```
threshold poll mme-attach-failure interval

Configures the polling interval to count the MME Attach Failure messages across all MME services in the system.

Product
MME

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure
Entering the above command sequence results in the following prompt:

[local] host_name(config) #

Syntax

threshold poll mme-attach-failure interval dur

default threshold poll mme-attach-failure interval

default
Restores the polling interval value to its default value of 900 seconds.

interval dur
Default: 900 seconds.
Specifies the polling interval (in seconds) for counting MME Attach Failure messages across all MME services in the system.
dur must be an integer from 30 through 60000 in multiples of 30.

Usage
Use this command to configure the polling interval to count the MME Attach Failure messages across all MME services in the system to generate threshold value.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring mme-service and other threshold commands for additional information on the system’s support for thresholds in this chapter.

Important: To enable an SNMP trap for monitoring this threshold use the snmp trap enable ThreshMMEAttachFail command in this mode.

Example

The following command configures the polling interval of 600 seconds to count the MME Attach Failure messages for threshold limit:
threshold poll mme-attach-failure interval 600
threshold poll mme-auth-failure interval

Configures the polling interval to count the MME Authentication Failure messages across all MME services in the system.

Product
MME

Privilege
Security Administrator, Administrator

Mode
 Exec > Global Configuration
 configure

Entering the above command sequence results in the following prompt:

[local]host_name(config) #

Syntax

threshold poll mme-auth-failure interval dur

default threshold poll mme-auth-failure interval

default
Restores the specified poll interval value to its default value of 900 seconds.

interval dur
Default: 900 seconds.
Specifies the polling interval (in seconds) for counting MME Authentication Failure messages across all MME services in the system.
dur must be an integer from 30 through 60000 in multiples of 30.

Usage
Use this command to configure the polling interval to count the MME Auth Failure messages across all MME services in the system to generate threshold value.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring mme-service and other threshold commands for additional information on the system’s support for thresholds in this chapter.

Important: To enable an SNMP trap for monitoring this threshold use the snmp trap enable ThreshMMEAuthFail command in this mode.

Example
The following command configures the polling interval of 600 seconds to count the MME Auth Failure messages for threshold limit:

```
threshold poll mme-auth-failure interval 600
```
threshold poll nat-port-chunks-usage interval

Configures the polling interval over which to measure the percentage of Network Address Translation (NAT) port chunk utilization.

**Product**
NAT

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration
```
configure
```
Entering the above command sequence results in the following prompt:
```
[local] host_name(config) #
```

**Syntax**

```
threshold poll nat-port-chunks-usage interval duration
```

```
default threshold poll nat-port-chunks-usage interval
```

```
default
```
Restores the specified poll interval value to its default value of 900 seconds.

```
interval duration
```
Specifies the amount of time (in seconds) that comprises the polling interval.
```
duration must be an integer from 30 through 60000.
```
Default: 900 seconds.

**Usage**
This command sets the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system’s support for thresholds in this chapter.

**Important:** To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshNATPortChunksUsage` command in this mode.

**Example**
The following command configures the polling interval to 600 seconds for (NAT) port chunk utilization:
```
threshold poll nat-port-chunks-usage interval 600
```
threshold poll npu-utilization interval

Configures the polling interval over which to measure the percentage of network processing unit (NPU) utilization.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration

`configure`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
threshold poll npu-utilization interval duration
```

**Usage**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the `threshold monitoring` and other threshold commands for additional information on the system’s support for thresholds in this chapter.

**Important:** To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshNPUUtilization` command in this mode.

**Example**

The following command configures the polling interval to **600** seconds for NPU utilization:

```
threshold poll npu-utilization interval 600
```
Chapter 144
Global Configuration Mode Commands (threshold poll commands O - Z)

This section includes the commands `threshold poll packets-filtered-dropped interval` through `threshold poll tpo-rto-timeout`.

The Global Configuration Mode is used to configure basic system-wide parameters.

**Mode**

`Exec > Global Configuration`

`configure`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config) #
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
threshold poll packets-filtered-dropped interval

Configures the polling interval over which to count the filtered/dropped packets.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration
`configure`

Entering the above command sequence results in the following prompt:

```
[local] host_name(config) #
```

**Syntax**

```
threshold poll packets-filtered-dropped interval duration
```

**Usage**
This command sets the time period over which to monitor the specified value for threshold crossing.

---
**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system’s support for thresholds in this chapter.

---
**Important:** To enable an SNMP trap for monitoring this threshold use the `snmp trap enable` ThreshPacketsFilteredDropped command in this mode.

**Example**
The following command configures the polling interval to 600 seconds for filtered/dropped packets:

```
threshold poll packets-filtered-dropped interval 600
```
threshold poll packets-forwarded-to-cpu interval

Configures the polling interval over which to count packets forwarded to active system CPUs in the system.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold poll packets-forwarded-to-cpu interval duration

interval duration
Default: 300 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
duration must be an integer from 30 through 60000.

Usage
This command sets the time period over which to monitor the specified value for threshold crossing.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system’s support for thresholds in this chapter.

Important: To enable an SNMP trap for monitoring this threshold use the snmp trap enable ThreshPacketsForwarded command in this mode.

Example
The following command configures the polling interval to 600 seconds for packets forwarded to active system CPUs in the system:

threshold poll packets-forwarded-to-cpu interval 600
threshold poll pdg-current-active-sessions interval

Configures the polling interval over which to count the total number of currently active Packet Data Gateway/Tunnel Termination Gateway (PDG/TTG) sessions.

Product
PDG
TTG

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local] host_name(config)#

Syntax

threshold poll pdg-current-active-sessions interval duration

interval duration
Default: 300 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
duration must be an integer from 30 through 60000.

Usage
This command sets the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system’s support for thresholds in this chapter.

**Important:** To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThresholdPDGCCurrActSess` command in this mode.

Example

The following command configures the polling interval to 600 seconds for PDG/TTG sessions:

```
threshold poll pdg-current-active-sessions interval 600
```
threshold poll pdg-current-sessions interval

Configures the polling interval over which to count the total number of current Packet Data Gateway/Tunnel Termination Gateway (PDG/TTG) sessions, including inactive sessions.

Product

PDG/TTG

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold poll pdg-current-sessions interval duration

interval duration

Default: 300 seconds.

Specifies the amount of time (in seconds) that comprises the polling interval.

duration must be an integer from 30 through 60000.

Usage

This command sets the time period over which to monitor the specified value for threshold crossing.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system’s support for thresholds in this chapter.

Important: To enable an SNMP trap for monitoring this threshold use the snmp trap enable ThreshPDGCurrSess command in this mode.

Example

The following command configures the polling interval to 600 seconds for PDG/TTG sessions:

threshold poll pdg-current-sessions interval 600
threshold poll pdif-current-active-sessions interval

Configures the polling interval over which to count the total number of currently active Packet Data Interworking Function (PDIF) sessions.

**Product**
PDIF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

```
configure
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config) #
```

**Syntax**

```
threshold poll pdif-current-active-sessions interval duration
```

**interval duration**

Default: 300 seconds.

Specifies the amount of time (in seconds) that comprises the polling interval.

*duration* must be an integer from 30 through 60000.

**Usage**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system’s support for thresholds in this chapter.

**Important:** To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshPDIFCurrActSess` command in this mode.

**Example**

The following command configures the polling interval to 600 seconds for PDIF sessions:

```
threshold poll pdif-current-active-sessions interval 600
```
threshold poll pdif-current-sessions interval

Configures the polling interval over which to count the total number of current Packet Data Interworking Function (PDIF) sessions, including inactive sessions.

Product
PDIF

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold poll pdif-current-sessions interval duration

interval duration
Default: 300 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
duration must be an integer from 30 through 60000.

Usage
This command sets the time period over which to monitor the specified value for threshold crossing.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system's support for thresholds in this chapter.

Important: To enable an SNMP trap for monitoring this threshold use the snmp trap enable ThreshPDIFCurrSess command in this mode.

Example

The following command configures the polling interval to 600 seconds for PDIF sessions:

threshold poll pdif-current-sessions interval 600
threshold poll pdsn-init-rrq-rcvd-rate interval

Configures the polling interval over which to count the total number of current Packet Data Serving Node (PDSN) sessions, including inactive sessions.

Product
PDSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config) #

Syntax

threshold poll pdsn-init-rrq-rcvd-rate interval duration

  interval duration

Default: 0 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
duration must be an integer from 60 through 60000.

Usage

This command sets the time period over which to monitor the specified value for threshold crossing.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system’s support for thresholds in this chapter.

Important: To enable an SNMP trap for monitoring this threshold use the snmp trap enable ThreshPDSNCallSetupRate command in this mode.

Example

The following command configures the polling interval to 600 seconds for PDSN sessions:

    threshold poll pdsn-init-rrq-rcvd-rate interval 600
threshold poll pdsn-svc-init-rrq-rcvd-rate interval

Configures the polling interval over which to count the total number of current Packet Data Serving Node (PDSN) sessions, including inactive sessions.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
threshold poll pdsn-svc-init-rrq-rcvd-rate interval duration
```

- `interval duration`
  - Default: 300 seconds.
  - Specifies the amount of time (in seconds) that comprises the polling interval.
  - `duration` must be an integer from 30 through 60000.

**Usage**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system’s support for thresholds in this chapter.

**Important:** To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshPDSNSvcCallSetupRate` command in this mode.

**Example**

The following command configures the polling interval to 600 seconds for PDSN sessions:

```
threshold poll pdsn-svc-init-rrq-rcvd-rate interval 600
```
threshold poll per-service-asngw-sessions interval

Configures the polling interval in seconds over which to count the number of PDP contexts per ASN-GW service in the system.

Product
ASN-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold poll per-service-asngw-sessions interval duration

interval duration

Default: 300 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
duration must be an integer from 30 through 60000.

Usage

This command sets the time period over which to monitor the specified value for threshold crossing.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system’s support for thresholds in this chapter.

Important: To enable an SNMP trap for monitoring this threshold use the snmp trap enable ThreshPerServiceASNGWSessions command in this mode.

Example

The following command configures the polling interval to 600 seconds for ASN-GW sessions:

    threshold poll per-service-asngw-sessions interval 600
threshold poll per-service-ggsn-sessions interval

Configures the polling interval in seconds over which to count the number of PDP contexts per GGSN service in the system.

Product: GGSN

Privilege: Security Administrator, Administrator

Mode: Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax:

threshold poll per-service-ggsn-sessions interval duration

- interval duration

Default: 300 seconds.

Specifies the amount of time (in seconds) that comprises the polling interval. duration must be an integer from 30 through 60000.

Usage:

This command sets the time period over which to monitor the specified value for threshold crossing.

⚠️ Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system’s support for thresholds in this chapter.

⚠️ Important: To enable an SNMP trap for monitoring this threshold use the snmp trap enable ThreshPerServiceGGSNSessions command in this mode.

Example:

The following command configures the polling interval to 600 seconds for GGSN sessions:

threshold poll per-service-ggsn-sessions interval 600
threshold poll per-service-gprs-pdp-sessions interval

Configures the polling interval in seconds over which to count the number of 2G-activated PDP contexts per GPRS service.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

```
[local] host_name(config)#
```

**Syntax**

```
threshold poll per-service-gprs-pdp-sessions interval duration
```

`interval duration`

Default: 300 seconds.

Specifies the amount of time (in seconds) that comprises the polling interval.
`duration` must be an integer from 30 through 60000.

**Usage**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system’s support for thresholds in this chapter.

**Important:** To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshPerServiceGPRSPDPSessions` command in this mode.

**Example**

The following command configures the polling interval to 600 seconds for 2G PDP contexts:

```
threshold poll per-service-gprs-pdp-sessions interval 600
```
threshold poll per-service-gprs-sessions interval

Configures the polling interval in seconds over which to count the number of 2G-attached subscribers per GPRS service.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
threshold poll per-service-gprs-sessions interval duration
```

```
interval duration
```

Default: 300 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
```
duration must be an integer from 30 through 60000.
```

**Usage**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system’s support for thresholds in this chapter.

**Important:** To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshPerServiceGPRSSessions` command in this mode.

**Example**

The following command configures the polling interval to 600 seconds for 2G GPRS sessions:

```
threshold poll per-service-gprs-sessions interval 600
```
threshold poll per-service-ha-sessions interval

Configures the polling interval in seconds over which to count the number of HA sessions per Home Agent (HA) service in the system.

Product
HA

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local] host_name (config) #

Syntax

threshold poll per-service-ha-sessions interval duration

interval duration

Default: 300 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
duration must be an integer from 30 through 60000.

Usage

This command sets the time period over which to monitor the specified value for threshold crossing.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system’s support for thresholds in this chapter.

Important: To enable an SNMP trap for monitoring this threshold use the snmp trap enable ThreshPerServiceHASSessions command in this mode.

Example

The following command configures the polling interval to 600 seconds for HA sessions:

threshold poll per-service-ha-sessions interval 600
threshold poll per-service-Ins-sessions interval

Configures the polling interval in seconds over which to count the number of L2TP Network Server (LNS) sessions per LNS service in the system.

Product: LNS
Privilege: Security Administrator, Administrator
Mode: Exec > Global Configuration configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold poll per-service-Ins-sessions interval duration

interval duration
Default: 300 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval. duration must be an integer from 30 through 60000.

Usage

This command sets the time period over which to monitor the specified value for threshold crossing.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system’s support for thresholds in this chapter.

Important: To enable an SNMP trap for monitoring this threshold use the snmp trap enable ThreshPerServiceLNSSessions command in this mode.

Example

The following command configures the polling interval to 600 seconds for LNS sessions:

threshold poll per-service-Ins-sessions interval 600
threshold poll per-service-pdg-sessions interval

Configures the polling interval in seconds over which to count the number of Packet Data Gateway (PDG) sessions per PDG/TTG service in the system.

Product
PDG/TTG

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

```
threshold poll per-service-pdg-sessions interval duration
```

```
interval duration
Default: 300 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
duration must be an integer from 30 through 60000.
```

Usage

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system’s support for thresholds in this chapter.

**Important:** To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThresholdPerServicePDGSessions` command in this mode.

Example

The following command configures the polling interval to 600 seconds for PDG/TTG sessions:

```
threshold poll per-service-pdg-sessions interval 600
```
threshold poll per-service-pdsn-sessions interval

Configures the polling interval in seconds over which to count the number of Packet Data Serving Node (PDSN) sessions per PDSN service in the system.

**Product**

PDSN

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
threshold poll per-service-pdsn-sessions interval duration
```

**interval** duration

Default: 300 seconds.

Specifies the amount of time (in seconds) that comprises the polling interval.

*duration* must be an integer from 30 through 60000.

**Usage**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system’s support for thresholds in this chapter.

**Important:** To enable an SNMP trap for monitoring this threshold use the **snmp trap enable ThreshPerServicePDNSessions** command in this mode.

**Example**

The following command configures the polling interval to *600* seconds for PDSN sessions:

```
threshold poll per-service-pdsn-sessions interval 600
```
threshold poll per-service-sgsn-pdp-sessions interval

Configures the polling interval in seconds over which to count the number of 3G-activated PDP contexts per SGSN service on the system.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
threshold poll per-service-sgsn-pdp-sessions interval duration
```

*interval duration*

Default: 300 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
*duration* must be an integer from 30 through 60000.

**Usage**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system’s support for thresholds in this chapter.

**Important:** To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshPerServiceSGSNPDPSessions` command in this mode.

**Example**

The following command configures the polling interval to 600 seconds for 3G PDP contexts:

```
threshold poll per-service-sgsn-pdp-sessions interval 600
```
threshold poll per-service-sgsn-sessions interval

Configures the polling interval in seconds over which to count the number of 3G-attached subscribers per SGSN service in the system.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

**Syntax**

```
threshold poll per-service-sgsn-sessions interval duration
```

**interval duration**
Default: 300 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
`duration` must be an integer from 30 through 60000.

**Usage**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the `threshold monitoring` and other threshold commands for additional information on the system’s support for thresholds in this chapter.

**Important:** To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshPerServiceSGSNSessions` command in this mode.

**Example**

The following command configures the polling interval to 600 seconds for SGSN sessions:

```
threshold poll per-service-sgsn-sessions interval 600
```
threshold poll phsgw-auth-failure interval

Configures the polling interval in seconds over which to count the number of Personal Handyphone System Gateway (PHSGW) authentication failures.

**Product**
PHSGW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

```
[local] host_name(config) #
```

**Syntax**

```
threshold poll phsgw-auth-failure interval duration
```

- **interval duration**
  - Default: 0 seconds.
  - Specifies the amount of time (in seconds) that comprises the polling interval.
  - `duration` must be an integer from 30 through 60000.

**Usage**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system’s support for thresholds in this chapter.

**Important:** To enable an SNMP trap for monitoring this threshold use the `snmp trap enable` `ThreshPHSGWAuthFail` command in this mode.

**Example**

The following command configures the polling interval to 600 seconds for PHSGW authentication failures:

```
threshold poll phsgw-auth-failure interval 600
```
threshold poll phsgw-eapol-auth-failure interval

Configures the polling interval in seconds over which to count the number of authentication failures for a PHSGW service using Extensible Authentication Protocol Over LAN (EAPOL).

Product
PHSGW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold poll phsgw-eapol-auth-failure interval duration

interval duration
Default: 0 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
duration must be an integer from 30 through 60000.

Usage
This command sets the time period over which to monitor the specified value for threshold crossing.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system’s support for thresholds in this chapter.

Important: To enable an SNMP trap for monitoring this threshold use the snmp trap enable ThreshPHSGWEAPOLAuthFailure command in this mode.

Example
The following command configures the polling interval to 600 seconds for PHSGW EAPOL failures:

threshold poll phsgw-eapol-auth-failure interval 600
threshold poll phsgw-handoff-denial interval

Configures the polling interval in seconds over which to count the number of handoff denials in PHSGW.

Product
PHSGW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:
[local] host_name(config) #

Syntax

```
threshold poll phsgw-handoff-denial interval duration

interval duration
Default: 0 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
duration must be an integer from 30 through 60000.
```

Usage
This command sets the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system’s support for thresholds in this chapter.

**Important:** To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshPHSGWMaxEAPOLRetry` command in this mode.

Example

The following command configures the polling interval to 600 seconds for PHSGW handoff denials:

```
threshold poll phsgw-handoff-denial interval 600
```
threshold poll phsgw-max-eap-retry interval

Configures the polling interval in seconds over which to count the maximum number of Extensible Authentication Protocol (EAP) retries in PHSGW.

**Product**
PHSGW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

**Syntax**

```
threshold poll phsgw-max-eap-retry interval duration
```

*interval duration*

Default: 0 seconds.

Specifies the amount of time (in seconds) that comprises the polling interval.

*duration* must be an integer from 30 through 60000.

**Usage**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system’s support for thresholds in this chapter.

**Important:** To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshPHSGWMaxEAPRetry` command in this mode.

**Example**

The following command configures the polling interval to 600 seconds for PHSGW EAP retries:

```
threshold poll phsgw-max-eap-retry interval 600
```
threshold poll phsgw-max-eapol-retry interval

Configures the polling interval in seconds over which to count the maximum number of Extensible Authentication Protocol Over LAN (EAPOL) retries in PHSGW.

Product
PHSGW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local] host_name(config) #

Syntax

threshold poll phsgw-max-eapol-retry interval duration

interval duration
Default: 0 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
duration must be an integer from 30 through 60000.

Usage
This command sets the time period over which to monitor the specified value for threshold crossing.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system’s support for thresholds in this chapter.

Important: To enable an SNMP trap for monitoring this threshold use the snmp trap enable ThreshPHSGWMaxEAPOLRetry command in this mode.

Example
The following command configures the polling interval to 600 seconds for PHSGW EAPOL retries:

threshold poll phsgw-max-eapol-retry interval 600
threshold poll phsgw-network-entry-denial interval

Configures the polling interval in seconds over which to count the number of network entry denials in PHSGW.

**Product**
PHSGW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
threshold poll phsgw-network-entry-denial interval duration
```

- **interval duration**
  - Default: 0 seconds.
  - Specifies the amount of time (in seconds) that comprises the polling interval.
  - *duration* must be an integer from 30 through 60000.

**Usage**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system’s support for thresholds in this chapter.

**Important:** To enable an SNMP trap for monitoring this threshold use the **snmp trap enable ThreshPHSGWNWEntryDenial** command in this mode.

**Example**

The following command configures the polling interval to *600* seconds for PHSGW network entry denials:

```
threshold poll phsgw-network-entry-denial interval 600
```
threshold poll phsgw-session-setup-timeout interval

Configures the polling interval in seconds over which to count the number of PHSGW sessions that timed out during setup.

**Product**
PHSGW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

*configure*

Entering the above command sequence results in the following prompt:

```
[local] host_name(config) #
```

**Syntax**

```
threshold poll phsgw-session-setup-timeout interval duration
```

**interval duration**

Default: 0 seconds.

Specifies the amount of time (in seconds) that comprises the polling interval.

*duration* must be an integer from 30 through 60000.

**Usage**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system’s support for thresholds in this chapter.

**Important:** To enable an SNMP trap for monitoring this threshold use the *snmp trap enable ThreshPHSGWSessSetupTimeout* command in this mode.

**Example**

The following command configures the polling interval to 600 seconds for PHSGW session setup timeouts:

```
threshold poll phsgw-session-setup-timeout interval 600
```
threshold poll phsgw-session-timeout interval

Configures the polling interval in seconds over which to count the number of PHSGW sessions that timed out.

**Product**
PHSGW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

```
configure
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
threshold poll phsgw-session-timeout interval duration
```

```
interval duration
```

Default: 0 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
`duration` must be an integer from 30 through 60000.

**Usage**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system’s support for thresholds in this chapter.

**Important:** To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshPHSGWSessTimeout` command in this mode.

**Example**

The following command configures the polling interval to 600 seconds for PHSGW session timeouts:

```
threshold poll phsgw-session-timeout interval 600
```
threshold poll phspc-session-setup-timeout interval

Configures the polling interval in seconds over which to count the number of Personal Handyphone System - Personal Computer (PHSPC) sessions that timed out during setup.

**Product**
PHSGW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

```
configure
```

Entering the above command sequence results in the following prompt:

```
[local] host_name (config) #
```

**Syntax**

```
threshold poll phspc-session-setup-timeout interval duration
```

*interval duration*

Default: 0 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
duration must be an integer from 30 through 60000.

**Usage**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system’s support for thresholds in this chapter.

**Important:** To enable an SNMP trap for monitoring this threshold use the **snmp trap enable ThreshPHSPCSessionSetupTimeout** command in this mode.

**Example**

The following command configures the polling interval to 600 seconds for PHSPC session setup timeouts:

```
threshold poll phspc-session-setup-timeout interval 600
```
threshold poll phspc-sleep-mode-timeout interval

Configures the polling interval in seconds over which to count the number of PHSPC sessions that timed out when the personal computer went into sleep mode.

**Product**
PHSGW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

`[local]host_name(config)#`

**Syntax**

```
threshold poll phspc-sleep-mode-timeout interval duration
```

`interval duration`

Default: 0 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
`duration` must be an integer from 30 through 60000.

**Usage**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the `threshold monitoring` and other threshold commands for additional information on the system’s support for thresholds in this chapter.

**Important:** To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshPHSPCSleepModeTimeout` command in this mode.

**Example**

The following command configures the polling interval to 600 seconds for PHSPC sleep mode timeouts:

```
threshold poll phspc-sleep-mode-timeout interval 600```
threshold poll phspc-sm-entry-denial interval

Configures the polling interval in seconds over which to count the number of denied PHSPC short message (SM) sessions.

**Product**
PHSGW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
threshold poll phspc-sm-entry-denial interval duration
```

- **interval duration**
  - Default: 0 seconds.
  - Specifies the amount of time (in seconds) that comprises the polling interval.
  - `duration` must be an integer from 30 through 60000.

**Usage**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the `threshold monitoring` and other threshold commands for additional information on the system’s support for thresholds in this chapter.

**Important:** To enable an SNMP trap for monitoring this threshold use the `snmp trap enable` **ThreshPHSPCSmEntryDenial** command in this mode.

**Example**

The following command configures the polling interval to 600 seconds for PHSPC SM session denials:

```
threshold poll phspc-sm-entry-denial interval 600
```
threshold poll port-high-activity interval

Configures the polling interval in seconds over which to measure the overall percentage of port utilization.

Product
All

Privilege
Administrator Security Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold poll port-high-activity interval seconds

intervals seconds

Configures the threshold polling interval in multiples of 30 seconds. seconds is an integer from 30 through 60000. Default is 300 seconds.

Usage

High port activity thresholds generate alerts or alarms based on the peak utilization percentage of each configured port during the specified polling interval. This threshold is configured on a per-port basis. Alerts or alarms are triggered for high port activity based on the following rules:
Enter condition: Actual percent peak utilization of a port is greater than or equal to the high threshold.
Clear condition: Actual percent peak utilization of a port is less than the low threshold.
If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval. This threshold is configured on a per-port basis configured using the port port-type slot#/port# command syntax.

Important: This command is not available on all platforms

Important: To enable an SNMP trap for monitoring this threshold use the snmp trap enable ThreshPortHighActivity command in this mode.

Important: To enable an SNMP trap for monitoring this threshold use the snmp trap enable ThreshPortHighActivity command in this mode.

Example

Use the following example to configure the polling interval over which to measure for high port activity to 300 seconds:
threshold poll port-high-activity interval

threshold poll port-high-activity interval 300
threshold poll port-rx-utilization interval

Configures the polling interval in seconds over which to measure the overall percentage of incoming traffic received over system ports.

Product
All

Privilege
Administrator Security Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold poll port-rx-utilization interval seconds

**interval seconds**

Configures the threshold polling interval in multiples of 30 seconds. **seconds** is an integer from 30 to 60000. Default is 300 seconds.

Usage

Receive port utilization thresholds generate alerts or alarms based on the utilization percentage of each configured port in relation to data received during the specified polling interval. This threshold is configured on a per-port basis configured using the **port port-type slot#/port#** command syntax.

**Important:** This command is not available on all platforms

**Important:** Ports configured for half-duplex do not differentiate between data received and data transmitted. (The transmitted and received percentages are combined.) Therefore, to avoid redundant alarms, it is recommended that only the receive or transmit utilization threshold be configured.

**Important:** To enable an SNMP trap for monitoring this threshold use the **snmp trap enable ThreshPortRxUtil** command in this mode.

Example

Use the following example to configure a threshold poll interval of 300 seconds (5 minutes)

threshold poll port-rx-utilization interval 300
threshold poll port-tx-utilization

Configures the polling interval in seconds over which to measure the overall percentage of outgoing traffic sent over system ports.

**Product**
All

**Privilege**
Administrator Security Administrator

**Mode**
Exec > Global Configuration
`configure`
Entering the above command sequence results in the following prompt:

```
[local] host_name(config) #
```

**Syntax**

```
threshold poll port-tx-utilization interval seconds
```

- **interval seconds**
  Configures the threshold polling interval in multiples of 30 seconds. `seconds` is an integer from 30 through 60000. Default is 300 seconds.

**Usage**
Transmit port utilization thresholds generate alerts or alarms based on the utilization percentage of each configured port in relation to data transmitted during the specified polling interval. This threshold is configured on a per-port basis configured using the `port port-type slot#/port#` command syntax.

**Important**: This command is not available on all platforms

**Important**: Ports configured for half-duplex do not differentiate between data received and data transmitted. (The transmitted and received percentages are combined.) Therefore, to avoid redundant alarms, it is recommended that only the receive or transmit utilization threshold be configured.

**Important**: To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshPortTxUtil` command in this mode.

**Example**

Use the following example to configure a threshold poll interval of **300** seconds (5 minutes)

```
threshold poll port-tx-utilization interval 300
```
threshold poll ppp-setup-fail-rate interval

Configures the polling interval in seconds over which to measure for the percentage of point-to-point protocol (PPP) setup failures.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

```
configure
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
threshold poll ppp-setup-fail-rate interval duration

interval duration
Default: 900 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.
duration must be an integer from 30 through 60000.
```

**Usage**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system’s support for thresholds in this chapter.

**Important:** To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshPPPSetupFailRate` command in this mode.

**Example**

The following command configures the polling interval to 600 seconds for PPP setup failures:

```
threshold poll ppp-setup-fail-rate interval 600
```
threshold poll reg-reply-error interval

Configures the polling interval over which to measure number of registration reply errors for Home Agent (HA) services.

Product
HA

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

```
threshold poll reg-reply-error interval duration
```

- **interval duration**

  Default: 0 seconds.
  Specifies the amount of time (in seconds) that comprises the polling interval.
  duration must be an integer from 30 through 60000.

Usage

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold monitoring** and other threshold commands for additional information on the system’s support for thresholds in this chapter.

**Important:** To enable an SNMP trap for monitoring this threshold use the **snmp trap enable** command in this mode.

Example

The following command configures the polling interval to 600 seconds for HA registration errors:

```
threshold poll reg-reply-error interval 600
```
threshold poll reg-total-active interval

Configures the polling interval over which to measure CSCF Total Active Registrations.

**Product**
SCM

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration
class configuration

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
threshold poll reg-total-active interval duration
```

- `interval duration`
  - Default: 300 seconds.
  - Specifies the amount of time (in seconds) that comprises the polling interval.
  - `duration` must be an integer from 30 through 60000.

**Usage**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system’s support for thresholds in this chapter.

**Important:** To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshCSCFSvcTotalActiveReg` command in this mode.

**Example**

The following command configures the polling interval to 600 seconds for CSCF active registrations:

```
threshold poll reg-total-active interval 600
```
threshold poll rereg-reply-error interval

Configures the polling interval over which to measure number of re-registration reply errors for HA services.

Product
HA

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

```
threshold poll rereg-reply-error interval duration
```

**interval duration**

Default: 0 seconds.
Specifies the amount of time (in seconds) that comprises the polling interval.

`duration` must be an integer from 30 through 60000.

Usage

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold monitoring and other threshold commands for additional information on the system’s support for thresholds in this chapter.

**Important:** To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshHASvcReregReplyError` command in this mode.

Example

The following command configures the polling interval to 600 seconds for HA re-registration reply errors:

```
threshold poll rereg-reply-error interval 600
```
threshold poll route-service interval

Configures the polling interval over which to count or measure the thresholding value for BGP route services on the system.

**Product**
All

**Privilege**
Administrator Security Administrator

**Mode**
Exec > Global Configuration

```
configure
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
threshold poll route-service interval dur
```

**default threshold poll route-service interval**

```
default
```

Restores the threshold poll interval value to its default value of 900 seconds.

```
interval time
```

Default: 900 seconds

Specifies the amount of time (in seconds) that comprises the polling interval.

```
dur` is any integer from 30 through 60000.
```

**Usage**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the `threshold model` and `threshold monitoring` commands for additional information on the system’s support for thresholding.

**Important:** To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshBGPRoutes` command in this mode.

**Example**

The following command configures the polling interval for the total BGP routes threshold polling duration value to 600 seconds (10 minutes):
threshold poll route-service interval

threshold poll route-service interval 600
threshold poll rp-setup-fail-rate interval

Configures the polling interval over which to measure the percentage of RAN PDSN (RP) setup failures.

**Product**
PDSN

**Privilege**
Administrator Security Administrator

**Mode**
Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
threshold poll rp-setup-fail-rate interval \( \text{dur} \)
```

```
default threshold poll route-service interval
```

**Usage**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold model and threshold monitoring commands for additional information on the system’s support for thresholding.

**Important:** To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshRPSetupFailRate` command in this mode.

**Example**

The following command configures the polling interval for the RP setup fail rate polling duration value to 600 seconds (10 minutes):

```
threshold poll rp-setup-fail-rate interval 600
```
threshold poll sess-flow-count interval

Configures the polling interval over which to measure the percentage of session manager flow count.

Product
All

Privilege
Administrator Security Administrator

Mode
Exec > Global Configuration
configure
Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold poll sess-flow-count interval dur

default threshold poll route-service interval

default
Restores the threshold poll interval value to its default value.

interval dur
Specifies the amount of time (in seconds) that comprises the polling interval.
dur is any integer from 30 through 60000.

Usage
This command sets the time period over which to monitor the specified value for threshold crossing.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold model and threshold monitoring commands for additional information on the system’s support for thresholding.

Example
The following command configures the polling interval for session manager flow count polling duration value to 600 seconds (10 minutes):

    threshold poll sess-flow-count interval 600
threshold poll storage-utilization interval

Configures the polling interval over which to measure the percentage of management card flash memory utilization.

Product
All

Privilege
Administrator Security Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold poll storage-utilization interval dur

default threshold poll route-service interval

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Restores the threshold poll interval value to its default value of 900 seconds.</td>
</tr>
<tr>
<td>interval time</td>
<td>Default: 900 seconds</td>
</tr>
<tr>
<td></td>
<td>Specifies the amount of time (in seconds) that comprises the polling interval.</td>
</tr>
<tr>
<td></td>
<td><em>dur</em> is any integer from 30 through 60000.</td>
</tr>
</tbody>
</table>

Usage

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold model** and **threshold monitoring** commands for additional information on the system’s support for thresholding.

**Important:** To enable an SNMP trap for monitoring this threshold use the **snmp trap enable** ThreshStorageUtilization command in this mode.

Example

The following command configures the polling interval for flash memory utilization polling duration value to 600 seconds (10 minutes):

threshold poll storage-utilization interval 600
threshold poll system-capacity interval

Configures the polling interval over which to measure the percentage of current system capacity.

Product
All

Privilege
Administrator Security Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold poll system-capacity interval dur

default threshold poll route-service interval

default

Restores the threshold poll interval value to its default value of 900 seconds.

interval time

Default: 900 seconds

Specifies the amount of time (in seconds) that comprises the polling interval.

dur is any integer from 30 through 60000.

Usage

This command sets the time period over which to monitor the specified value for threshold crossing.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold model and threshold monitoring commands for additional information on the system’s support for thresholding.

Important: To enable an SNMP trap for monitoring this threshold use the snmp trap enable ThreshSystemCapacity command in this mode.

Example

The following command configures the polling interval for flash memory utilization polling duration value to 600 seconds (10 minutes):

threshold poll system-capacity interval 600
**threshold poll total-asngw-sessions interval**

Configures the polling interval over which to count or measure the thresholding value for the total number of sessions across all the ASN-GW services on a system to trigger an alert or alarm.

**Product**
ASN-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
threshold poll total-asngw-sessions interval time
```

```
default threshold poll total-asngw-sessions interval
```

**Default threshold poll total-asngw-sessions interval**

```
default
```

Restores the threshold polling interval value to its default value of 300 seconds.

```
interval time
```

Default: 300 seconds

Specifies the amount of time (in seconds) that comprises the polling interval.

`time` must be an integer from 30 through 60000.

**Usage**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold model** and **threshold monitoring** commands for additional information on the system’s support for thresholding.

**Important:** To enable an SNMP trap for monitoring this threshold use the **snmp trap enable** **ThreshASNGWSessions** command in this mode.

**Example**

The following command configures the polling interval for counting the total number of ASN-GW sessions across all the ASN-GW services on a system, to 600 seconds (10 minutes):
threshold poll total-asngw-sessions interval 600
threshold poll total-ggsn-sessions interval

Configures the polling interval over which to count or measure the thresholding value for the total number of sessions across all the GGSN services on a system to trigger an alert or alarm.

Product
GGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax
threshold poll total-ggsn-sessions interval time
default threshold poll total-ggsn-sessions interval

default
Restores the threshold polling interval value to its default value of 300 seconds.

interval time
Default: 300 seconds
Specifies the amount of time (in seconds) that comprises the polling interval. time must be an integer from 30 through 60000.

Usage
This command sets the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold model and threshold monitoring commands for additional information on the system’s support for thresholding.

**Important:** To enable an SNMP trap for monitoring this threshold use the snmp trap enable ThreshGGSNSessions command in this mode.

Example
The following command configures the polling interval for counting the total number of GGSN sessions across all the GGSN services on a system, to 600 seconds (10 minutes):
threshold poll total-ggsn-sessions interval 600
threshold poll total-gprs-pdp-sessions interval

Configures the polling interval over which to count the total number of 2G-activated PDP contexts per GPRS sessions on the system.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold poll total-gprs-pdp-sessions interval time

default threshold poll total-gprs-pdp-sessions interval
default
Restores the threshold polling interval value to its default value of 300 seconds.

interval time
Default: 300 seconds
Specifies the amount of time (in seconds) that comprises the polling interval.
time must be an integer from 30 through 60000.

Usage
This command sets the time period over which to monitor the specified value for threshold crossing.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold model and threshold monitoring commands for additional information on the system’s support for thresholding.

Important: To enable an SNMP trap for monitoring this threshold use the snmp trap enable ThreshGPRSPDPSessions command in this mode.

Example
The following command configures the polling interval for counting the total number of 2G-activated PDP contexts per GPRS sessions, to 600 seconds (10 minutes):
threshold poll total-gprs-pdp-sessions interval 600
threshold poll total-gprs-sessions interval

Configures the polling interval over which to count the total number of 2G-attached subscribers on the system.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold poll total-gprs-sessions interval time

default threshold poll total-gprs-sessions interval

  default
  Restores the threshold polling interval value to its default value of 300 seconds.

  interval time
  Default: 300 seconds
  Specifies the amount of time (in seconds) that comprises the polling interval.
  time must be an integer from 30 through 60000.

Usage

This command sets the time period over which to monitor the specified value for threshold crossing.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold model and threshold monitoring commands for additional information on the system’s support for thresholding.

Important: To enable an SNMP trap for monitoring this threshold use the snmp trap enable ThreshGPRSSessions command in this mode.

Example

The following command configures the polling interval for counting the total number of 2G-attached subscribers, to 600 seconds (10 minutes):

   threshold poll total-gprs-sessions interval 600
threshold poll total-ha-sessions interval

Configures the polling interval over which to count the total number of Home Agent (HA) sessions on the system.

**Product**
HA

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

```
configure
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config) #
```

**Syntax**

```
threshold poll total-ha-sessions interval time
```

```
default threshold poll total-ha-sessions interval
```

- **default**
  Restores the threshold polling interval value to its default value of 300 seconds.

- **interval time**
  Default: 300 seconds
  Specifies the amount of time (in seconds) that comprises the polling interval.
  `time` must be an integer from 30 through 60000.

**Usage**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold model** and **threshold monitoring** commands for additional information on the system’s support for thresholding.

**Important:** To enable an SNMP trap for monitoring this threshold use the **snmp trap enable ThreshHASessions** command in this mode.

**Example**

The following command configures the polling interval for counting the total number of HA sessions on the system, to 600 seconds (10 minutes):

```
threshold poll total-ha-sessions interval 600
```
threshold poll total-henbgw-henb-sessions

Configures the polling interval on how frequently the thresholds are polled for total HeNB-GW HeNB sessions.

Product
HeNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:
[local]host_name(config)#

Syntax

threshold poll total-henbgw-henb-sessions interval time

default threshold poll total-henbgw-henb-sessions interval

default
Restores the threshold polling interval value to its default value of 900 seconds.

interval time
Default: 900 seconds
Specifies the amount of time (in seconds) that comprises the polling interval.
"time" must be an integer from 30 through 60000.

Usage

This command sets the time period over which to monitor the specified value for threshold crossing.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold model and threshold monitoring commands for additional information on the system’s support for thresholding.

Important: To enable SNMP trap for threshold monitoring of this threshold use snmp trap enable ThreshHeNBGWHenbSessions command in this mode.

Example

The following command configures the polling interval to 600 seconds (10 minutes):

threshold poll total-henbgw-henb-sessions interval 600
threshold poll total-henbgw-ue-sessions

Configures the polling interval on how frequently the thresholds are polled for total HeNB-GW UE sessions.

**Product**
HeNB-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

**Syntax**

```
threshold poll total-henbgw-ue-sessions interval time
```

```
default threshold poll total-henbgw-ue-sessions interval
```

<table>
<thead>
<tr>
<th><strong>default</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Restores the threshold polling interval value to its default value of 900 seconds.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>interval time</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Default: 900 seconds</td>
</tr>
<tr>
<td>Specifies the amount of time (in seconds) that comprises the polling interval.</td>
</tr>
<tr>
<td><code>time</code> must be an integer from 30 through 60000.</td>
</tr>
</tbody>
</table>

**Usage**
This command sets the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the `threshold model` and `threshold monitoring` commands for additional information on the system’s support for thresholding.

**Important:** To enable SNMP trap for threshold monitoring of this threshold use `snmp trap enable ThreshHeNBGWUeSessions` command in this mode.

**Example**
The following command configures the polling interval to 600 seconds (10 minutes) for HeNB-GW UE sessions:

```
threshold poll total-henbgw-ue-sessions interval 600
```
threshold poll total-hnbgw-hnb-sessions

Configures the polling interval over which to count or measure the thresholding value for the total number of IuH sessions between the HNB and HNB-GW to count across all the HNB-GW services on a system to trigger an alert or alarm.

Product
HNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold poll total-hnbgw-hnb-sessions interval time

default threshold poll total-hnbgw-hnb-sessions interval

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Restores the threshold polling interval value to its default value of 900 seconds.</td>
</tr>
<tr>
<td>interval time</td>
<td>Specifies the amount of time (in seconds) that comprises the polling interval. time must be an integer from 30 through 60000.</td>
</tr>
</tbody>
</table>

Usage

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold model and threshold monitoring commands for additional information on the system’s support for thresholding.

**Important:** To enable SNMP trap for threshold monitoring of this threshold use snmp trap enable ThreshTotalHNBGWnBSSess command in this mode.

Example

The following command configures the polling interval for counting the total number of HNB sessions between HNB and HNB-GW across all the HNB-GW services on a system, to 600 seconds (10 minutes):

```
```
threshold poll total-hnbgw-hnb-sessions

threshold poll total-hnbgw-hnb-sessions interval 600
threshold poll total-hnbgw-iu-sessions

Configures the polling interval over which to count or measure the thresholding value for the total number of subscriber sessions on HNB-GW service (over Iu-CS/Iu-PS interface) to count across all the HNB-GW services on a system to trigger alert or alarm.

Product
HNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold poll total-hnbgw-iu-sessions interval time

default threshold poll total-hnbgw-iu-sessions interval

default
Restores the threshold poll interval value to its default value of 300 seconds.

interval time
Default: 300 seconds
Specifies the amount of time (in seconds) that comprises the polling interval.

time must be an value from 30 through 60000.

Usage

This command sets the time period over which to monitor the specified value for threshold crossing.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold model and threshold monitoring commands for additional information on the system’s support for thresholding.

Important: To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshTotalHNBGWlUSess` command in this mode.

Example

The following command configures the polling interval for counting the total number of subscriber sessions across all the HNB-GW services on a system, to 600 seconds (10 minutes):
threshold poll total-hnbgw-iu-sessions

threshold poll total-hnbgw-iu-sessions interval 600
threshold poll total-hnbgw-ue-sessions

Configures the polling interval over which to count or measure the thresholding value for the total number of UEs connected to HNB-GW service to count across all the HNB-GW services on a system to trigger alert or alarm.

Product
HNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold poll total-hnbgw-ue-sessions interval time

default threshold poll total-hnbgw-ue-sessions interval

default
Restores the threshold poll interval value to its default value of 300 seconds.

interval time
Default: 300 seconds
Specifies the amount of time (in seconds) that comprises the polling interval.
time must be an integer from 30 through 60000.

Usage
This command sets the time period over which to monitor the specified value for threshold crossing.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold model and threshold monitoring commands for additional information on the system’s support for thresholding.

Important: To enable an SNMP trap for monitoring this threshold use the \texttt{snmp trap enable ThreshTotalHNBGWUeSess} command in this mode.

Example
The following command configures the polling interval for the total number of UEs connected to an HNB-GW service across all the HNB-GW services on a system, to 600 seconds (10 minutes):
threshold poll total-hnbgw-ue-sessions

threshold poll total-hnbgw-ue-sessions interval 600
threshold poll total-hsgw-sessions interval

Configures the polling interval over which to count the total number of HRPD Serving Gateway (HSGW) sessions across all services in the system.

Product
HSGW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[llocal]host_name(config)#

Syntax

threshold poll total-hsgw-sessions interval time

default threshold poll total-hsgw-sessions interval

default
Restores the threshold poll interval value to its default value of 300 seconds.

interval time
Default: 300 seconds
Specifies the amount of time (in seconds) that comprises the polling interval.
time must be an integer from 30 through 60000.

Usage
This command sets the time period over which to monitor the specified value for threshold crossing.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold model and threshold monitoring commands for additional information on the system’s support for thresholding.

Important: To enable an SNMP trap for monitoring this threshold use the snmp trap enable ThreshHSGWSessions command in this mode.

Example

The following command configures the polling interval for the total number of HSGW sessions across all the HSGW services on a system, to 600 seconds (10 minutes):
threshold poll total-hsgw-sessions interval 600
threshold poll total-lma-sessions interval

Configures the polling interval over which to count the total number of Local Mobility Anchor (LMA) sessions across all services in the system.

**Product**
P-GW
SAEGW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
threshold poll total-lma-sessions interval time
default threshold poll total-lma-sessions interval
```

**Usage**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the `threshold model` and `threshold monitoring` commands for additional information on the system’s support for thresholding.

**Important:** To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshLMASessions` command in this mode.

**Example**
The following command configures the polling interval for the total number of LMA sessions across all the LMA sessions on a system, to 600 seconds (10 minutes):

```
threshold poll total-lma-sessions interval 600
```
threshold poll total-lns-sessions interval

Configures the polling interval over which to count the total number of L2TP Network Server (LNS) sessions in the system.

**Product**

PDSN
GGSN
HA

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

```
[local-host_name(config)]#
```

**Syntax**

```
threshold poll total-lns-sessions interval time
default threshold poll total-lns-sessions interval
```

**Usage**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the `threshold model` and `threshold monitoring` commands for additional information on the system’s support for thresholding.

**Important:** To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshLNSSessions` command in this mode.

**Example**
The following command configures the polling interval for the total number of LNS sessions across all the LNS sessions on a system, to 600 seconds (10 minutes):

```
threshold poll total-Ins-sessions interval 600```

threshold poll total-mme-sessions

Configures the polling interval over which to count or measure the thresholding value for MME sessions on the system.

Product
MME

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold poll total-mme-sessions interval time

default threshold poll total-mme-sessions interval

default
Restores the threshold poll interval value to its default value of 900 seconds.

interval time
Default: 900 seconds
Specifies the polling interval (in seconds) for counting the total number of MME sessions on the system.
time must be any integer from 30 through 60000.

Usage

This command sets the time period over which to monitor the specified value for threshold crossing.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold model and threshold monitoring commands for additional information on the system’s support for thresholding.

Important: To enable an SNMP trap for monitoring this threshold use the snmp trap enable ThresholdMMESessions command in this mode.

Example

The following command configures the polling interval for the total MME session threshold polling duration value to 600 seconds (10 minutes):

threshold poll total-mme-sessions interval 600
threshold poll total-pdsn-sessions interval

Configures the polling interval over which to count the total number of Packet Data Serving Node (PDSN) sessions in the system.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

```
configure
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config)#
```

**Syntax**

```
threshold poll total-pdsn-sessions interval time

default threshold poll total-pdsn-sessions interval
```

- **default**
  Restores the threshold poll interval value to its default value of 300 seconds.

- **interval time**
  Default: 300 seconds
  Specifies the amount of time (in seconds) that comprises the polling interval.
  `time` must be an integer from 30 through 60000.

**Usage**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the `threshold model` and `threshold monitoring` commands for additional information on the system’s support for thresholding.

**Important:** To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshPDSNSessions` command in this mode.

**Example**

The following command configures the polling interval for the total number of PDSN sessions across all the PDSN sessions on a system, to `600` seconds (10 minutes):
threshold poll total-pdsn-sessions interval 600
threshold poll total-pgw-sessions interval

Configures the polling interval over which to count the total number of Packet Data Network Gateway (P-GW) sessions across all services in the system.

Product
P-GW
SAEGW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold poll total-pgw-sessions interval time

default threshold poll total-pgw-sessions interval

```bash
default
Restores the threshold poll interval value to its default value of 300 seconds.

interval time
Default: 300 seconds
Specifies the amount of time (in seconds) that comprises the polling interval.
time must be an integer from 30 through 60000.
```

Usage

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the `threshold model` and `threshold monitoring` commands for additional information on the system’s support for thresholding.

**Important:** To enable an SNMP trap for monitoring this threshold use the `snmp trap enable` `ThreshPGWSessions` command in this mode.

Example
The following command configures the polling interval for the total number of P-GW sessions across all the P-GW sessions on a system, to 600 seconds (10 minutes):

```
threshold poll total-pgw-sessions interval 600
```
threshold poll total-saegw-sessions interval

Configures the polling interval over which to count the total number of System Architecture Evolution Gateway (SAEGW) sessions across all services in the system.

**Product**
SAEGW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
threshold poll total-saegw-sessions interval time
```

**default threshold poll total-saegw-sessions interval**

<table>
<thead>
<tr>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restores the threshold poll interval value to its default value of 300 seconds.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>interval time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default: 300 seconds</td>
</tr>
<tr>
<td>Specifies the amount of time (in seconds) that comprises the polling interval.</td>
</tr>
<tr>
<td>time must be an integer from 30 through 60000.</td>
</tr>
</tbody>
</table>

**Usage**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the `threshold model` and `threshold monitoring` commands for additional information on the system’s support for thresholding.

**Example**

The following command configures the polling interval for the total number of SAEGW sessions on a system, to 600 seconds (10 minutes):

```
threshold poll total-saegw-sessions interval 600
```
threshold poll total-sgsn-pdp-sessions interval

Configures the polling interval over which to count the total number of PDP contexts for all Serving GPRS Support Node (SGSN) sessions in the system.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold poll total-sgsn-pdp-sessions interval time

default threshold poll total-sgsn-pdp-sessions interval

default
Restores the threshold poll interval value to its default value of 300 seconds.

interval time
Default: 300 seconds
Specifies the amount of time (in seconds) that comprises the polling interval.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold model and threshold monitoring commands for additional information on the system’s support for thresholding.

Important: To enable an SNMP trap for monitoring this threshold use the snmp trap enable ThreshSGSNPDPSessions command in this mode.

Example

The following command configures the polling interval for the total number of PDP contexts across all the SGSN sessions on a system, to 600 seconds (10 minutes):
threshold poll total-sgsn-pdp-sessions interval 600
threshold poll total-sgsn-sessions interval

Configures the polling interval over which to count the total number of SGSN sessions in the system.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

**configure**
Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
threshold poll total-sgsn-sessions interval time

default threshold poll total-sgsn-sessions interval
```

**Usage**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the **threshold model** and **threshold monitoring** commands for additional information on the system’s support for thresholding.

**Important:** To enable an SNMP trap for monitoring this threshold use the **snmp trap enable** **ThreshSGSNSessions** command in this mode.

**Example**

The following command configures the polling interval for the total number of SGSN sessions on a system, to 600 seconds (10 minutes):

```
threshold poll total-sgsn-sessions interval 600
```
threshold poll total-sgw-sessions interval

Configures the polling interval over which to count the total number of Serving Gateway (S-GW) sessions across all services in the system.

Product
S-GW
SAEGW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold poll total-sgw-sessions interval time

default threshold poll total-sgw-sessions interval

default
Restores the threshold poll interval value to its default value of 300 seconds.

interval time

Default: 300 seconds
Specifies the amount of time (in seconds) that comprises the polling interval.
time must be an integer from 30 through 60000.

Usage

This command sets the time period over which to monitor the specified value for threshold crossing.

Important: All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the threshold model and threshold monitoring commands for additional information on the system’s support for thresholding.

Important: To enable an SNMP trap for monitoring this threshold use the snmp trap enable ThreshSGWSessions command in this mode.

Example
The following command configures the polling interval for the total number of S-GW sessions on a system, to 600 seconds (10 minutes):

```
threshold poll total-sgw-sessions interval 600
```
**threshold poll total-subscriber interval**

Configures the polling interval over which to count the total number of subscriber sessions across all services in the system.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration  
```
configure
```
Entering the above command sequence results in the following prompt:
```
[local]host_name(config)#
```

**Syntax**

```
threshold poll total-subscriber interval time
```

**default threshold poll total-subscriber interval**

```
default
```
Restores the threshold poll interval value to its default value of 300 seconds.

```
interval time
```
Default: 300 seconds  
Specifies the amount of time (in seconds) that comprises the polling interval.  
*time* must be an integer from 30 through 60000.

**Usage**

This command sets the time period over which to monitor the specified value for threshold crossing.

**Important:** All configured polling intervals are rounded up to the closest multiple of 30. For example, if a polling interval is configured for 130 seconds, the system uses a polling interval of 150 seconds.

Refer to the *threshold model* and *threshold monitoring* commands for additional information on the system’s support for thresholding.

**Important:** To enable an SNMP trap for monitoring this threshold use the *snmp trap enable* ThreshSubscriberTotal command in this mode.

**Example**

The following command configures the polling interval for the total number of subscribers on a system, to 600 seconds (10 minutes):
threshold poll total-subscriber interval 600
threshold poll tpo-dns-failure

The Traffic Performance Optimization (TPO) in-line service is not supported in this release.
threshold poll tpo-low-compression-gain

The Traffic Performance Optimization (TPO) in-line service is not supported in this release.
threshold poll tpo-rto-timeout

The Traffic Performance Optimization (TPO) in-line service is not supported in this release.
This section includes the commands `threshold ppp-setup-fail-rate` through `url-blacklisting database`. The Global Configuration Mode is used to configure basic system-wide parameters.

**Mode**

Exec > Global Configuration

`configure`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
**threshold ppp-setup-fail-rate**

Configures alarm or alert thresholds for the percentage of point-to-point protocol (PPP) setup failures.

**Product**
- PDSN
- GGSN

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration
  - configure

Entering the above command sequence results in the following prompt:

```
[local] host_name(config) #
```

**Syntax**

```
threshold ppp-setup-fail-rate high_thresh [ clear low_thresh ]
```

- **high_thresh**
  - Default: 0
  - Specifies the high threshold rate percentage for PPP setup failures experienced by the system that must be met or exceeded within the polling interval to generate an alert or alarm.
  - `high_thresh` is an integer from 0 through 100. A value of 0 disables the threshold.

- **clear low_thresh**
  - Default: 0
  - Specifies the low threshold rate percentage for PPP setup failures experienced by the system that maintains a previously generated alarm condition. If the number of setup failures falls beneath the low threshold within the polling interval, a clear alarm will be generated.
  - `low_thresh` is an integer from 0 through 100. A value of 0 disables the threshold.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**

PPP setup failure rate thresholds generate alerts or alarms based on the rate of call setup failures experienced by the system during the specified polling interval. The failure rate is the percentage of failures as determined by number of PPP setup failures divided by the total number of PPP sessions initiated.

Alerts or alarms are triggered for PPP setup failure rates based on the following rules:

- **Enter condition:** Actual number of call setup failures is greater than or equal to the high threshold.

- **Clear condition:** Actual number of call setup failures is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Example**

The following command configures a PPP setup failure rate high percentage threshold of 50 percent and a clear threshold of 45 percent:

```
threshold ppp-setup-fail-rate 50 clear 45
```
threshold route-service bgp-routes

Configures alarm or alert thresholds for the percentage of route services to BGP routes.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure
Entering the above command sequence results in the following prompt:
[local]host_name(config)#

Syntax

threshold route-service bgp-routes high_thresh [ clear low_thresh ]

high_thresh
Default: 0
Specifies the high threshold rate percentage for BGP routes on the system that must be met or exceeded within the polling interval to generate an alert or alarm.
high_thresh is an integer from 0 through 100. A value of 0 disables the threshold.

clear low_thresh
Default: 0
Specifies the low threshold rate percentage for BGP routes on the system that maintains a previously generated alarm condition. If the number of setup failures falls beneath the low threshold within the polling interval, a clear alarm will be generated.
low_thresh is an integer from 0 through 100. A value of 0 disables the threshold.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Use this command to configure a threshold in percentage of maximum BGP routes allowed. If the percentage of the number of BGP routes in a context (including all VRFs) reaches high_thresh, a notification is generated. Optionally, if the threshold subsystem is configured in ‘alarm’ mode, a Threshold_Clear notification is generated when the percentage of the number of BGP routes in a context (including all VRFs) goes below low_thresh. The maximum number of BGP routes is also sent by BGP task when getting the statistics.
Alerts or alarms are triggered for BGP routes based on the following rules:
• Enter condition: Actual number of call setup failures is greater than the high threshold.
• Clear condition: Actual number of call setup failures is less than the low threshold.
If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval. Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Example**

The following command configures system for high threshold of 50 percent and a clear threshold of 45 percent:

```
threshold route-service bgp-routes 50 clear 45
```
threshold rp-setup-fail-rate

Configures alarm or alert thresholds for the percentage of RAN PDSN (RP) setup failures.

Product
PDSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold rp-setup-fail-rate high_thresh [ clear low_thresh ]

high_thresh
Default: 0
Specifies the high threshold rate percentage for RP setup failures experienced by the system that must be met or exceeded within the polling interval to generate an alert or alarm.
high_thresh is an integer from 0 through 100. A value of 0 disables the threshold.

clear low_thresh
Default: 0
Specifies the low threshold rate percentage for RP setup failures experienced by the system that maintains a previously generated alarm condition. If the number of setup failures falls beneath the low threshold within the polling interval, a clear alarm will be generated.
low_thresh is an integer from 0 through 100. A value of 0 disables the threshold.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage
RP setup failure rate thresholds generate alerts or alarms based on the rate of call setup failures experienced by the system during the specified polling interval. The failure rate is the percentage of failures as determined by number of Registration Request Messages rejected divided by the total number of Registration Request Messages received.
Alerts or alarms are triggered for RP setup failure rates based on the following rules:

• Enter condition: Actual number of call setup failures is greater than or equal to the high threshold.

• Clear condition: Actual number of call setup failures is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Example**

The following command configures a RP setup failure rate high threshold of 50 percent and a clear threshold of 45 percent:

```
threshold rp-setup-fail-rate 50 clear 45
```
threshold sess-flow-count

Configures alarm or alert thresholds for the percentage of session manager flow count.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration

configure
Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold sess-flow-count flow_count_thresh [ clear clear_thresh ]

flow_count_percent

Default: 90
Specifies the high threshold rate percentage for session manager flow count to generate an alert or alarm. flow_count_thresh is an integer from 1 through 100.

clear clear_thresh

Specifies the low threshold rate percentage for session manager flow count. If the number of session manager flow count falls beneath the low threshold, a clear alarm will be generated. clear_thresh is an integer from 1 through 100. The value chosen for the clear_thresh must always be lesser than the flow_count_thresh.

Usage
Use this command to configure thresholds for monitoring the session flow count. Refer to the threshold poll command to configure the polling interval and the threshold monitoring command to enable thresholding for this value.

Example
The following command configures a session flow count high threshold of 50 percent and a clear threshold of 45 percent:

threshold sess-flow-count 50 clear 45
threshold spc-cpu-memory-usage

This command has been renamed to threshold mgmt-cpu-memory-usage. Please refer to that command for details. Note that for backwards compatibility, the system accepts this command as valid.

⚠️ Important: This command is not supported on all platforms.
threshold spc-cpu-utilization

This command has been renamed to `threshold mgmt-cpu-utilization`. Please refer to that command for details. Note that for backwards compatibility, the system accepts this command as valid.
threshold storage-utilization

Configures alarm or alert thresholds for the percentage of management card flash memory utilization.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold storage-utilization high_thresh [ clear low_thresh ]

high_thresh

Default: 90
Specifies the high threshold storage utilization percentage that must be met or exceeded within the polling interval to generate an alert or alarm.

high_thresh is an integer from 0 through 100. A value of 0 disables the threshold.

clear low_thresh

Default: 90
Specifies the low threshold storage utilization percentage that maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.

low_thresh is an integer from 0 through 100. A value of 0 disables the threshold.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Flash memory utilization thresholds generate alerts or alarms based on the utilization percentage of storage available to the system.
Alerts or alarms are triggered for storage utilization based on the following rules:

- Enter condition: Actual percentage storage utilization is greater than or equal to the high threshold.
- Clear condition: Actual percentage storage utilization is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the threshold poll command to configure the polling interval and the threshold monitoring command to enable thresholding for this value.
Example

The following command configures a high threshold for storage utilization percentage of 85 for a system using the Alert thresholding model:

```
threshold storage-utilization 85
```
threshold subscriber active

Configures alarm or alert thresholds for the number of active subscribers in the system.

Product
PDSL
GGSN
SGSN
HA

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold subscriber active high_thresh [ clear low_thresh ]

high_thresh
Default: 0
Specifies the high threshold number of active subscriber sessions facilitated by the system that must be met or exceeded within the polling interval to generate an alert or alarm.
high_thresh is an integer from 0 through 4000000. A value of 0 disables the threshold.

clear low_thresh
Default: 0
Specifies the low threshold number of active subscriber sessions facilitated by the system that maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.
low_thresh is an integer from 0 and 4000000. A value of 0 disables the threshold.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage
Active subscriber thresholds generate alerts or alarms based on the total number of active subscriber sessions facilitated by the system during the specified polling interval.
Alerts or alarms are triggered for active subscriber totals based on the following rules:

• Enter condition: Actual total number of active subscriber sessions is greater than or equal to the high threshold.

• Clear condition: Actual total number of active subscriber sessions is less than the low threshold.
If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Example**

The following command configures an active subscriber high threshold count of **150000** and a low threshold of **100000** for a system using the Alarm thresholding model:

```
threshold subscriber active 150000 clear 100000
```
threshold subscriber total

Configures alarm or alert thresholds for the total number of active and inactive subscribers in the system.

**Product**
PDSN
GGSN
HA

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
threshold subscriber total high_thresh [ clear low_thresh ]
```

**high_thresh**

Default: 0
Specifies the high threshold number of subscriber sessions (active and dormant) facilitated by the system that must be met or exceeded within the polling interval to generate an alert or alarm. The high threshold is an integer from 0 through 4000000. A value of 0 disables the threshold.

**clear low_thresh**

Default: 0
Specifies the low threshold number of subscriber sessions (active and dormant) facilitated by the system that maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated. The low threshold is an integer from 0 and 4000000. A value of 0 disables the threshold.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**

Total subscriber thresholds generate alerts or alarms based on the total number of subscriber sessions (active and dormant) facilitated by the system during the specified polling interval. Alerts or alarms are triggered for subscriber totals based on the following rules:

- **Enter condition:** Actual total number of subscriber sessions is greater than or equal to the high threshold.
- **Clear condition:** Actual total number of subscriber sessions is less than the low threshold.
Global Configuration Mode Commands (threshold ppp - url-blacklisting)

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Example**

The following command configures an active subscriber high threshold count of **450000** and a low threshold of **250000** for a system using the Alarm thresholding model:

```
threshold subscriber total 450000 clear 250000
```
threshold system-capacity

Configures alarm or alert thresholds based on the percentage of current system capacity.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

```
configure
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
threshold system high_thresh [ clear low_thresh ]
```

- `high_thresh`
  Default: 90
  Specifies the high threshold system capacity percentage that must be met or exceeded within the polling interval to generate an alert or alarm.
  `high_thresh` is an integer from 0 through 100. A value of 0 disables the threshold.

- `clear low_thresh`
  Default: 90
  Specifies the low threshold system capacity percentage that maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.
  `low_thresh` is an integer from 0 through 100. A value of 0 disables the threshold.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**

Flash memory utilization thresholds generate alerts or alarms based on the system utilization. Alerts or alarms are triggered for system capacity based on the following rules:

- **Enter condition:** Actual percentage of system capacity is greater than or equal to the high threshold.
- **Clear condition:** Actual percentage of system capacity is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Example**
The following command configures a high threshold for system capacity percentage of 95 for a system using the Alert thresholding model:

```
threshold system-capacity 95
```
threshold total-asngw-sessions

Configures alarm or alert thresholds for the total number of ASN-GW sessions across all the services in the system.

Product
ANS-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold total-asngw-sessions high_thresh [ clear low_thresh ]

**high_thresh**
Default: 0 (Disabled)
Specifies the high threshold number of total ASN-GW sessions across all the sessions in the system that must be met or exceeded within the polling interval to generate an alert or alarm.

*high_thresh* is an integer from 0 through 4000000. A value of 0 disables the threshold.

**clear low_thresh**
Default: 0 (Disabled)
Specifies the low threshold number of total ASN-GW sessions that maintains a previously generated alarm condition. If the number of ASN-GW sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.

*low_thresh* is an integer from 0 and 4000000. A value of 0 disables the threshold.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Monitor and set alarms or alerts when the total number of ASN-GW sessions across all the services in the system is equal to or greater than the set limit.

Alerts or alarms are triggered for the total number of ASN-GW sessions based on the following rules:

- **Enter condition:** Actual total number of ASN-GW sessions is greater than or equal to the high threshold.

- **Clear condition:** Actual total number of ASN-GW sessions is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the threshold poll command to configure the polling interval and the threshold monitoring command to enable thresholding for this value.
Example

The following command configures a total ASN-GW session high threshold count of 10000 for a system using the Alert thresholding model:

```
threshold total-asngw-sessions 10000
```
threshold total-ggsn-sessions

Configures alarm or alert thresholds for the total number of GGSN sessions across all the services in the system.

Product
GGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold total-ggsn-sessions high_thresh [ clear low_thresh ]

high_thresh
Default: 0 (Disabled)
Specifies the high threshold number of total GGSN sessions across all the sessions in the system that must be met or exceeded within the polling interval to generate an alert or alarm.
high_thresh is an integer from 0 through 4000000. A value of 0 disables the threshold.

clear low_thresh
Default: 0 (Disabled)
Specifies the low threshold number of total GGSN sessions that maintains a previously generated alarm condition. If the number of GGSN sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.
low_thresh is an integer from 0 and 4000000. A value of 0 disables the threshold.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Monitor and set alarms or alerts when the total number of GGSN sessions across all the services in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for the total number of GGSN sessions based on the following rules:
- **Enter condition:** Actual total number of GGSN sessions is greater than or equal to the high threshold.
- **Clear condition:** Actual total number of GGSN sessions is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the threshold poll command to configure the polling interval and the threshold monitoring command to enable thresholding for this value.

Example
The following command configures a total GGSN session high threshold count of 10000 for a system using the Alert thresholding model:

```
threshold total-ggsn-sessions 10000
```
threshold total-gprs-pdp-sessions

Configures alarm or alert thresholds for the total number of PDP contexts per GPRS sessions in the system.

Product
SGSN

Privilege
Administrator

Mode
Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold total-gprs-pdp-sessions high_thresh [ clear low_thresh ]

high_thresh

Default: 0
Specifies the high threshold number of total PDP contexts per GPRS session for all GPRS services that must be met or exceeded within the polling interval to generate an alert or alarm.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

low_thresh is an integer from 1 through 2000000. A value of 0 disables the threshold.

clear low_thresh

Default: 0
Specifies the low threshold number of total PDP contexts per GPRS session for all GPRS services that maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.

low_thresh is an integer from 0 and 2000000. A value of 0 disables the threshold.

Usage

Monitor and set alarms or alerts when the total number of GPRS sessions in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for GPRS sessions based on the following rules:

- **Enter condition**: Actual total number of PDP Contexts is greater than or equal to the high threshold.
- **Clear condition**: Actual total number of PDP contexts is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the threshold poll command to configure the polling interval and the threshold monitoring command to enable thresholding for this value.

Example

Refer to the threshold poll command to configure the polling interval and the threshold monitoring command to enable thresholding for this value.
The following command configures a total number of PDP contexts per GPRS session high threshold count of 10000 for a system using the Alert thresholding model:

```bash
threshold total-gprs-pdp-sessions 10000
```
threshold total-gprs-sessions

Configures alarm or alert thresholds for the total number of GPRS sessions in the system.

Product
SGSN

Privilege
Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold total-gprs-sessions high_thresh [ clear low_thresh ]

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>high_thresh</td>
<td>Specifies the high threshold number of total GPRS sessions for all GPRS services that must be met or exceeded within the polling interval to generate an alert or alarm. high_thresh is an integer from 1 through 2000000. A value of 0 disables the threshold.</td>
</tr>
<tr>
<td>clear low_thresh</td>
<td>Specifies the low threshold number of total GPRS sessions for all GPRS services that maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated. low_thresh is an integer from 0 and 2000000. A value of 0 disables the threshold.</td>
</tr>
</tbody>
</table>

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Monitor and set alarms or alerts when the total number of GPRS sessions in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for GPRS sessions based on the following rules:

- **Enter condition:** Actual total number of GPRS sessions is greater than or equal to the high threshold.
- **Clear condition:** Actual total number of GPRS sessions is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the command to configure the polling interval and the threshold monitoring command to enable thresholding for this value.

Example
The following command configures a total number of GPRS sessions high threshold count of 10000 for a system using the Alert thresholding model:

```plaintext
threshold total-gprs-sessions 10000
```
threshold total-ha-sessions

Configures alarm or alert thresholds for the total number of Home Agent (HA) sessions across all services in the system.

Product
HA

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold total-ha-sessions high_thresh [ clear low_thresh ]

high_thresh
Default: 0
Specifies the high threshold number of HA sessions for all HA services that must be met or exceeded within the polling interval to generate an alert or alarm.
high_thresh is an integer from 0 through 4000000. A value of 0 disables the threshold.

clear low_thresh
Default: 0
Specifies the low threshold number of HA sessions for all HA services that maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.
low_thresh is an integer from 0 and 4000000. A value of 0 disables the threshold.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Monitor and set alarms or alerts when the total number of HA sessions in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for HA sessions based on the following rules:
• Enter condition: Actual total number of HA sessions is greater than or equal to the high threshold.
• Clear condition: Actual total number of HA sessions is less than the low threshold.
If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the threshold poll command to configure the polling interval and the threshold monitoring command to enable thresholding for this value.

Example
The following command configures a total number of HA sessions high threshold count of 10000 for a system using the Alert thresholding model:

```
threshold total-ha-sessions 10000
```
threshold total-hnb-gw-hnb-sessions

Configures alarm or alert thresholds for the total number of Home NodeB (HNB) sessions across all the HNB Gateway (HNB-GW) services in the system.

Product
HNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

```
threshold total-hnb-gw-hnb-sessions high_thresh [ clear low_thresh ]
```

<table>
<thead>
<tr>
<th>high_thresh</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default: 0 (Disabled)</td>
</tr>
<tr>
<td>Specifies the high threshold for the total number of HNB-HNB-GW sessions on IuH interfaces across all HNB-GW services on a system that must be met or exceeded within the polling interval to generate an alert or alarm.</td>
</tr>
<tr>
<td>high_thresh is an integer from 0 through 1000000. A value of 0 disables the threshold.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>clear low_thresh</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default: 0 (Disabled)</td>
</tr>
<tr>
<td>Specifies the low threshold for the total number of HNB-HNB-GW sessions on IuH interfaces across all services on a system that maintains a previously generated alarm condition. If the number of HNB-HNB-GW sessions in a system falls beneath the low threshold within the polling interval, a clear alarm will be generated.</td>
</tr>
<tr>
<td>low_thresh is an integer from 0 through 1000000. A value of 0 disables the threshold.</td>
</tr>
</tbody>
</table>

⚠️ Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Use this command to monitor and set alarms or alerts when the total number of HNB-HNB-GW sessions on IuH interface across all HNB-GW services in the system is equal to or greater than the set limit. Alerts or alarms are triggered for the total number of HNB-HNB-GW sessions on IuH interface based on the following rules:

- **Enter condition:** Actual total number of HNB-HNB-GW sessions on IuH interface is greater than the high threshold.
threshold total-hnbgw-hnb-sessions

- **Clear condition:** Actual total number of HNB-HNB-GW sessions on IuH interfaces is less than the low threshold.

  If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

  Refer to the `threshold poll total-hnbgw-hnb-sessions` command to configure the polling interval and the `threshold monitoring hnbgw-service` command to enable thresholding for this value.

**Important:** To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshTotalHNBGWHnbSess` command in this mode.

**Example**

The following command configures the total number of HNB-GW-HNB sessions on IuH interfaces to a high threshold count of 10000 for a system using the Alert thresholding model:

```
threshold total-hnbgw-hnb-sessions 10000
```
threshold total-hnbgw-iu-sessions

Configures alarm or alert thresholds for the total number of subscriber sessions towards the Core Networks (CN) across all HNB-GW services over Iu interfaces (Iu-CS/Iu-PS interface) on a system.

**Product**
HNB-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
threshold total-hnbgw-iu-sessions high_thresh [ clear low_thresh ]
```

- **high_thresh**
  Default: 0 (Disabled)
  Specifies the high threshold for the total number of subscriber sessions towards CN across all HNB-GW services on a system that must be met or exceeded within the polling interval to generate an alert or alarm.
  `high_thresh` is an integer from 0 through 3000000. A value of 0 disables the threshold.

- **clear low_thresh**
  Default: 0 (Disabled)
  Specifies the low threshold for the total number of subscriber sessions towards CN across all services on a system that maintains a previously generated alarm condition. If the number of subscriber sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.
  `low_thresh` is an integer from 0 through 3000000. A value of 0 disables the threshold.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**

Use this command to monitor and set alarms or alerts when the total number of subscriber sessions towards CN across all HNB-GW services in the system is equal to or greater than the set limit. Alerts or alarms are triggered for the total number of subscriber sessions towards CN across all HNB-GW service on a system based on the following rules:

- **Enter condition:** Actual total number of subscriber sessions across all HNB-GW service on a system is greater than the high threshold.
- **Clear condition:** Actual total number of subscriber sessions across all HNB-GW service on a system is less than the low threshold.
If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval. Refer to the `threshold poll total-hnbgw-iu-sessions` command to configure the polling interval and the `threshold monitoring hnbgw-service` command to enable thresholding for this value.

**Important:** To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshTotalHNBGWIuSess` command in this mode.

**Example**

The following command configures the total number of subscriber sessions towards CN across all HNB-GW services to a high threshold count of 30000 for a system using the Alert thresholding model:

```
threshold total-hnbgw-iu-sessions 30000
```
threshold total-hnbgw-ue-sessions

Configures alarm or alert thresholds for the total number of UEs connected to an HNB-GW service across all the HNB-GW services in the system.

Product: HNB-GW
Privilege: Security Administrator, Administrator
Mode: Exec > Global Configuration configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

```
threshold total-hnbgw-ue-sessions high_thresh [ clear low_thresh ]
```

**high_thresh**

Default: 0 (Disabled)
Specifies the high threshold for the total number of UEs connected across all HNB-GW services on a system that must be met or exceeded within the polling interval to generate an alert or alarm. `high_thresh` is an integer from 0 through 4000000. A value of 0 disables the threshold.

**clear low_thresh**

Default: 0 (Disabled)
Specifies the low threshold for the total number of UEs connected to HNB-GW service across all HNB-GW services that maintains a previously generated alarm condition. If the number of UE sessions across all the services in a system, falls beneath the low threshold within the polling interval, a clear alarm will be generated.
`low_thresh` is an integer from 0 and 4000000. A value of 0 disables the threshold.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**

Use this command to monitor and set alarms or alerts when the total number of UEs connected to HNB-GW service across all HNB-GW services in the system is equal to or greater than the set limit. Alerts or alarms are triggered for the total number of UEs connected across all HNB-GW service on a system based on the following rules:

- **Enter condition:** Actual total number of UEs connected to HNB-GW service across all HNB-GW services on a system is greater than the high threshold.

- **Clear condition:** Actual total number of UEs connected to HNB-GW service across all HNB-GW services on a system is less than the low threshold.
Global Configuration Mode Commands (threshold ppp - url-blacklisting)

threshold total-hnbgw-ue-sessions

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval. Refer to the `threshold poll total-hnbgw-ue-sessions` command to configure the polling interval and the `threshold monitoring hnbgw-service` command to enable thresholding for this value.

**Important:** To enable an SNMP trap for monitoring this threshold use the `snmp trap enable ThreshTotalHNBGWUeSess` command in this mode.

**Example**

The following command configures the total number of UEs connected to HNB-GW service across all HNB-GW services to a high threshold count of 40000 for a system using the Alert thresholding model:

```
threshold total-hnbgw-ue-sessions 40000
```
threshold total-hsgw-sessions

Configures alarm or alert thresholds for the total number of HRPD Serving Gateway (HSGW) sessions across all services in the system.

Product
HSGW

Privilege
Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold total-hsgw-sessions high_thresh [ clear low_thresh ]

high_thresh
Default: 0
Specifies the high threshold for the number of HSGW sessions for all HSGW services that must be met or exceeded within the polling interval to generate an alert or alarm. high_thresh is an integer from 1 through 2500000. A value of 0 disables the threshold.

clear low_thresh
Default: 0
Specifies the low threshold for the number of HSGW sessions for all HSGW services that maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated. low_thresh is an integer from 0 and 2500000. A value of 0 disables the threshold.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Monitor and set alarms or alerts when the total number of HSGW sessions in the system is equal to or greater than the set limit. Alerts or alarms are triggered for HSGW sessions based on the following rules:

- **Enter condition:** Actual total number of HSGW sessions is greater than or equal to the high threshold.
- **Clear condition:** Actual total number of HSGW sessions is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval. Refer to the threshold poll command to configure the polling interval and the threshold monitoring command to enable thresholding for this value.
Example

The following command configures a total number of HSGW sessions high threshold count of \textit{500000} for a system using the Alert thresholding model:

\begin{verbatim}
threshold total-hsgw-sessions 500000
\end{verbatim}
threshold total-lma-sessions

Configures alarm or alert thresholds for the total number of Local Mobility Anchor (LMA) sessions across all services in the system.

Product
P-GW
SAEGW

Privilege
Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

```
threshold total-lma-sessions high_thresh [ clear low_thresh ]
```

- **high_thresh**
  Default: 0
  Specifies the high threshold number of LMA sessions for all LMA services that must be met or exceeded within the polling interval to generate an alert or alarm.
  `high_thresh` is an integer from 1 through 1500000. A value of 0 disables the threshold.

- **clear low_thresh**
  Default: 0
  Specifies the low threshold number of LMA sessions for all LMA services that maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.
  `low_thresh` is an integer from 0 through 1500000. A value of 0 disables the threshold.

- **Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Monitor and set alarms or alerts when the total number of LMA sessions in the system is equal to or greater than the set limit.

Alerts or alarms are triggered for LMA sessions based on the following rules:

- **Enter condition:** Actual total number of LMA sessions is greater than or equal to the high threshold.
- **Clear condition:** Actual total number of LMA sessions is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Example**

The following command configures a total number of LMA sessions high threshold count of 500000 for a system using the Alert thresholding model:

```
threshold total-lma-sessions 500000
```
threshold total-lns-sessions

Configures alarm or alert thresholds for the total number of L2TP Network Server (LNS) sessions in the system.

Product
PDSN
GGSN
HA

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

```
threshold total-lns-sessions high_thresh [ clear low_thresh ]
```

**high_thresh**

Default: 0
Specifies the high threshold number of total LNS sessions that must be met or exceeded within the polling interval to generate an alert or alarm.
`high_thresh` is an integer value from 0 through 4000000. A value of 0 disables the threshold.

**clear low_thresh**

Default: 0
Specifies the low threshold number of total LNS sessions that maintains a previously generated alarm condition. If the number of LNS sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.
`low_thresh` is an integer from 0 and 4000000. A value of 0 disables the threshold.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Monitor and set alarms or alerts when the total number of LNS sessions in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for the total number of LNS sessions based on the following rules:

- **Enter condition:** Actual total number of LNS sessions is greater than or equal to the high threshold.
- **Clear condition:** Actual total number of LNS sessions is less than the low threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Example**

The following command configures a total LNS session high threshold count of 10000 for a system using the Alert thresholding model:

```
threshold total-Ins-sessions 10000
```
threshold total-mme-sessions

Configures alarm or alert thresholds for the total number of Mobility Management Entity (MME) sessions across all the MME services in the system.

**Product**
MME

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration
`configure`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
threshold total-mme-sessions high_thresh [ clear low_thresh ]
```

- **`high_thresh`**
  - Default: 0 (Disabled)
  - Specifies the high threshold number of total MME sessions that must be met or exceeded within the polling interval to generate an alert or alarm.
  - `high_thresh` is an integer value from 0 through 2500000. A value of 0 disables the threshold.

- **`clear low_thresh`**
  - Default: 0 (Disabled)
  - Specifies the low threshold number of total MME sessions that maintains a previously generated alarm condition. If the number of MME sessions, across all the services in a system, falls beneath the low threshold within the polling interval, a clear alarm will be generated.
  - `low_thresh` is an integer from 0 and 2500000. A value of 0 disables the threshold.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**

Use this command to monitor and set alarms or alerts when the total number of MME sessions across all the MME services in the system is equal to or greater than the set limit.

Alerts or alarms are triggered for the total number of MME sessions based on the following rules:

- **Enter condition:** Actual total number of MME sessions is greater than or equal to the high threshold.
- **Clear condition:** Actual total number of MME sessions is less than the low threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the `threshold poll total-mme-sessions` command to configure the polling interval and the `threshold monitoring mme-service` command to enable thresholding for this value.
Example

The following command configures a total MME session high threshold count of 10000 for a system using the Alert thresholding model:

```
threshold total-mme-sessions 10000
```
threshold total-pdsn-sessions

Configures alarm or alert thresholds for the total number of Packet Data Serving Node (PDSN) sessions in the system.

**Product**

PDSN

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration

```
configure
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config) #
```

**Syntax**

```
threshold total-pdsn-sessions high_thresh [ clear low_thresh ]
```

- **high_thresh**
  - Default: 0
  - Specifies the high threshold number of total PDSN sessions that must be met or exceeded within the polling interval to generate an alert or alarm.
  - `high_thresh` is an integer from 0 through 2500000. A value of 0 disables the threshold.

- **clear**
  - **low_thresh**
  - Default: 0
  - Specifies the low threshold number of total PDSN sessions that maintains a previously generated alarm condition. If the number of PDSN sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.
  - `low_thresh` is an integer from 0 and 2500000. A value of 0 disables the threshold.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**

Monitor and set alarms or alerts when the total number of PDSN sessions in the system is equal to or greater than the set limit.

Alerts or alarms are triggered for the total number of PDSN sessions based on the following rules:

- **Enter condition:** Actual total number of PDSN sessions is greater than or equal to the high threshold.
- **Clear condition:** Actual total number of PDSN sessions is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Example**
The following command configures a total PDSN session high threshold count of 10000 for a system using the Alert thresholding model:

```
threshold total-pdsn-sessions 10000
```
threshold total-pgw-sessions

Configures alarm or alert thresholds for the total number of Packet Data Network Gateway (P-GW) sessions across all services in the system.

**Product**
P-GW
SAEGW

**Privilege**
Administrator

**Mode**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

```
[local] host_name(config) #
```

**Syntax**

```
threshold total-pgw-sessions high_thresh [ clear low_thresh ]
```

<table>
<thead>
<tr>
<th>high_thresh</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default: 0</td>
</tr>
<tr>
<td>Specifies the high threshold number of P-GW sessions for all P-GW services that must be met or exceeded within the polling interval to generate an alert or alarm.</td>
</tr>
<tr>
<td>high_thresh is an integer from 1 through 3000000. A value of 0 disables the threshold.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>clear low_thresh</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default: 0</td>
</tr>
<tr>
<td>Specifies the low threshold number of P-GW sessions for all P-GW services that maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.</td>
</tr>
<tr>
<td>low_thresh is an integer from 0 through 3000000. A value of 0 disables the threshold.</td>
</tr>
</tbody>
</table>

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**

Monitor and set alarms or alerts when the total number of P-GW sessions in the system is equal to or greater than the set limit.

Alerts or alarms are triggered for P-GW sessions based on the following rules:

- **Enter condition:** Actual total number of P-GW sessions is greater than or equal to the high threshold.
- **Clear condition:** Actual total number of P-GW sessions is less than the low threshold

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the threshold poll command to configure the polling interval and the threshold monitoring command to enable thresholding for this value.

**Example**

The following command configures a total number of P-GW sessions high threshold count of 500000 for a system using the Alert thresholding model:

```
threshold total-pgw-sessions 500000
```
threshold total-saegw-sessions

Configures alarm or alert thresholds for the total number of System Architecture Evolution Gateway (SAEGW) sessions across all services in the system.

Product
SAEGW

Privilege
Administrator

Mode
Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold total-saegw-sessions high_thresh [ clear low_thresh ]

high_thresh

Default: 0

Specifies the high threshold number of SAEGW sessions for all SAEGW services that must be met or exceeded within the polling interval to generate an alert or alarm.

high_thresh is an integer from 1 through 3000000. A value of 0 disables the threshold.

clear low_thresh

Default: 0

Specifies the low threshold number of SAEGW sessions for all SAEGW services that maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.

low_thresh is an integer from 0 through 3000000. A value of 0 disables the threshold.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Monitor and set alarms or alerts when the total number of SAEGW sessions in the system is equal to or greater than the set limit.

Alerts or alarms are triggered for SAEGW sessions based on the following rules:

- **Enter condition:** Actual total number of SAEGW sessions is greater than or equal to the high threshold.

- **Clear condition:** Actual total number of SAEGW sessions is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.

**Example**

The following command configures a total number of SAEGW sessions high threshold count of 500000 for a system using the Alert thresholding model:

```
threshold total-saegw-sessions 500000
```
threshold total-sgsn-pdp-sessions

Configures alarm or alert thresholds for the total number of PDP contexts for all Serving GPRS Support Node (SGSN) sessions in the system.

Product
SGSN

Privilege
Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:
[local]\host_name(config)#

Syntax

threshold total-sgsn-pdp-sessions high_thresh [ clear low_thresh ]

| high_thresh
Default: 0
Specifies the high threshold number of total PDP contexts per SGSN session for all SGSN services that must be met or exceeded within the polling interval to generate an alert or alarm.
high_thresh is an integer from 1 through 4000000. A value of 0 disables the threshold.

| clear low_thresh
Default: 0
Specifies the low threshold number of total PDP contexts per SGSN session for all SGSN services that maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.
low_thresh is an integer from 0 through 4000000. A value of 0 disables the threshold.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Monitor and set alarms or alerts when the total number of SGSN sessions in the system is equal to or greater than the set limit.
Alerts or alarms are triggered for SGSN sessions based on the following rules:
• Enter condition: Actual total number of PDP contexts is greater than or equal to the high threshold.
• Clear condition: Actual total number of PDP contexts is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.
Refer to the threshold poll command to configure the polling interval and the threshold monitoring command to enable thresholding for this value.
Example

The following command configures a total number of PDP contexts per SGSN session high threshold count of 10000 for a system using the Alert thresholding model:

```
threshold total-sgsn-pdp-sessions 10000
```
threshold total-sgsn-sessions

Configures alarm or alert thresholds for the total number of SGSN sessions in the system.

Product
SGSN

Privilege
Administrator

Mode
Exec > Global Configuration

configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

threshold total-sgsn-sessions high_thresh [ clear low_thresh ]

**high_thresh**

Default: 0
Specifies the high threshold number of total SGSN sessions for all SGSN services that must be met or exceeded within the polling interval to generate an alert or alarm.

**low_thresh** is an integer from 1 through 2000000. A value of 0 disables the threshold.

**clear low_thresh**

Default: 0
Specifies the low threshold number of total SGSN sessions for all SGSN services that maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.

**low_thresh** is an integer from 0 through 2000000. A value of 0 disables the threshold.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Monitor and set alarms or alerts when the total number of SGSN sessions in the system is equal to or greater than the set limit.

Alerts or alarms are triggered for SGSN sessions based on the following rules:

- **Enter condition:** Actual total number of SGSN sessions is greater than or equal to the high threshold.
- **Clear condition:** Actual total number of SGSN sessions is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the threshold poll command to configure the polling interval and the threshold monitoring command to enable thresholding for this value.

Example
The following command configures a total number of SGSN sessions high threshold count of 10000 for a system using the Alert thresholding model:

```
threshold total-sgsn-sessions 10000
```
**threshold total-sgw-sessions**

Configures alarm or alert thresholds for the total number of Serving Gateway (S-GW) sessions across all services in the system.

**Product**
S-GW

**Privilege**
Administrator

**Mode**
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
threshold total-sgw-sessions high_thresh [ clear low_thresh ]
```

- **high_thresh**
  
  Default: 0
  
  Specifies the high threshold number of S-GW sessions for all S-GW services that must be met or exceeded within the polling interval to generate an alert or alarm. 
  
  `high_thresh` is an integer from 1 through 3000000. A value of 0 disables the threshold.

- **clear low_thresh**

  Default: 0
  
  Specifies the low threshold number of S-GW sessions for all S-GW services that maintains a previously generated alarm condition. If the number of sessions falls beneath the low threshold within the polling interval, a clear alarm will be generated.
  
  `low_thresh` is an integer from 0 through 3000000. A value of 0 disables the threshold.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**

Monitor and set alarms or alerts when the total number of S-GW sessions in the system is equal to or greater than the set limit.

Alerts or alarms are triggered for S-GW sessions based on the following rules:

- **Enter condition:** Actual total number of S-GW sessions is greater than or equal to the high threshold.
- **Clear condition:** Actual total number of S-GW sessions is less than the low threshold.

If a trigger condition occurs within the polling interval, the alert or alarm will not be generated until the end of the polling interval.

Refer to the `threshold poll` command to configure the polling interval and the `threshold monitoring` command to enable thresholding for this value.
Example

The following command configures a total number of S-GW sessions high threshold count of 500000 for a system using the Alert thresholding model:

```
threshold total-sgw-sessions 500000
```
threshold tpo-dns-failure

The Traffic Performance Optimization (TPO) in-line service is not supported in this release.
threshold tpo-low-compression-gain

The Traffic Performance Optimization (TPO) in-line service is not supported in this release.
threshold tpo-rto-timeout

The Traffic Performance Optimization (TPO) in-line service is not supported in this release.
**timestamps**

Enables or disables the generation of a timestamp in response to each commands entered. The timestamp does not appear in any logs as it is a CLI output only. This command affects all future CLI sessions. Use the `timestamps` command in the Exec Mode to change the behavior for the current CLI session only.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

```
configure
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
timestamps
```

```
no timestamps
```

Disables generation of timestamps for each command entered. When omitted, the output of a timestamp for each entered command is enabled.

**Usage**

Enable the timestamps when logging a CLI session on a remote terminal such that each command will have a line of text indicating the time when the command was entered.

**Example**

```
timestamps
```

```
no timestamps
```
**upgrade limit**

Configures upgrade session limits that trigger when the system may execute the software upgrade.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration

**configure**

Entering the above command sequence results in the following prompt:

```
[local] host_name(config)#
```

**Syntax**

```
upgrade limit [ time session_life ] [ usage session_num ]
```

- **upgrade limit**
  This command issued with no keywords sets all parameters to their defaults.

- **time session_life**
  Default: 120
  Defines the maximum number of minutes that a session may exist on the system undergoing a software upgrade, before it is terminated by the system. As individual user sessions reach this lifetime limit, the system terminates the individual session(s). The lifetime limit must be an integer ranging from 1 through 1440.

- **usage session_num**
  Default: 100
  This keyword defines a low threshold limit of sessions running either on a packet processing card or system-wide. When a software upgrade is invoked, this parameter applies to the entire system. When the threshold is crossed (when the number of sessions on the packet processing card or system is less than this value), the remaining sessions on the card or system are terminated allowing the upgrade to begin. The remaining sessions on the packet processing card or system are terminated regardless of their session life. The session limit must be an integer from 0 through 6000.

**Usage**

Use this command to configure upgrade session limits that trigger the system to begin executing the software upgrade.

**Important:** This command is not supported on all platforms.

**Important:** Software Patch Upgrades are not supported in this release.
Example

The following command sets the number of minutes a session can exist to 200, and the minimum number of sessions that may exist before terminating them to 50:

```
upgrade limit time 200 usage 50
```
url-blacklisting database

This command configures URL Blacklisting database directory parameters.

Product
CF

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration
configure

Entering the above command sequence results in the following prompt:

[local]host_name(config)#

Syntax

url-blacklisting database { directory path path | max-versions max_versions | override file file_name }

default url-blacklisting database { directory path | max-versions | override file }

- **default**
  Configures this command with the default settings.

- **directory path path**
  Specifies the path to the directory to be used for storing URL Blacklisting databases.
  *path* must be an alphanumeric string of 1 through 255 characters.
  Default: /flash/bl

- **max-versions max_versions**
  Specifies the maximum number of URL Blacklisting database versions to be maintained in the URL Blacklisting database directory path with the base file name specified by the URL Blacklisting database override file.
  *max_versions* must be an integer from 0 through 3.
  Default: 0

- **override file file_name**
  Specifies the URL Blacklisting database override file name.
  *file_name* must be in *name.extension* format. For example, *abc.bin*.
  And, must be an alphanumeric string of 1 through 10 characters.
  Default: optblk.bin

Usage

Use this command to configure URL Blacklisting database directory parameters.

Example
The following command configures the maximum number of URL Blacklisting database versions to be maintained to 3:

```
url-blacklisting database max-versions 3
```
### wsg-lookup

Enters the WSG lookup priority list configuration mode for site-to-site tunnels.

**Product**

WSG

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration

```
configure
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config)#
```

**Syntax**

```
wsg-lookup
```

**Usage**

Use this command to enter the WSG lookup priority list configuration mode for site-to-site tunnels.

**Examples**

```
wsg-lookup
```
Chapter 146
GPRS Service Configuration Mode Commands

The GPRS Service Configuration Mode is used within the context configuration mode to define the criteria the SGSN needs to operate within a GPRS network. The GPRS Service works with other services, such as SGSN GPRS Tunneling Protocol (see SGTP Service Configuration Mode Commands) and Mobile Application Part (see MAP Service Configuration Mode Commands), to handle communication parameters required to work with other network entities such as the base station subsystem (BSS).

Exec > Global Configuration > Context Configuration > GPRS Service Configuration

configure > context context_name > gprs-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-gprs-service)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
accounting

Defines the accounting context name and enables/disables specific types of CDR generation for the accounting in the GPRS service.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > GPRS Service Configuration

configure > context context_name > gprs-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-gprs-service)#

Syntax

accounting { cdr-types { mcdr | scdr | sms { mo-cdr | mt-cdr } | lcs { mt-cdr | mo-cdr } | smbmscdr } + | context cntx_name }

default accounting cdr-types

no accounting { cdr-types | context }

default

Returns the system to default CDR generation which includes:

• M-CDR
• S-CDR
• SMS CDRs
• LCS CDRs
• SMBMS CDR

no

Disables all CDR types.

cdr-types { mcdr | scdr | sms { mo-cdr | mt-cdr } | lcs { mt-cdr | mo-cdr } | smbmscdr }

Default: all types enabled.

Defines the types of CDRs to be generated within the specified GPRS service for accounting:

• mcdr: Enables generation of M-CDRs.
• scdr: Enables generation of S-CDRs.
• sms: Enables generation of SMS-type CDRs based on one of the following:
  • mo-cdr: SMS CDRs originates from the mobile.
• mt-cdr: SMS CDRs terminates at the mobile.
• smbmscdr: This CDR type is currently under development and should not be included in configuration for this release.
• lcs: Enables the generation of LCS CDRs, based on:
  • mt-cdr: Mobile terminated location request CDR
  • mo-cdr: Mobile originated location request CDR

This symbol indicates that more than one keyword can be used and repeated. This enables you to include more than one type of CDR selection in a single command.

context cntx_name

Specifies an accounting context to be associated with the GPRS service.
cntx_name: Define a string of 1 to 79 alphanumeric characters.

Usage

Use this command to define the type of CDRs to generate for GPRS service. By default all types of CDRs are generated. Note that change of this configuration will be applied to new calls and/or to new PDP contexts only.
By default, the generation of all CDR types is enabled.

Example

The following command configures the system to generate only M-CDRs for accounting in the current GPRS service:

```
accounting cdr-types mcdr
```
admin-disconnect-behavior

This command defines some of the actions the SGSN will take during an Admin-Disconnect procedure.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > GPRS Service Configuration
configure > context context_name > gprs-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-gprs-service)#

Syntax

admin-disconnect-behavior { clear-subscription | detach-type { reattach-not-required | reattach-required } }

default admin-disconnect-behavior { clear-subscription | detach-type }

clear-subscription

Including this keyword in the configuration instructs the SGSN to clear subscriber contexts and the subscription data database whenever the clear subscribers all command is issued (from the Exec mode) for attached subscribers. As well, the SGSN will issue an appropriate Map-Purge-MS-Req to the HLR if needed.
Default: disabled

detach-type

Including this keyword defines which type of detach instruction to include in the Detach-Request message during an Admin-Disconnect procedure. One of the following options must be included when this command is entered:

• reattach-not-required
• reattach-required

Default: reattach-required

default

Including the default keyword in the command, instructs the SGSN to use the default value for the specified parameter.

no

Returns the SGSN to the default where this clear function is disabled
Usage

Using the `clear subscribers all` command (in the Exec Mode) will clear subscriber contexts and the subscription data database, and if needed, issue an appropriate Map-Purge-MS-Req to the HLR. Include the `clear-subscription` keyword with this command configuration to ensure that more than attached MM-context and active PDP-contexts are cleared when the clear `subscribers all` command is issued for attached subscribers.

To clear subscription data for detached subscribers, refer to the `sgsn clear-detached-subscriptions` command described in the Exec mode chapter.

Including the `detach-type` keyword with this command instructs the SGSN to include either a ‘reattach-required’ or a ‘reattach-no-required’ instruction in the Detach-Request message.

Example

Enable the clearing function so that subscription data is cleared from the HLR database:

```
admin-disconnect-behavior clear-subscription
```
associate

Associates or disassociates supportive services and policies, such as an Evolved GPRS Tunnelling Protocol (eGTP) service or a DSCP marking template with this GPRS service configuration.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > GPRS Service Configuration

```
configure > context context_name > gprs-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-gprs-service)#
```

**Syntax**

```
associate { { camel-service service_name [ context context_name ] | dscp-template downlink dscp_template_name | egtp-service egtp_svc_name [ context context_name ] | gs-service gs_svc_name [ context context_name ] | hss-peer-service hss_svc_name [ context context_name ] | location-service loc_name [ context context_name ] | map-service map_svc_name [ context context_name ] | network-global-mme-id-mgmt-db | sgtp-service sgtp_svc_name [ context context_name ] | tai-mgmt-db database_name }

no associate { camel-service | dscp-template downlink | egtp-service | gs-service | hss-peer-service | location-service | map-service | network-global-mme-id-mgmt-db | sgtp-service | tai-mgmt-db }
```

**no**

Disassociates a previously associated service, DSCP marking template or management database with this GPRS service.

```
context ctx_name
```

Identifies an existing context name in which the named service is configured. If this keyword is omitted, the named service must exist in the same context as the GPRS service.

**camel-service camel_svc_name**

Associates a CAMEL service with this GPRS service.

**camel_svc_name** specifies the name for a configured CAMEL service to associate with the GPRS service. Enter an alphanumeric string of 1 to 63 characters.

**dscp-template downlink template_name**

Associates a DSCP template with the GPRS service.

**template_name** specifies a configured DSCP marking template to associate with this GPRS service. Enter an alphanumeric string of 1 to 64 characters.
GPRS Service Configuration Mode Commands

**egtp-service egtp_svc_name**

Associates an eGTP service with GPRS service.

*egtp_svc_name* specifies the name for a configured eGTP service to associate with this GPRS service.

Enter an alphanumeric string of 1 to 63 characters.

The eGTP service is created with the **egtp-service** command in the *Context Configuration Mode Commands* chapter. The eGTP service provides eGTP-C protocol interface support between the SGSN and EPS nodes. For more information on the eGTP service and the supported interface type(s), refer to the *eGTP Service Configuration Mode Commands* chapter.

**Important:** Only one eGTP service can be associated with a GPRS service. The eGTP service should be configured prior to issuing this command.

**gs-service gs_svc_name**

Associates a Gs service with this GPRS service.

*gs_svc_name* specifies the name for a configured Gs service to associate with the GPRS service. Enter an alphanumeric string of 1 to 63 characters.

The Gs service is created with the **gs-service** command in the *Context Configuration Mode Commands* chapter. The Gs service provides Gs interface support between the SGSN and MSC/VLR nodes. For more information on the Gs service and the supported interface type, refer to the *Gs Service Configuration Mode Commands* chapter.

**Important:** Only one Gs service can be associated with a GPRS service. The Gs service should be configured prior to issuing this command.

**hss-peer-service hss_svc_name**

Associates an HSS peer service with this GPRS service.

*hss_svc_name* specifies the name for a configured HSS peer service to associate with this GPRS service.

Enter an alphanumeric string of 1 to 63 characters.

The HSS peer service provides S6d and S13-prime interface support via the Diameter protocol between the GPRS and an HSS (S6d) or EIR (S13-prime). For more information about the HSS peer service, refer to the **hss-peer-service** command in the *Context Configuration Mode Commands* chapter and the *HSS Peer Service Configuration Mode Commands* chapter.

**Important:** Only one HSS peer service can be associated to a service in this release. The HSS peer service should be configured prior to issuing this command.

**location-service loc_svc_name**

**map-service map_svc_name**

Associates a location service with this GPRS service.

*loc_svc_name* specifies the name for a pre-configured location service to associate with the GPRS service.

Enter an alphanumeric string of 1 to 63 characters.

The location service is created with the **location-service** command in the *Context Configuration Mode Commands* chapter. For more information on the location services, refer to the *Location Services Configuration Mode* section.
**Important:** Only one MAP service can be associated with a GPRS service. The MAP service should be configured prior to issuing this command.

```
associate
```

network-global-mme-id-mgmt-db

Associates the configured global MME ID management database with the GPRS service. This enables operators to associate a single list of MME Group IDs for use in GPRS to E-UTRAN handovers on the S4-SGSN. The global MME ID management database is configured in the LTE Policy Configuration Mode using the network-global-mme-id-mgmt-db command.

This command is available only if the SGSN S4 Interface license is enabled on the SGSN.

```
associate network-global-mme-id-mgmt-db
```

sgtp-service sgtp_svc_name

Associates an SGTP service with this GPRS service. sgtp_svc_name specifies the name for a configured SGTP service to associate with the GPRS service. Enter an alphanumeric string of 1 to 63 characters.

The SGSN GPRS Tunneling Protocol (SGTP) service manages the configuration of the GTP-C and GTP-U related parameters. For more information on the SGTP service, refer to the sgtp-service command in the Context Configuration Mode Commands chapter and/or the SGTP Service Configuration Mode Commands chapter.

**Important:** Only one SGTP service can be associated with a GPRS service. The SGTP service should be configured prior to issuing this command. When co-locating an SGSN and MME, the GPRS Service cannot be associated with the same SGTP service that is used by the MME.

```
associate sgtp-service sgtp_svc_name
```

tai-mgmt-db database_name

Associates this GPRS service with a pre-configured TAI Management Database. database_name specifies the name of a pre-configured TAI Management Database to associate with the SGSN service as an alphanumeric string of 1 through 64 characters. For more information on subscriber maps, refer to the tai-mgmt-db command in the LTE Policy Configuration Mode Commands chapter and the LTE TAI Management Database Configuration Mode Commands chapter.

This command is available only if the SGSN S4 Interface license is enabled on the SGSN.

```
associate tai-mgmt-db database_name
```

**Usage**

Use this command to associate a pre-configured service and/or DSCP marking template and/or management database with this GPRS service. The command can be repeated as necessary to configure associations for all desired services/templates/databases.

**Caution:** This is a critical configuration. The GPRS service cannot be started without this configuration. Any change to this configuration would lead to restarting the GPRS service. Removing or disabling this configuration will stop the GPRS service.

**Example**

The following command associates a previously-configured eGTP service called egtp1 in the dst_ctx context to this GPRS service:

```
associate egtp-service egtp1 context dst_ctx
```
The following command disassociates a MAP service called `map1` that was previously associated with this GPRS service:

```
no associate map-service egtp1
```

The following command associates an HSS peer service called `hss1`, previously-configured in the same context as the GPRS service, to this GPRS service:

```
associate hss-peer-service hss1
```

The following command associates a previously-configured DSCP marking template called `dscp-temp1` to this GPRS service:

```
associate dscp-template downlink dscp-temp1
```
associate-dscp-template

Identifies a DSCP template to be associated with the GPRS service.

**Important:** This command is used only in Releases 12.0 and 12.2. For Release 14.0 refer to the `associate` command.

**Important:** This command can be used before the associated DSCP template instance is created and configured but care should be used to match the template names.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > GPRS Service Configuration

```
configure > context context_name > gprs-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-gprs-service)#
```

**Syntax**

```
associate-dscp-template downlink template_name

no associate-dscp-template downlink
```

**Usage**

Use this command to associate DSCP templates with this GPRS service. A single template can be associated with multiple GPRS services.

**Related commands:**
- The `dscp-template` command in the SGSN Global configuration mode creates / deletes an instance of a template. This command also provides access to the mode containing all the configuration commands used to define DSCP settings for the control packets for the Iu interface and the control and data packets for the Gb interface (see the *DSCP Template Configuration Mode Commands* section).
To check the list of DSCP templates configured, use the \texttt{show sgsn-mode} command documented in the \textit{Exec Mode Commands} section.

\textbf{Example}

The following command associates the template with DSCP settings for traffic going through one of the SGSNs located in Paris mobile network:

\begin{verbatim}
associate-dscp-template dscp-template-paris3
\end{verbatim}
**associate-service**

Identifies services to be associated with the GPRS Service.

**Important:** This command is used only in Releases 12.0 and 12.2. For Release 14.0 refer to the `associate` command.

**Important:** This command can be used before the associated service instance is created and configured but care should be used to match the service names.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > GPRS Service Configuration

```
configure > context context_name > gprs-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-gprs-service)#
```

**Syntax**

```
[ no ] associate-service { gs name | map name | sgtp name } [ context ctxt_name ]
```

- **no**
  Removes the service association definition from the configuration.

- **gs name**
  Specifies the Gs service configuration to associate with this GPRS service.
  `name` must be a string of 1 to 63 alphanumeric characters with no spaces.

- **map name**
  Specifies the MAP service configuration to associate with this GPRS service.
  `name` must be a string of 1 to 63 alphanumeric characters with no spaces.

- **sgtp name**
  Specifies the SGTP service configuration to associate with this GPRS service.
  `name` must be a string of 1 to 63 alphanumeric characters with no spaces.

- **context ctxt_name**
  Defines the context in which the service was created.
  `ctxt_name` must be a string of 1 to 63 alphanumeric characters with no spaces.
Usage

Use this command to associate other services, that have been or will be configured, to this GPRS service.

Example

The following command associates Gs service gs1 with this GPRS service.

```
associate-service gs gs1 context sgsn2
```
cc profile

Configures the charging characteristic (CC) profile index properties.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > GPRS Service Configuration
configure > context context_name > gprs-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-gprs-service)#

Syntax

[ no ] cc profile index { buckets number | interval time | tariff time1 mins hours [ time2 mins hours [ time3 mins hours [ time4 mins hours ] ] ] | volume { downlink octets | uplink octets | total octets } }

default cc profile index

no

Removes the a specific charging characteristics configuration definition.

default

Resets the charging characteristics to system defaults.

index

Configures a profile index for the parameter to be specified. index can be configured to any integer value from 0 to 15.

Important: 3GPP standards suggest that profile index values of 1, 2, 4, and 8 be used for hot billing, flat rate billing, prepaid billing and normal billing, respectively. A single charging characteristics profile can contain multiple behavior settings.

buckets number

Default: 4
Specifies the number of statistics container changes due to QoS changes or tariff time that can occur before an accounting record should be closed.
number can be configured to any integer value from 1 through 4.

interval time

time is measured in seconds and can be configured to any integer value from 60 to 40,000,000.
### GPRS Service Configuration Mode Commands

#### cc profile

```plaintext
tariff time1 mins hours time2 mins hours time3 mins hours time4 mins hours
```

Specifies time-of-day time values to close the current statistics container (but not necessarily the accounting record). Six different tariff times may be specified. If less than six times are required, the same time can be specified multiple times.

**Important:** The system assumes that the billing system uses the day/date to determine if the statistics container represents an actual tariff period.

For each of the different tariff times, the following parameters must be configured:

- **mins**: The minutes of the hour, an integer value from 0 to 59.
- **hours**: The hour of the day, an integer value from 0 to 23.

```plaintext
volume { downlink vol_down_octets uplink vol_up_octets | total total_octets }
```

Specifies the downlink, uplink, and total volumes that must be met before closing a CDR.

- **vol_down_octets**: Measured in octets; can be configured to any integer value from 100,000 to 4,000,000,000.
- **vol_up_octets**: Measured in octets; can be configured to any integer value from 100,000 to 4,000,000,000.
- **total_octets**: The total traffic volume (up and downlink) measured in octets; can be configured to any integer value from 100,000 to 4,000,000,000.

**Usage**

Charging characteristics consist of a profile index and behavior settings. This command configures profile indexes for the SGSN’s charging characteristics. The SGSN supports up to 16 profile indexes. This command works in conjunction with the `cc-sgsn` command located in the APN configuration mode that dictates which CCs should be used for subscriber PDP contexts.

**Example**

The following command configures a profile index of 10 for tariff times of 7:00 AM and 7:30 PM:

```
cr profile 10 tariff time1 0 7 time2 30 19
```
check-imei

This command configures the action the SGSN will take if the route towards the EIR is down.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > GPRS Service Configuration
configure > context context_name > gprs-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-gprs-service)#

Syntax

check-imei { gf-failure-action | gf-timeout-action } { continue | reject }
default check-imei { gf-failure-action | gf-timeout-action }

default
Resets the default function to reject the Attach.

gf-failure-action
Coupled with either continue or reject, this keyword instructs the SGSN to take action if a valid EIR configuration exists under the MAP service and if the EIR is temporarily unreachable due to associated DPC/SSN inaccessible/out-of-service.

gf-timeout-action
Coupled with either continue or reject, this keyword instructs the SGSN to take action if a valid EIR configuration exists under the MAP service and the route to the EIR is available, but no response is received from the EIR.

continue
Instructs the SGSN to continue the Attach process.

reject
Instructs the SGSN to reject the Attach process.

Usage

Typically, the Attach process will be continued when there is an IMEI check timeout based on the configuration under the SGSN service configuration and/or the GPRS service configuration. But this works only if the route towards the EIR is UP and the IMEI request timer expires. This command configures the SGSN to allow the Attach process to continue in the case the route towards the EIR is down, that is the DPC / SSN is out-of-service.
Example

Use the following command to reset the default and reject Attach:

```
default check-imei gf-failure-action
```
check-imei-timeout-action

This command has been deprecated.
ciphering-algorithm

This command configures the priority, ordering, for the use of the GPRS encryption ciphering algorithms.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > GPRS Service Configuration

`configure > context context_name > gprs-service service_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-gprs-service)#
```

Syntax

```
ciphering-algorithm { negotiation-failure-action { reject [ failure-code cause_code ] | use-geo0 } priority priority [ algorithm ] } 
default ciphering-algorithm priority priority
```

default

Returns the system ciphering-algorithm priority to the default of GEA0 - which means that no ciphering will be done.

```
negotiation-failure-action { reject [ failure-code cause_code ] | use-geo0 }
```

This set of keywords configure the SGSN's action if there is not a match between the MS and SGSN ciphering algorithm configurations.

*reject*: Instructs the SGSN to reject a call when the ciphering algorithms do not match.

*failure-code cause_code*: Instructs the SGSN to include a GMM cause code in the Reject message. Enter an integer from 2 to 111; default code is 14 (GPRS services not allowed in this PLMN). Refer to the GMM failure cause codes listed below (information has been taken from section 10.5.5.14 of the 3GPP TS 124.008 v7.2.0 R7):

- 2 - IMSI unknown in HLR
- 3 - Illegal MS
- 6 - Illegal ME
- 7 - GPRS services not allowed
- 8 - GPRS services and non-GPRS services not allowed
- 9 - MSID cannot be derived by the network
- 10 - Implicitly detached
- 11 - PLMN not allowed
- 12 - Location Area not allowed
- 13 - Roaming not allowed in this location area
 ciphering-algorithm

- 14 - GPRS services not allowed in this PLMN
- 15 - No Suitable Cells In Location Area
- 16 - MSC temporarily not reachable
- 17 - Network failure
- 20 - MAC failure
- 21 - Synch failure
- 22 - Congestion
- 23 - GSM authentication unacceptable
- 40 - No PDP context activated
- 48 to 63 - retry upon entry into a new cell
- 95 - Semantically incorrect message
- 96 - Invalid mandatory information
- 97 - Message type non-existent or not implemented
- 98 - Message type not compatible with state
- 99 - Information element non-existent or not implemented
- 100 - Conditional IE error
- 101 - Message not compatible with the protocol state
- 111 - Protocol error, unspecified

**use-geo0**: Instructs the SGSN to honor the Attach/RAU Request without ciphering (geo0). This is the default action for negotiation failure.

**priority priority algorithm**

Defines the priority, order of use, for the ciphering algorithm.

**priority**: Must be an integer from 1 to 4.

**algorithm**

Identifies the algorithm to be matched to the priority. Options include:
- gea0 - No ciphering
- gea1 - GPRS Encryption Algorithm - GEA1
- gea2 - GPRS Encryption Algorithm - GEA2
- gea3 - GPRS Encryption Algorithm - GEA3

**Usage**

Use this command to specify the order (priority) of usage for the GPRS encryption algorithms. All of the GPRS encapsulation algorithms use a 64-bit key derived from a common mechanism: the mobile receives a random challenge, then the SIM calculates an authentication signature and an encryption key.

Also use this command to define the action to be taken if there is not a match between the MS and the SGSN ciphering algorithm configurations.

**Example**

The following command sets no ciphering to be used after two encryption algorithms have been used:
ciphering-algorithm priority 3 gea0

The following command configures the SGSN to reject calls if the ciphering algorithm configurations don’t match:

ciphering-algorithm negotiation-failure-action reject
dns israu-mcc-mnc-encoding

Configures either decimal or hexadecimal format for the MCC and MNC values in the DNS query.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > GPRS Service Configuration
classify > context context_name > gprs-service service_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-gprs-service)#
```

**Syntax**

dns israu-mcc-mnc-encoding { decimal | hexadecimal }

default dns israu-mcc-mnc-encoding

default
Resets the SGSN to send the MCC and MNC values in decimal format for DNS queries.

decimal
Default.
Instructs the SGSN to send the MCC and MNC in decimal format in the DNS query.

hexadecimal
Instructs the SGSN to send the MCC and MNC in hexadecimal format in the DNS query.

**Usage**

Use this command to determine the type of encoding for the MCC and MNC to be included in the DNS query. For example:
In decimal, the MNC/MCC in a DNS query would appear like:

```
rac0017.lac42e3.mnc310.mcc722.gprs
```

In hexadecimal, the MNC/MCC in a DNS query would appear like:

```
rac0017.lac42e3.mnc0136.mcc02d2.gprs
```

**Example**

Use hexadecimal values for the MCC/MNC in the DNS query.

dns israu-mcc-mnc-encoding hexadecimal
end

Exits the current configuration mode and returns to the Exec mode.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax
dend

Usage
Return to the Exec mode.
exit

Exits the current configuration mode and returns to the previous configuration mode.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Return to the context configuration mode.
gmm

`gmm` actually provides a set of commands used to define the GPRS mobility management parameters for the SGSN service.

**Important:** The `gmm` commands can be repeated as needed to set each timer.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > GPRS Service Configuration

`configure > context context_name > gprs-service service_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-gprs-service)##
```

**Syntax**

```plaintext

   default gmm { attach ptmsi-signature-mismatch | ciph-gmm-msg-from-unknown-ms | mobile-reachable-timeout | implicit-detach-timeout secs | negotiate-t3314-timeout | purge-timeout | T3302-timeout | T3312-timeout | T3313-timeout | T3350-timeout | T3360-timeout | T3370-timeout | trau-timeout }

   no gmm  | negotiate-t3314-timeout
```

**Default**

Disables the specified function or resets the specified timer to system defaults.

**No**

Removes the specified GMM definition from the configuration.

**accept-procedure [ new-tlli | old-tlli ]**

Default: new-tlli

This keyword enables the use of either a new TLLI (temporary logical link identifier) or an old TLLI for attach-accept or RAU-accept messages sent by the SGSN to the MS during related procedures.
attach ptmsi-signature-mismatch send-reject failure-code cause_code

Default: disabled
This keyword enables the SGSN to validate the P-TMSI signature, present in the Attach Request, against the PTMSI-SIGNATURE stored at the SGSN. The SGSN then sends an Attach Reject to the MS if the PTMSI-SIGNATURE does not match.
The P-TMSI signature validation functionality only works if the feature is enabled. But even if it is enabled, the feature does not validate in the following situations:
- when the PTMSI-SIGNATURE is absent from the 2G Attach Request.
- if the first subscriber being in DETACHED state or is purged with FREEZE-PTMSI. In both the scenarios PTMSI-SIGNATURE cannot be validated.
- when the 2G subscriber(MS2) attaches with the same P-TMSI and a different P-TMSI_Signature as previously attached 2G subscriber (MS1), both the subscriber profiles are cleared from the system.
  This is relevant where the old RAI for MS-2 is the same as the current RAI for MS-1.
Optional, a GMM failure cause_code can be configured to include in the Attach Reject if one is sent.
Refer to the GMM failure cause codes listed below (information has been taken from section 10.5.5.14 of the 3GPP TS 124.008 v7.2.0 R7):
- 2 - IMSI unknown in HLR
- 3 - Illegal MS
- 6 - Illegal ME
- 7 - GPRS services not allowed
- 8 - GPRS services and non-GPRS services not allowed
- 9 - MSID cannot be derived by the network
- 10 -Implicitly detached
- 11 - PLMN not allowed
- 12 - Location Area not allowed
- 13 - Roaming not allowed in this location area
- 14 - GPRS services not allowed in this PLMN
- 15 - No Suitable Cells In Location Area
- 16 -MSC temporarily not reachable
- 17 - Network failure
- 20 - MAC failure
- 21 - Synch failure
- 22 - Congestion
- 23 - GSM authentication unacceptable
- 40 - No PDP context activated
- 48 to 63 - retry upon entry into a new cell
- 95 - Semantically incorrect message
- 96 - Invalid mandatory information
- 97 - Message type non-existent or not implemented
- 98 - Message type not compatible with state
GPRS Service Configuration Mode Commands

- 99 - Information element non-existent or not implemented
- 100 - Conditional IE error
- 101 - Message not compatible with the protocol state
- 111 - Protocol error, unspecified

ciph-gmm-msg-from-unknown-ms { detach | ignore }

Configures how the SGSN will behave when it receives a ciphered GMM message from an unknown MS.

detach - Instructs the SGSN to send a Detach message to the MS.
ignore - Instructs the SGSN to send an Ignore (drop) message to the MS.
Default: ignore

implicit-detach-timeout secs

Specifies the implicit detach timer (IDT) value for the 2G ISR implicit detach procedure on the network side (see ISR -- Idle Mode Signaling Reduction on the S4-SGSN feature chapter in the SGSN Administration Guide for additional timer usage details).
The IDT is configurable from release 15.0 onwards and it is only applicable to 2G ISR activated calls. If ISR is not activated on a 2G call then the subscriber is detached soon after expiry of the mobile reachability timer (MNR) timer.

secs must be an integer from 240 to 86400 and the default value is 3600.

mobile-reachable-timeout mins

Default: 58 minutes
Specifies the timeout value for the mobile reachability timer (MNR). This timer is used with the IDT timer described above.

mins must be an integer from 4 to 1440.

negotiate-T3314-timeout secs

Set the number of seconds for the T3314-timeout ready timer value. Value sent out from SGSN so MS can negotiate ready timer.

secs must be an integer from 0 to 11160. Default is 44 seconds.

- If the MS does not send the ready timer in the Attach/RAU request, then the SGSN sends this T3314-timeout (ready timer) value.
- If the MS sends the requested value of the ready timer in the Attach/RAU Request, and if the requested value is less than or equal to the value of the negotiate-T3314-timeout timer, then the SGSN sends Att/RAU Accept with the requested T3314 value.
- If the MS sends the requested value of the ready timer in the Attach/RAU Request, and if the requested value is greater than the value of the negotiate-T3314-timeout timer, then the SGSN sends Att/RAU Accept with the negotiate-T3314-timeout value.

**Important:** This is the only GMM timer that can be disabled by entering no at the beginning of the command

**syntax:** no gmm negotiate-t3314-timeout

By disabling negotiation of the T3314-timeout value, if the MS sends the requested value of the ready timer in the Att/RAU Request, then the SGSN sends the T3314-timeout value in the Att/RAU Accept.
**paging-failure-action downlink-data-lockout-timer**  
*seconds [ repeat number_repeats ]*

Default: 1000 seconds.
Enables and configures the downlink data lockout timer, for the SGSN services, to reduce the frequency of mobile-initiated keep alive messages.

*seconds* set the number of seconds before timer expire, range of 0 to 10000.

*repeat*  
optionally sets the number of times (1 to 10) that the timer restarts after paging failure.  
*Note:* If repeat is not configured then paging proceeds endlessly until the MR timer expires.

[ default | no ] **gmm paging-failure-action**  
disables the downlink data lockout timer.

**purge-timeout**  
*mins*

Default: 10080 minutes
The purge timer defines the MM-context lifetime, part of the MM-context procedure on the network side. The configured value sets the duration (number of minutes) the SGSN holds the detached subscriber’s MM-context profile. If the subscriber does not reattach to the SGSN during this time, then the SGSN purges this detached subscriber’s MM-context information from its database and sends a MAP purge request towards the HLR to indicate that the subscribers profile is gracefully purged from SGSN’s database.

*mins* must be an integer from 1 to 20160.

**T3302-timeout**  
*mins*

Default: 12 minutes
Defines the number of minutes for timer to send to MS.

*mins* is an integer from 1 to 186.

**T3312-timeout**  
*min*

Default: 54 minutes
Periodic RAU update timer to send to MS.

*mins* is an integer from 0 to 186.

**T3313-timeout**  
*secs*

Default: 5 seconds
Initial page timeout timer for retransmission for Paging Requests.

*secs* is an integer from 1 to 60.

**T3314-timeout**  
*secs*

Default: 44 seconds
Ready Timer for controlling Cell Update Procedure.

*secs* must be an integer from 0 to 11519.

**T3350-timeout**  
*secs*

Default: 6 seconds
Retransmission timer for Attach Accept/RAU Accept/P-TMSI Realloc Command.

*secs* must be an integer from 1 to 20.

**T3360-timeout**  
*secs*

Default: 6 seconds
Retransmission timer for Authentication Request.

*secs* must be an integer from 1 to 20.
### T3370-timeout secs

Default: 6 seconds
Retransmission timer for Identity Request.
`secs` must be an integer from 1 to 20.

### traU-timeout secs

This timer is available in releases 9.0 and higher.
Default: 30
Specifies the number of seconds the “old” 3G SGSN waits to purge the MS’s data. This timer is started by the “old” SGSN after completion of the inter-SGSN RAU.
`secs`: Must be an integer from 5 to 60.

---

**Usage**

Use this command to set GMM timers.

**Example**

Set the t3370 timer expiration for 15 seconds:

```
  gmm t3370-timeout 15
```
llc

Configures the timers that control the data flow for the logical link control (LLC) sub-layer.

**Important:** This command may be repeated as often as necessary to define the needed timers.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > GPRS Service Configuration

`configure > context context_name > gprs-service service_name`

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-gprs-service)#`

**Syntax**

```plaintext
```

```plaintext
default llc { iov-ui-in-xid-reset | n201u-max { sapi11 | sapi3 | sapi5 | sapi9 } | nu-overflow-detection | pdu-lifetime | random-value-in iov-ui | reset-vur | T200 [ sapi1 | sapi11 | sapi3 | sapi5 | sapi7 | sapi9 ] | uplink-pdu-len-validation }
```

```plaintext
no llc { iov-ui-in-xid-reset | nu-overflow-detection | random-value-in iov-ui | reset-vur | uplink-pdu-len-validation }
```

**default**

Resets the configuration parameter to the default values.

**no**

Disables a defined configuration parameter and returns to the SGSN default.

**iov-ui-in-xid-reset**

This keyword makes it possible for the operator to configure whether or not to send IOV-UI in an XID-RESET. This is useful when the MS is not setup to accept IOV-UI (for example, MS sends Attach/RAU Requests with cksn=7) and including IOV-UI in the XID-Reset would result in Attach/RAU failure.

Default: Enabled
n201u-max sapi n pkt_size

This keyword sets the maximum number of octets, per service access point identifier (SAPI), for the downlink data packets. This is the upper limit that the SGSN will negotiate with the subscriber for packets sent from the SGSN to the BSC.

sapi n: Command must identify one of the following SAPI: sapi11, sapi3, sapi5, or sapi9.

pkt_size: Must be an integer from 140 to 1520. Default size is 1520 octets.

nu-overflow-detection high-watermark high_num low-watermark low_num increment-oc

Enables/disables overflow detection for the N(u) counter and setting overflow high/low thresholds facilitates ciphering synchronization between the MS and SGSN.

high_num: Enter an integer between 1 and 511.

low_num: Enter an integer between 0 and 510.

If the expected value of nu(Vur) is greater than or equal to the configured high-watermark, and the received nu(LFN) is less than or equal to the configured low-watermark, the SGSN increments the overflow counter (VurOC).

The recommended overflow settings are as follows: llc nu-overflow-detection high-watermark 496 low-watermark 15 increment-oc While expecting a packet with 496 < nu < 511 and a packet with 0 < nu < 15 is received, overflow is detected and VurOC is incremented.

pdu-lifetime secs

Defines LLC layer PDU lifetime at the BSC.

secs must be an integer from 0 to 90.

Default: 6

random-value-in iov-ui [ negotiation-failure-action { fallback-to-default iov-ui | reject } ]

Including this keyword enables the SGSN to negotiate the sending of a random value for the IOV-UI in the XID Request sent to the MS. If this keyword is not included, then by default the SGSN sends a zero (0) as the value of the IOV-UI in the XID message.

Including default in a command with the negotiation-failure-action keyword resets the SGSN configuration so that all calls are rejected whenever the decipering fails due to failure of the XID negotiation for random IOV-UI

If the negotiation-failure-action fallback-to-default iov-ui option is included in the configuration, then the SGSN will fall back to unencrypted mode whenever the XID negotiation for random IOV-UI negotiation fails.

If the negotiation-failure-action reject option is included in the configuration to return the SGSN to the default functionality and reject all calls when random IOV-UI negotiation fails. This option is typically used only if the negotiaiton-failure-action fallback-to-default iov-ui option has previously been part of the configuration.

The reject option conditionally causes the SGSN to reject calls, for example, when XID for random IOV-UI negotiation failure occurs during intra-RAU or standalone authentication for SMS, the SGSN moves the subscriber to STANDBY and marks the XID negotiation as a failure.

OR

Despite the reject configuration, the SGSN may respond to XID negotiation failure in one of the following manners according to associated circumstances:

• Initiates XID for new random IOV-UI negotiation:

• with the MS is in STANDBY state, any uplink packet (in either ciphered or unencrypted mode, except Attach / Intra-RAU) from the MS which results in CELL-UPDATE, READY
TIMER START and RADIO STATUS READY causes an event indication to the application.

- Initiates Detach:
  - with the MS is in STANDBY state, any uplink activity causes the SGSN to initiate a new XID exchange, which if it fails or aborts due to the reception of SUSPEND, RADIO-STATUS and READY-TIMER expiry, results in the SGSN initiating Detach.
  - when PAGING is ongoing, any Page response from the MS results in the SGSN initiating Detach.
  - during OLD_SGSN ISRAU, when any uplink data comes before T3 tunnel timer expiry then the SGSN initiates Detach.

- Handles Messages:
  - Attach and intra-RAU (from both local and non-local TLLI or from both the same and different RA) will be processed in any state.

- Moves to STANDBY state:
  - MS is moved to STANDBY state if the XID exchange failed due to any of the following cases: suspend, radio status, BVC block, BVC reset, ready timer expiry, no response received for XID exchange during INTRA-RAU/Standalone Authentication for SMS.
  - XID is ongoing in READY state and if the MS moves to either 3G or to the peer-SGSN then the subscriber is moved to STANDBY state.

```
reset-vur
```
Enables/disables the mechanism to reset the Vur value maintained at LLC if the intra RAU request is received with N(U) = 0
Default: Disabled

```
T200 sapi1 time
```
Sets the retransmission timer (in seconds) for sapi1.
`time` must be an integer of 1 to 10.
Default: 5

```
T200 sapi11 time
```
Sets the retransmission timer (in seconds) for sapi11.
`time` must be an integer of 1 to 50.
Default: 40

```
T200 sapi3 time
```
Sets the retransmission timer (in seconds) for sapi3.
`time` must be an integer of 1 to 10.
Default: 5

```
T200 sapi5 time
```
Sets the retransmission timer (in seconds) for sapi5.
`time` must be an integer of 1 to 20.
Default: 10
### T200 sapi7 time

Sets the retransmission timer (in seconds) for sapi7. 

*time* must be an integer of 1 to 40. 

Default: 20

### T200 sapi9 time

Sets the retransmission timer (in seconds) for sapi9. 

*time* must be an integer of 1 to 40. 

Default: 20

### uplink-pdu-len-validation

Available in releases 8.1 and higher. 

This feature enables validation of the size of the uplink LLC packets. With validation enabled, the SGSN will drop any uplinked packets that are larger than the negotiated limit. 

If the no form of the command is used, then this feature is disabled. The SGSN will be more flexible with uplink packet sizes. So if the SGSN and MS have a mismatch and the MS sends packets that are larger than expected, then the SGSN will not drop the packets. 

Default: Enabled.

#### Usage

Use the command repeatedly to configure additional timers and features for the LLC sub-layer.

#### Example

Set the T200 retransmission timer to timeout at 12 seconds for SAPI5:

```text
llc t200 sapi5 12
```

Use the following command to instruct the SGSN to ignore the N201_U packet size limits for uplink packets from an MS:

```text
no uplink-pdu-len-validation
```
network-sharing

This command enables or disables CS-PS coordination checking for homers (UEs in their home network) or roamers (UEs from outside the home network). The command also sets the failure code that will be sent for GPRS MOCN.

**Product**
SGSN

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > GPRS Service Configuration
configure > context context_name > gprs-service service_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-gprs-service)#
```

**Syntax**

```
network-sharing { cs-ps-coordination { failure-code <gmm-cause> | homer | roamer } |
  failure-code <gmm-cause>

no network-sharing cs-ps-coordination { homer | roamer }

default network-sharing cs-ps-coordination
```

- **no**
  Disables CS-PS coordination check for either homers or roamers.

- **default**
  Set the CS-PS coordination parameters to default values.

**failure-code <gmm-cause>**

This keyword has two optional functions:

- When used with the `cs-ps-coordination` keyword, it sets the GMM cause code that is to be included in the message when the SGSN requests the BSC to provide CS-PS coordination. Default value is 14.

- When used as an independent keyword with the `network-sharing` command, it sets the failure cause that is used by GPRS MOCN if no failure cause is available when the SGSN sends a Reject message. Default value is 7.

**<gmm-cause>** is an integer from 2-111. Valid options include:

- 2 - IMSI unknown in HLR
- 3 - Illegal MS
- 6 - Illegal ME
- 7 - GPRS services not allowed
- 8 - GPRS services and non-GPRS services not allowed
- 9 - MSID cannot be derived by the network
- 10 - Implicitly detached
- 11 - PLMN not allowed
- 12 - Location Area not allowed
- 13 - Roaming not allowed in this location area
- 14 - GPRS services not allowed in this PLMN
- 15 - No Suitable Cells In Location Area
- 16 - MSC temporarily not reachable
- 17 - Network failure
- 20 - MAC failure
- 21 - Synch failure
- 22 - Congestion
- 23 - GSM authentication unacceptable
- 40 - No PDP context activated
- 48 to 63 - retry upon entry into a new cell
- 95 - Semantically incorrect message
- 96 - Invalid mandatory information
- 97 - Message type non-existent or not implemented
- 98 - Message type not compatible with state
- 99 - Information element non-existent or not implemented
- 100 - Conditional IE error
- 101 - Message not compatible with the protocol state
- 111 - Protocol error, unspecified

**homer**

Enables checking for CS-PS coordination for UEs from inside the home network (homers) only.

**roamers**

Enables checking for CS-PS coordination for UEs from another network (roamers) only.

**Usage**

The operator can use this command to configure CS-PS coordination checking explicitly for homer or roamers subscribers and for the failure-code to be sent when the SGSN asks the BSC to perform CS-PS coordination.

**Example**

Use a command similar to the following to have the SGSN perform CS-PS coordination checking only for all UEs from outside of the home network. `network-sharing cs-ps-coordination homer`
nri

This command configures the network resource identifier (NRI) to identify a specific SGSN. The NRI information is stored in the P-TMSI. The SGSN uses a portion of this NRI to set the parameters for Gb flex (SGSN pooling) functionality.

**Product**  
SGSN

**Privilege**  
Security Administrator, Administrator

**Mode**  
Exec > Global Configuration > Context Configuration > GPRS Service Configuration

configure > context context_name > gprs-service service_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-gprs-service)#
```

**Syntax**

```
nri length nri_length { nri-value nri_value | null-nri-value null_nri_value non-broadcast-lac lac_id rac rac_id [ nri-value value ] }

default nri

no nri
```

**default nri**

A default configuration has been made available beginning in Release 14.0. Using this keyword now resets the nri configuration to nri length 6 and nri-value 0.

**Important:** Behavior change in Release 14.0 -- it is no longer necessary to configure NRI as default values have been enabled.

**no**

**Important:** no nri command form is deprecated in Release 14.0. To ensure backward compatibility with configuration files created with pre-Release 14.0 builds, the no nri configuration will be automatically converted to the Release 14.0 default values of nri 6 and 0.

This command removes the configured NRI value and location information in the P-TMSI that would be retrieved by this SGSN.
**length nri_length**

Specifies the number of bits to be used in the P-TMSI, bits 23 to 18 are used to define the network resource identifier (NRI). The NRI length configuration also sets the maximum size of the pool. If not configured, the NRI length will be of zero length.

**nri_length**: Must be an integer from 1 to 6 to identify the number of bits.

**null-nri-value null_nri_value**

Configures the null NRI value which must be unique across the pool areas. This keyword is used for the offloading procedure for SGSN pooling (enabled with the sgsn offloading command, see the Exec Mode chapter).

**null_nri_value** is an integer from 0 (zero) to 63 used to identify the SGSN to be used for the offloading procedure for SGSN pooling. There is no default value for this parameter.

**non-broadcast lac lac_id rac rac_id**

Defines the non-broadcast LAC/RAC to be used in combination with the null-NRI for the offloading procedure.

**lac_id** defines a location area code associated with a BSS. Must be an integer between 1 and 65535.

**rac_id** defines the remote area code to be associated with a BSS. Must be an integer between 1 and 255.

**nri-value nri_value**

Specifies the MS-assigned value of the NRI to retrieve from the P-TMSI. This value must not exceed the maximum possible value specified by the NRI length. The NRI value must be unique across the pool or across all overlapping pools.

**nri_value** must be an integer from 1 to 63 to identify a specific SGSN in a pool. Use of 0 (zero) value is not recommended.

Multiple NRI values can be identified by providing multiple nri-values separated by a blank space for example: *nri length 6 nri-value 29 43 61*

**Usage**

Use this command to add or remove the Gb flex pool configuration for this GPRS service. The command can be repeated to specify different values for any of the keyword parameters. If more than one NRI is configured, the GPRS service will round-robin between the available NRIs when new subscribers (re)connect.

Use this command to retrieve the NRI (identity of an SGSN) stored in in bits 23 to 18 of the packet-temporary mobile subscriber identity (P-TMSI). If more than one NRI value is configured, the GPRS service will round-robin between the available NRIs when new subscribers (re)connect.

**Example**

The following command specifies the the NRI length as 5 bits, identifies SGSN 23 with LAC 222 and RAC 12 for offloading procedure with NRIs 6 and 41:

```
nri length 5 null-nri-value 34 non-broadcast lac 222 rac 12 nri-value 6 41
```
paging-policy

Configures the paging parameters for the GPRS service.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > GPRS Service Configuration

```
configure > context context_name > gprs-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-gprs-service)#
```

**Syntax**

```
paging-policy { last-known-area { all | bsc | cell | location-area | routing-area } + | max-retransmissions retran_num }
```

```
no paging-policy last-known-area { bsc | cell | location-area | routing-area }
```

```
default paging-policy { last-known-area | max-retransmissions }
```

---

**no**
Disables the paging-policy definition for this GPRS service configuration.

---

**default**
Resets the defaults for parameters managed by this paging policy.

---

**last-known-area**
Select one or more paging areas and enter them in preferred paging order:
- **all** : Pages in the last known BSC.
- **bsc** : Pages in last known BSC.
- **cell** : Pages in last known cell.
- **location-area** : Pages in last known location area.
- **routing-area** : Pages in last known routing area.

By default, paging occurs in the following order:
cell, BSC, routing area, location area.

---

**max-retransmission retran_num**

Configures the maximum number of retries for a page request per paging area.

- **retran_num**: Enter an integer from 0 to 5.
  - **2**: default.
○ 0: disables retransmission for paging request so that the SGSN only sends a single 2G PS-paging request to the BSC with no retransmissions.

+ Keywords can be repeated or combined as needed to complete the paging policy configuration.

Usage

Use this command to configure the order of preference for retransmitting into specified paging-areas.

Example

Use the following command to instruct the SGSN to page the cell and BSC as the last-known areas:

```
paging-policy last-known-area cell bsc
```
**peer-nsei**

This command associates a peer (remote) network service entity (NSEI) for a BSS with this GPRS service.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > GPRS Service Configuration

configure > context context_name > gprs-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-gprs-service)#

**Syntax**

```
peer-nsei nse_id { associate dscp-template downlink template_name | lac lac_id rac rac_id | name peer_nsei_name | pooled }

no peer-nsei nse_id [ associate dscp-template downlink | lac lac_id rac rac_id | name | pooled ]
```

- **no**
  - Removes the specified configuration from this peer-nsei configuration.

### Important:
Deleting the LAC/RAC portion of the configuration will probably result in the loss of subscriber connections.

- **nse_id**
  - Defines a specific peer NSEI configuration for this GPRS service.
  - `nse_id` - enter an integer from 0 to 65535.

- **associate dscp-template downlink template_name**
  - Identifies a specific DSCP marking template to associate with the peer-NSE. The DSCP template must first be created with SGSN Global configuration mode and then defined with the commands in the DSCP Template configuration mode. The template provides a mechanism for differentiated services code point (DSCP) marking of control packets and LLC signaling messages on Gb interfaces. This DSCP marking feature enables the SGSN to perform classifying and managing of network traffic and to determine quality of service (QoS) for the interfaces to an IP network.
  - `template_name` - enter an alphanumeric string of 1 to 64 characters.

- **lac lac_id**
  - Defines a location area code associated with the NSE BSS.
  - `lac_id` must be an integer between 1 and 65535.
rac rac_id
Defines the remote area code to be associated with the NSE BSS
rac_id must be an integer between 1 and 255.

name peer_nsei_name
Enables identifying a BSC by a name which is stored in SCT.
peer_nsei_name - enter an alphanumeric string of 1 to 64 characters.

pooled
Enables pooling with non-pooled BSCs within the pool area.

Usage
Use this command repeatedly to associate one or more LAC/RAC combinations and/or pooling with this peer-GPRS service configuration. Also repeat the command as needed to create an association with a DSCP marking template, to define a name for a BSC, and to enable pooling with non-pooled BSCs.

The Network Service Entity (NSE) at the BSS and the SGSN provides the network management functionality required for the operation of the Gb interface. Each NSE is identified by means of NSE identifier (NSEI).

Example
The following command configures the NSE with identifier as 4114 having location area code 234 and routing area code as 22:

    peer-nsei 4114 lac 234 rac 22

The following command enables Gb flex (pooling) functionality for NSEI 4414 for this GPRS service:

    peer-nsei 4114 pooled
plmn

This command identifies the Public Land Mobile Network (PLMN) for the GPRS service. It also configures the common PLMN-Id and an optional list of dedicated PLMN-Ids in support of Multi-Operator Core Network (MOCN) operation.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > GPRS Service Configuration

```
configure > context context_name > gprs-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-gprs-service)#
```

**Syntax**

```
plmn id mcc mcc_num mnc mnc_num [ network-sharing common-plmn mcc mcc_num mnc mnc_num [ plmn-list mcc mcc_num mnc mnc_num [ mcc mcc_num mnc mnc_num ] + ] ]
```

```
no plmn id
```

**no**

Removes the PLMN information from the configuration for the current SGSN service.

```
mcc mcc_num
```

Define the mobile country code (MCC) portion of the PLMN Id.

- `mcc_num` must be a 3 digit integer from 100 to 999. MCC values of 000-099 are Reserved codes.

```
mnc mnc_num
```

Define the mobile network code (MNC) portion of the PLMN Id.

- `mnc_num` must be a 2 or 3 digit integer from 00 to 999. MNC value of 000 is reserved.

```
network-sharing common-plmn
```

Configures the common PLMN-Id broadcast by a radio network. An MS that does not support network sharing will only see this PLMN-Id. An MS that supports network sharing (MOCN) will see this PLMN-Id and the list of PLMN-Ids configured using the `plmn-id` keyword.

```
plmn-list
```

Configures a list of PLMN-Ids that an MS will see when network sharing is enabled.

```
+
```

The plus symbol indicates that indicates that more than one more than one set of the keywords, for PLMN-Id, can be entered within a single command.
Usage
Use this command to set PLMN parameters for the current SGSN service. This command also sets the common PLMN-Id and a list of PLMN-Ids employed in network sharing (MOCN) deployments. There is no limit to the number of PLMN-Ids that can be included in the list.

Example
The following command identifies the PLMN MCC as 200 and the MNC as 10:

```
plmn id mcc 200 mnc 10
```
reporting-action event-record

This command enables the SGSN to log GMM/SM events in EDR files for 2G services.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > GPRS Service Configuration
configure > context context_name > gprs-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-gprs-service)#

Syntax

reporting-action event-record

[ default | no ] reporting-action event-record

default
Disables the logging function.

no
Removes the logging function from the configuration file.

Usage

This command is one of the steps needed to enable the SGSN to create a log for events such as Attach, RAU, and Activations. The log is an EDR (event data record) in CSV format. For details about how this feature works, refer to the GMM-SM Event Logging chapter in the SGSN Administration Guide.

Related Commands:
- To enable GMM/SM event logging for 2G services, the reporting-action event-record command must be configured in the SGSN service configuration.
- To enable a log to be generated in an EDR file, the edr-module active-charging-service command must be enabled in the Context configuration mode.
- To configure parameters for the logging file characteristics and for file transfer, use the commands in the EDR Module Configuration Mode.

Example

Enable GMM/SM event logging for 3G services:

reporting-action event-record
**setup-timeout**

This command configures the maximum number of seconds allowed for session setup.

**Product**  
SGSN

**Privilege**  
Security Administrator, Administrator

**Mode**  
Exec > Global Configuration > Context Configuration > GPRS Service Configuration

```
configure > context context_name > gprs-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-gprs-service)#
```

**Syntax**

```
setup-timeout seconds
```

```
default setup-timeout
```

```
default
```

Returns the configuration to the default, 60 seconds.

```
seconds
```

An integer from 1 to 100000.

**Usage**

Use this command to set the time allowed for session setup.

**Example**

The following command sets the maximum session setup time to 300 seconds:

```
setup-timeout 300
```
sgsn-context-request

This command specifies whether or not the PTMSI signature check should be skipped if the PTMSI signature is not included in the SGSN context request.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > GPRS Service Configuration

```bash
configure > context context_name > gprs-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-gprs-service)#
```

**Syntax**

```
sgsn-context-request ptmsi-signature-absence allowed

default sgsn-context-request ptmsi-signature-absence

no sgsn-context-request ptmsi-signature-absence allowed
```

- **default**
  Returns the configuration to the default action to perform the PTMSI signature check.

- **no**
  Removes this definition from the system configuration.

**Usage**

Use this command to skip the PTMSI signature check.

**Example**

The following command instructs the system to perform the PTMSI signature check.

```
default sgsn-context-request ptmsi-signature-absence
```
sgsn-number

Define the SGSN E.164 number to be used when interacting via MAP protocol for this GPRS service.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > GPRS Service Configuration

configure > context context_name > gprs-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-gprs-service)#

**Syntax**

```
sgsn-number sgsn_number

no sgsn-number
```

**Usage**

Use this command to identify the ISDN number for the SGSN associated with this GPRS service. The SGSN supports multiple SGSN numbers – different numbers in the 2G GPRS service configuration and the 3G SGSN service configuration. If an HLR-initiated dialog is received, the SGSN will perform a lookup based on the IMSI and find the correct SGSN number with which the MS is associated. Subsequent messaging will use this address.

**Example**

Disable the E.164 number for this GPRS service.

```
no sgsn-number
```
This command configures the session management (SM) parameters associated with this particular GPRS service context.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > GPRS Service Configuration

```
configure > context context_name > gprs-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-gprs-service)\#
```

**Syntax**

```
sm { activate-max-retransmissions num_retries | deactivate-max-retransmissions num_retries | guard-timer guard_seconds | ignore-pco-decode-error | modify-max-retransmissions num_retries | partial-apn-match | requested-apn-from-first-subrec | t3385-timeout secs | t3386-timeout secs | t3395-timeout secs | t3396 min minimum max maximum cause cause_code | trim-trailing-spaces-in-apn }
```

default sm { activate-max-retransmissions | deactivate-max-retransmissions | ignore-pco-decode-error | modify-max-retransmissions | t3385-timeout | t3386-timeout | t3395-timeout | trim-trailing-spaces-in-apn }

default

Resets the SM parameters to their defaults.

---

### activate-max-retransmissions num_retries

Defines the maximum number of retries to transmit ‘activate PDP context request’.

- **num_retries**: Must be an integer from 1 to 10.
- Default: 4

### deactivate-max-retransmissions num_retries

Defines the maximum number of retries to transmit ‘deactivate PDP context request’.

- **num_retries**: Must be an integer from 1 to 10.
- Default: 4

### guard-timer guard_seconds

Sets the number of seconds before the session manager resources are cleared.

- **guard_seconds**: is an integer from 30 to 150.
- Default: 80 seconds
ignore-pco-decode-error
Enables the SGSN to ignore received decode errors that are due to incorrectly encoded PCO IE length in SM Requests.
Default: disabled

modify-max-retransmissions num_retries
Defines the maximum number of retries to transmit ‘modify PDP context request’.
num_retries: integer from 1 to 10.
Default: 4

partial-apn-match
Enables partial matching of requested APN during APN selection.
Partial APN or APN with trailing spaces may be present in an Activate Request because incorrect information was keyed in by the user. Though it is valid to reject such Activation Requests, it increases the signaling between the MS and the SGSN. This has an impact on the radio resources.

requested-apn-from-first-subrec
Enables use of a ‘requested APN’ from the first subscription record. When this feature is enabled, the PDP Activation is not rejected during APN Selection; instead, the APN from the first subscription record is used as the requested APN and the SGSN continues with the rest of the APN Selection process.
A requested APN is an optional IE in an Activate PDP Request. To get the requested PDP type, if multiple PDP subscription records exist for the subscriber, then the MS has to include the APN information to choose the PDP subscription record during APN selection. Otherwise, such activations will be rejected during APN selection (per TS 23.060 Appendix A). Though it is valid to reject such activation requests, it increases the signaling between the MS and the SGSN, which impacts the radio resources.

t3385-timeout secs
Defines the maximum amount of time for retransmission of ‘activate request’ messages.
secs: Must be an integer from 1 to 60.
Default: 8

t3386-timeout secs
Defines the maximum amount of time for retransmission of ‘modify request’ messages.
secs: Must be an integer from 1 to 60.
Default: 8 seconds.

t3395-timeout secs
Defines the maximum amount of time for retransmission of ‘deactivate request’ messages.
secs: Must be an integer from 1 to 60.
Default: 8

trim-trailing-spaces-in-apn
Enables SGSN to strip off any trailing space(s) in requested APN.
If a requested APN in an Activate PDP Context Request has any trailing spaces, then those trailing spaces will be removed and the length field will be updated.
Usage
Repeat this command with different keywords (parameters) to configure the SM (session management) as needed for this GPRS service. Keywords can be used to optimize signaling between the MS and the SGSN to reduce the impact on the radio resources.

Example
Reset the number of retransmission messages for deactivate PDP context request to 5.

```sh
sm deactivate-max-retransmissions 5
```
sndcp

Define the sub-network dependent convergence protocol (SNDCP) network packet data unit (N-PDU) reassembly timeout interval associated with this GPRS service.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > GPRS Service Configuration
configure > context context_name > gprs-service service_name

Entering the above command sequence results in the following prompt:
[context_name]host_name(config-gprs-service)#

Syntax

sndcp reassembly-timeout seconds

default sndcp reassembly-timeout

default

Resets the timer configuration to the default value of 30 seconds.

seconds

Defines the number of seconds the SGSN waits for all the SNDCP segments to arrive before dropping all the disassembled segments.
seconds: Must be an integer from 1 to 300.

Usage

Use this command to modify the SNDCP reassembly timer. This timer starts as soon as the first N-PDU segment is received (either in-order or out-of-order). If all the segments belong to the N-PDU arrive before the timer expires then the segments are reassembled. If all the segments do not arrive before the timer expires, then the stored segments are discarded.

Example

Reset the default for the timer.

default sndcp reassembly-timeout
Chapter 147
GRE Tunnel Interface Configuration Mode Commands

The Generic Routing Encapsulation (GRE) Tunnel Interface Configuration Mode is used to create and manage the GRE tunneling interfaces for addresses, address resolution options, etc.

Mode

Exec > Global Configuration > Context Configuration > Tunnel Interface Configuration > GRE Tunnel Interface Configuration

configure > context context_name > interface interface_name tunnel > tunnel-mode gre

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-if-tunnel-mode)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
destination

This command configures the destination IP address of the tunnel by specifying the destination end address. This is a mandatory configuration for a GRE tunnel interface.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Tunnel Interface Configuration > GRE Tunnel Interface Configuration

```
configure > context context_name > interface interface_name tunnel > tunnel-mode gre
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-tunnel-mode)#
```

Syntax

```
[ no ] destination address ip_address
```

no

Removes or disassociates the configured destination IP address from a specific GRE tunnel interface configuration.

```
address ip_address
```

Configures the IP address for the interface.

*ip_address* must be specified using the IPv4 dotted-decimal notation.

Usage

Use this command to configure the destination IP address of the tunnel by specifying the IP address of destination tunnel end for GRE tunnel interface.

**Important:** State of source address will affect the operational state of the tunnel.

Example

The following command sets the 10.2.3.4 as destination IP address of the GRE tunnel interface:

```
destination address 10.2.3.4
```
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
```
end
```

**Usage**
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Use this command to return to the parent configuration mode.
keepalive

This command configures various parameters for sending Keepalive messages to the remote end-point in GRE tunnel interface configuration. By default sending keepalives is disabled.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Tunnel Interface Configuration > GRE Tunnel Interface Configuration

```
configure > context context_name > interface interface_name tunnel > tunnel-mode gre
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-tunnel-mode)#
```

**Syntax**

```
keepalive [ interval time_interval num-retry retry ]
[ default | no ] keepalive
```

- **default**
  Sets the sending of Keepalives with default parameters.
  - interval: 10 seconds
  - num-retry: 3 retries

- **no**
  Disables the keepalive and turns off the sending of Keepalives messages.

- **interval time_interval**
  Default: 10
  Specifies the time interval (in seconds) between two Keepalives sent to remote ends of GRE tunnel interface configuration.
  - *time_interval* must be an integer from 5 through 3600.

- **num-retry retry**
  Default: 3
  Specifies number of retransmission of keepalives to remote node without getting any response before the remote node is marked as dead/down.
  - *retry* must be an integer between 0 through 10.

**Usage**

Use this command to configure the parameters for sending Keepalives to the remote end-point of GRE tunnel. It also configures the interval at which GRE Keepalives are sent on the interface and number of retries.
without getting a response from the remote end-point before the tunnel is shutdown. By default, Keepalives will not be sent.

Example
The following command enables the keepalive and sets the other parameters to defaults:

```
default keepalive
```
source

This command configures the source IP address of the tunnel either by specifying the IP address (host address) or by specifying another configured non-tunnel IP interface. This is a mandatory configuration for GRE tunnel interface.

<table>
<thead>
<tr>
<th>Product</th>
<th>All</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privilege</td>
<td>Security Administrator, Administrator</td>
</tr>
</tbody>
</table>
| Mode          | Exec > Global Configuration > Context Configuration > Tunnel Interface Configuration  
                configure > context context_name > interface interface_name tunnel > tunnel-mode gre |

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-tunnel-mode)#
```

Syntax

```
[ no ] source { address ip_address | interface interface_name }
```

- **no**
  - Removes/disassociates the configured source IP address or host interface from a specific GRE tunnel interface configuration.

- **address ip_address**
  - Configures the IP address for the interface specifying the IP address.
  - `ip_address` must be specified using IPv4 dotted-decimal notation.

- **interface interface_name**
  - Specifies the name of the preconfigured non-tunnel IP interface, whose address is used as the source address of the GRE tunnel.

Usage

Use this command to configure the source IP address of the tunnel either by specifying the IP address (host address) or by specifying another configured non-tunnel IP interface for GRE tunnel interface.

**Important:** State of source address will affect the operational state of the tunnel.

Example

The following command sets the 10.2.3.4 as source IP address of the GRE tunnel interface:

```
source address 10.2.3.4
```
tos

This command configures the parameters/action for the type of Service (ToS) parameter in the IP tunnel transport protocol header.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Tunnel Interface Configuration > GRE Tunnel Interface Configuration

configure > context context_name > interface interface_name tunnel > tunnel-mode gre

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-if-tunnel-mode)#

Syntax

tos { value [ af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be | ef | lower-bits tos_value ] | copy }

default

Sets the IP TOS to lower bits value of 0.

value [ tos_value ]

Default: af11

Specifies the IP QoS DSCP per-hop behavior to be marked on the outer header of signalling packets originating from the Access Gateway. This is a standards-based feature (RFC 2597). The following forwarding types are supported:

• af11: Assured Forwarding 11 per-hop behavior
• af12: Assured Forwarding 12 per-hop behavior
• af13: Assured Forwarding 13 per-hop behavior
• af21: Assured Forwarding 21 per-hop behavior
• af22: Assured Forwarding 22 per-hop behavior
• af23: Assured Forwarding 23 per-hop behavior
• af31: Assured Forwarding 31 per-hop behavior
• af32: Assured Forwarding 32 per-hop behavior
• af33: Assured Forwarding 33 per-hop behavior
• af41: Assured Forwarding 41 per-hop behavior
• af42: Assured Forwarding 42 per-hop behavior
• af43: Assured Forwarding 43 per-hop behavior
**be**: Best Effort forwarding per-hop behavior  
**ef**: Expedited Forwarding per-hop behavior typically dedicated to low-loss, low-latency traffic.

The assured forwarding behavior groups are listed in the table below.

<table>
<thead>
<tr>
<th></th>
<th>Class 1</th>
<th>Class 2</th>
<th>Class 3</th>
<th>Class 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low Drop</td>
<td>AF11</td>
<td>AF21</td>
<td>AF31</td>
<td>AF41</td>
</tr>
<tr>
<td>Medium Drop</td>
<td>AF12</td>
<td>AF22</td>
<td>AF32</td>
<td>AF42</td>
</tr>
<tr>
<td>High Drop</td>
<td>AF13</td>
<td>AF23</td>
<td>AF33</td>
<td>AF43</td>
</tr>
</tbody>
</table>

Traffic marked with a higher class is given priority during congestion periods. If congestion occurs to traffic with the same class, the packets with the higher AF value are dropped first.

**lower-bits** **tos_value**

Default: 0

Sets the least-significant 6 bits in the ToS byte with the specified numeric value. **tos_value** must be an integer from 0 through 255.

**copy**

This keyword instructs the system to copy the ToS value from the passenger IPv4 packet or Traffic class value from the passenger IPv6 packet to the ToS value of the IPv4 tunnel transport protocol header.

**Usage**

Use this command either to set the ToS parameter in the IPv4 tunnel transport protocol header to the specified value or instructs to copy the ToS value from the passenger IPv4 packet or Traffic class value from the passenger IPv6 packet to the ToS value of the IPv4 tunnel transport protocol header. If one of the enumerated values is set, the DSCP bits which are the six most-significant bits in the ToS byte are marked. If the integer value is set, it will be written into the six least-significant bits of the ToS byte.

**Example**

The following command instructs the system to copy the ToS value from the passenger IPv4 packet or Traffic class value from the passenger IPv6 packet to the ToS value of the IPv4 tunnel transport protocol header:

```plaintext
tos copy
```
**ttl**

This command configures the Time to live (TTL) parameter to be used in the tunnel transport protocol header for the current GRE tunnel interface.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Tunnel Interface Configuration > GRE Tunnel Interface Configuration

`configure > context context_name > interface interface_name tunnel > tunnel-mode gre`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-tunnel-mode)#
```

**Syntax**

```
ttl ttl_value

default ttl
```

- **default**
  
  Sets the TTL value to system default value.

- **ttl_value**
  
  Default: 15
  
  Specifies the maximum time to live to be used in the tunnel transport protocol header.
  
  The time to live (TTL) is not a measure of time but the number of hops through the network.
  
  `ttl_value` must be an integer between 1 through 255.

**Usage**

Use this command to set the TTL parameter to be used in the tunnel transport protocol header for the GRE tunnel configuration.

**Example**

The following configures the TTL to a value of 10:

```
ttl 10
```
Chapter 148
Gs Service Configuration Mode Commands

The Gs Service configuration mode configures the parameters used to setup and maintain a Gs interface for a connection between the SGSN and an MSC/VLR.

**Mode**

Exec > Global Configuration > Context Configuration > Gs Service Configuration

```
configure > context context_name > gs-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-gs-service)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
associate-sccp-network

This command associates a previously defined Signaling Connection Control Part (SCCP) network instance with the Gs service. This association is required to access Visitor Location Register(s) (VLRs).

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Gs Service Configuration

```
configure > context context_name > gs-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-gs-service)#
```

**Syntax**

```
associate-sccp-network sccp_net_id

no associate-sccp-network
```

- **no**
  Removes the associated SCCP network configuration instance from this Gs service configuration.

- **sccp_net_id**
  Identifies the SCCP network configuration instance to associate with this Gs interface to enable connection with VLR(s).
  `sccp_network_num`: Must be an integer from 1 through 12.

**Usage**

Use this command to associate the SCCP network configuration instance with the Gs interface in this service.

**Important:** A single SCCP network configuration instance can not be shared with multiple Gs services.

**Important:** To enable a Gs service, the user needs to configure `ssn` with the `bssap+` command.

**Example**

Following command associates SCCP network 2 with this Gs service.

```
associate-sccp-network 2
```
bssap+

This command defines the Base Station System Application Part Plus configuration parameters for the Gs service to enable the SGSN to access a Visitor Location Register(s) (VLRs).

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Gs Service Configuration

```
configure > context context_name > gs-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-gs-service)#
```

**Syntax**

```
bssap+ ssn ss_num

no bssap+ ssn ss_num
```

<table>
<thead>
<tr>
<th>no</th>
</tr>
</thead>
<tbody>
<tr>
<td>Removes the configured BSSAP+ subsystem number from this Gs service.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ssn ss_num</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the subsystem number to configure in this Gs interface to use BSSAP+.</td>
</tr>
</tbody>
</table>

**Usage**
Use this command to configure the BSSAP+ subsystem with Gs interface in this service to communicate with VLR(s).

**Important:** A single SCCP network configuration instance can not be shared with multiple Gs services.

**Important:** To start a Gs service, the user needs to configure the `command parameter.

**Example**

Following command configures subsystem 101 with BSSAP+ in this Gs service.

```
bssap+ ssn 101
```
end

Exits the current configuration mode and returns to the Exec mode.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Return to the Exec mode.
exit

Exits the current configuration mode and returns to the previous configuration mode.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

exit

Usage
Return to the previous configuration mode.
max-retransmission

This command configures the retransmission values for different procedure counters in Gs service as described in TS 29.018.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Gs Service Configuration
configure > context context_name > gs-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-gs-service)#

Syntax

max-retransmissions { n8 | n9 | n10 | n12 } retrans_num

default max-retransmissions { n8 | n9 | n10 | n12 }

no

Removes the configured Gs procedures from this Gs service.

{ n8 | n9 | n10 | n12 }

Specifies the various Gs service procedures that are available to be used to communicate with VLR(s).

- n8: Defines the maximum number of retries for explicit IMSI detach from a non-GPRS service. Default is 2.
- n9: Defines the maximum number of retries for explicit IMSI detach from a non-GPRS service. Default is 2.
- n10: Defines the maximum number of retries for implicit IMSI detach from the GPRS service. Default is 2.
- n12: Defines the maximum number of retries for BSSAP+ to send Reset Indication messages. Default is 2.

retrans_num

Default: 2

Specifies the number of re-transmission of message for specified procedures.

retrans_num: Must be an integer from 0 through 10.

Usage

Use this command to configure the retransmission values for specific procedure counters in Gs service. Counters are based on TS 29.018.

This command can be entered for each procedure counter separately.
Example

Following command configure retransmission value as 3 for counter for procedure to send BSSAP+ Reset Indication messages in this Gs service.

```
max-retransmissions n12 3
```
non-pool-area

This command creates a non-pool area for a set of subscriber location area code (LAC) values that can be used with a specific VLR for the Gs service.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Gs Service Configuration

configure > context context_name > gs-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-gs-service)#

Syntax

non-pool-area non_pool_name \{ use-vlr vlr_name lac lac_num \} +

no non-pool-area non_pool_name \{ lac lac_num \}

<table>
<thead>
<tr>
<th>no</th>
</tr>
</thead>
<tbody>
<tr>
<td>Removes the configured non-pool area from this Gs service.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>non_pool_name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the name of the non-pool area to configure with this command.</td>
</tr>
<tr>
<td><strong>non_pool_name</strong> must be an alpha and/or numeric string of 1 to 63 characters.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>use-vlr vlr_name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the name of the VLR to be associated with this non-pool area.</td>
</tr>
<tr>
<td><strong>vlr_name</strong> is the name of VLR and must be an alpha and/or numeric string of 1 to 63 characters.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>lac lac_num</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the subscribers’ location area code to be attached with this non-pool area and specific VLR. This LAC of subscriber is obtained from the radio area indicator (RAI).</td>
</tr>
<tr>
<td>Including this keyword with the <strong>no</strong> form of the command enables the operator to remove a specific LAC from the non-pool area configuration.</td>
</tr>
<tr>
<td><strong>lac_num</strong> is the LAC value and must be an integer value from 1 through 65535.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>+</th>
</tr>
</thead>
<tbody>
<tr>
<td>More than one <strong>lac_num</strong>, separated by a space, can be entered within a single command.</td>
</tr>
</tbody>
</table>

Usage

This command can be repeated as necessary to define a total of 32 configured LACs for the combined **non-pool-area** and **pool-area** configurations per Gs service.
Example

Following command configure a non-pool area `starpool1` to use VLR named `starvlr1` for LAC 101 in a Gs service.

```
non-pool-area starpool1 use-vlr starvlr1 lac 101
```
pool-area

This command creates a pool area configuration instance. This command also enters the Pool Area configuration mode to define the set of VLRs to use for a pool area for a set of subscriber location area code (LAC) values in the Gs service.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Gs Service Configuration
configure > context context_name > gs-service service_name

Entering the above command sequence results in the following prompt:

```
[context_name] host_name(config-gs-service) #
```

**Syntax**

```
pool-area pool_name [ -noconfirm ]
no pool-area non_pool_name
```

no

Removes the configured pool area from this Gs service.

---

pool_name

Specifies the name of the pool area to configure with this command for VLR pooling and association of a LAC.

pool_name: Must be an alpha and/or numeric string of 1 to 63 characters.

---

-noconfirm

Indicates that the command is to execute without any additional prompt and confirmation from the user.

---

**Usage**

Use this command to create/enter the pool area configuration mode. This mode is used configure the set of VLRs to be used for a set of subscriber LAC.

This command can be used multiple times, subject to a limit of 128 LAC values (the total number of non-pool-area and pool-area configurations) per Gs service.

---

**Example**

The following command configures a pool area named starpool in a Gs service without any confirmation prompt.

```
pool-area starpool -noconfirm
```
sgsn-number

Define the SGSN’s E164 number to associate an SGSN with this Gs Service.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Gs Service Configuration

```
configure > context context_name > gs-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-gs-service)#
```

**Syntax**

```
sgsn-number E.164_number
```

<table>
<thead>
<tr>
<th>E.164_number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defines the SGSN’s ‘telephone’ number, the ISDN number for per ITU-T E.164 numbering plan. The number must be a numerical string of 1 to 15 digits.</td>
</tr>
</tbody>
</table>

**Usage**

For releases 8.1 or higher, use this command to define the SGSN’s E.164 ISDN number. This value should match the *sgsn-number* defined for SGSN Service or GPRS Service.

**Important:** Note: the Gs Service will not start unless the SGSN’s E.164 number is configured.

**Example**

```
sgsn-number 12345678901234
```
timeout

This command configures various timers defining the wait before retransmitting a specific message for Gs service procedures.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Gs Service Configuration

configure > context context_name > gs-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-gs-service)#

Syntax

timeout { t6-1-timer t6_1_dur | t8-timer t8_dur | t9-timer t9_dur | t10-timer t10_dur | t12-1-timer minute t12_1_dur | t12-2-timer t12_2_dur }

[ default ] timeout { t6-1-timer | t8-timer | t9-timer | t10-timer | t12-1-timer | t12-2-timer }

default

Sets the timer value to wait in seconds/minutes to default values. Default values for timers are:
- t6-1-timer: 10 seconds
- t8-timer: 4 seconds
- t9-timer: 4 seconds
- t10-timer: 4
- t12-1-timer: 54 mins (+ 8 seconds)
- t12-2-timer: 4 seconds

t6-1-timer t6_1_dur

Default: 10
Specifies the retransmission timer value to guard the location update.
t6_1_dur is the waiting duration in seconds before retransmitting the specific message and must be an integer from 10 through 90.

t8-timer t8_dur

Default: 4
Specifies the retransmission timer value to guard the explicit IMSI detach from the GPRS service procedure.
t8_dur is the waiting duration in seconds before retransmitting the specific message and must be an integer from 1 through 30.
**t9-timer t9_dur**

Default: 4  
Specifies the retransmission timer value to guard the explicit IMSI detach from the non-GPRS service procedure.  
*t9_dur* is the waiting duration in seconds before retransmitting the specific message and must be an integer from 1 through 30.

**t10-timer t10_dur**

Default: 4  
Specifies the retransmission timer value to guard the implicit IMSI detach from the GPRS service procedure.  
*t10_dur* is the waiting duration in seconds before retransmitting the specific message and must be an integer from 1 through 30.

**t12-1-timer minute t12_1_dur**

Default: 54 minutes (plus 8 seconds for transmission delay)  
Specifies the retransmission timer value to control the resetting of SGSN-Reset variable procedure.  
*t12_1_dur* is the waiting duration in minutes before retransmitting reset message for the SGSN Reset variable and must be an integer from 0 through 384.

**t12-2-timer t12_2_dur**

Default: 4  
Specifies the retransmission timer value to guard the SGSN reset procedure.  
*t12_2_dur* is the waiting duration in seconds before retransmitting the specific message and must be an integer from 1 through 120.

**Usage**

Use this command to configure the time, for different procedure timers, to wait before retransmitting a procedure message.  
This command can be repeated for each timer to configure multiple timers.

**Example**

Following command sets the timeout duration of 4 seconds for t8 timer to wait before retransmitting the procedure message to explicitly do the IMSI detach from GPRS service:

```
default timeout t8-timer
```
vlr

This command defines a VLR configuration for use with this Gs service.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Gs Service Configuration
configure > context context_name > gs-service service_name
Entering the above command sequence results in the following prompt:
[context_name]host_name(config-gs-service)#

Syntax

vlr vir_name isdn-number E164_num [ bssap+ ssn ssn ] [ point-code pt_code ]
no vlr vir_name

no
Removes the configured VLR from the Gs service.

vir_name
Specifies the name of the VLR to configure in this Gs mode with ISDN number.
vir_name must be an alpha and/or numeric string of 1 to 63 characters.

isdn-number E164_num
Specifies the VLR number to configure with this command.
E164_num: The ISDN number for the target VLR. Value must be defined according to the E.164 numbering plan and must be a numeric string of 1 to 15 digits.

bssap+ ssn ssn
Specifies the subsystem number to configure with this VLR to use BSSAP+.
ssn: Must be an integer from 1 through 255. Default value is 252.

point-code pt_code
Specifies SS7 address of VLR in point code value to this configured VLR name.
pt_code: Must be in SS7 point code dotted-decimal ###.###.### format or decimal ####### format.

Usage
Use this command to define VLR configuration instances to be associated with the Gs service.
A maximum of 32 VLRs can be configured per Gs service.

Example
Following command configures the VLR named starvlr1 with an ISDN number 12344567, a subsystem number of 252, and a point code value of 123.345.567:

```
vlr starvlr1 isdn-number 12344567 point-code 123.345.567
```
Chapter 149
GT-Format1 Configuration Mode Commands

The GT-Format1 configuration mode is a sub-mode for either the Global Title Translation Association configuration mode or the Global Title Translation Address-Map configuration mode. This sub-mode configures a set of rules used in the global title translation (GTT) process.

Mode

Exec > Global Configuration > GTT Association Configuration > GT-Format1 Configuration

configure > global title translation association instance instance_number > gt-format format_number

Entering the above command sequence results in the following prompt:

[local]host_name(config-gtt-instance-format1)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
end

Exits the configuration mode and returns to the Exec mode.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Change the mode back to the Exec mode.
exit

Exits the configuration mode and returns to the Global configuration mode.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

```
exit
```

Usage
Return to the Global configuration mode.
nature-of-address

Configures the indicator to identify the nature of the address.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > GTT Association Configuration > GT-Format1 Configuration

```
configure > global title translation association instance <instance_number> > gt-format <format_number>
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-gtt-instance-format1)#
```

**Syntax**

```
nature-of-address { international | national | subscriber }
```

- **international**
  Identifies the numbers as international.

- **national**
  Identifies the numbers as matching the national configuration.

- **subscriber**
  Identifies the numbers as subscriber numbers.

**Usage**

Configure the identify of the GT format as national.

**Example**

```
nature-of-address national
```
odd-even-indicator

Configures the bits for matching the global title translation.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > GTT Association Configuration > GT-Format1 Configuration

configure > global title translation association instance instance_number > gt-format format_number

Entering the above command sequence results in the following prompt:

[local]host_name(config-gtt-instance-format1)#

Syntax

odd-even-indicator type

type
• odd: Sets the odd bit for matching the GTT.
• even: Sets the even bit for matching the GTT.
Chapter 150
GT-Format2 Configuration Mode Commands

The GT-Format2 configuration mode is a sub-mode for either the Global Title Translation Association configuration mode or the Global Title Translation Address-Map configuration mode. This sub-mode configures a set of rules used in the global title translation (GTT) process.

Mode

Exec > Global Configuration > GTT Association Configuration > GT-Format2 Configuration

configure > global title translation association instance instance_number > gt-format format_number

Entering the above command sequence results in the following prompt:

[local]host_name(config-gtt-instance-format2)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
end

Exits the configuration mode and returns to the Exec mode.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
del
```

**Usage**
Change the mode back to the Exec mode.
**exit**

Exits the configuration mode and returns to the Global configuration mode.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**
```
exit
```

**Usage**
Return to the Global configuration mode.
translation-type

Configures the translation type to be applied during the translation process.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > GTT Association Configuration > GT-Format2 Configuration

configure > global title translation association instance instance_number > gt-format format_number

Entering the above command sequence results in the following prompt:

[l]ocal host_name(config-gtt-instance-format2)#

Syntax

translation-type number

number

Must be an integer between 0 and 255.
Default is 0

Usage
Use this command to configure the GTT translation type to be applied during global title translation process.

Example

translation-type 232
Chapter 151
GT-Format3 Configuration Mode Commands

The GT-Format3 configuration mode is a sub-mode for either the Global Title Translation Association configuration mode or the Global Title Translation Address-Map configuration mode. This sub-mode configures a set of rules used in the global title translation (GTT) process.

Mode

Exec > Global Configuration > GTT Association Configuration > GT-Format3 Configuration

configure > global title translation association instance instance_number > gt-format format_number

Entering the above command sequence results in the following prompt:

[local]host_name(config-gtt-instance-format3)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
encoding-scheme

Configures the encoding-scheme to use during global title translation (GTT).

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > GTT Association Configuration > GT-Format3 Configuration

```bash
configure > global title translation association instance instance_number > gt-format format_number
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-gtt-instance-format3)#
```

**Syntax**

```bash
encoding scheme scheme_type
```

**scheme_type**
Select one of the following encoding scheme types to determine the encoding type to be used during GTT:

- **bcd-even**: BCD even encoding scheme
- **bcd-odd**: BCD odd encoding scheme
- **nw-specific**: Network specific encoding scheme
- **unknown**: Unknown encoding scheme

**Usage**
Select BCD even encoding for GTT

**Example**

```bash
encoding scheme bcd-even
```
end

Exits the configuration mode and returns to the Exec mode.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Change the mode back to the Exec mode.
exit

Exits the configuration mode and returns to the Global configuration mode.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Return to the Global configuration mode.
numbering-plan

Configures the GTT process to apply one of the numbering-plans during the GT translation process.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > GTT Association Configuration > GT-Format3 Configuration

```
configure > global title translation association instance instance_number > gt-format format_number
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-gtt-instance-format3)#
```

**Syntax**

```plaintext
numbering-plan plan_type
```

**plan_type**
Select one of the following numbering plans be employed during GTT:

- **data**: Data numbering plan
- **generic**: Generic number plan
- **isdn**: ISDN tel numbering plan
- **isdn-mobile**: ISDN mobile numbering plan
- **land-mobile**: Land mobile numbering plan
- **maritime-mobile**: Maritime mobile numbering plan
- **nw-specific**: Private network / network-specific numbering plan
- **telex**: Telex numbering plan
- **unknown**: Unknown numbering plan

**Usage**
Select ISN telephone number plan for GTT process.

**Example**
The following command sets the numbering plan to use during GTT processing to isdn

```plaintext
numbering-plan isdn
```
translation-type

Configures the global title translation (GTT) process to apply a specific number for translation during the GTT process.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > GTT Association Configuration > GT-Format3 Configuration

```
configure > global title translation association instance instance_number > gt-format format_number
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-gtt-instance-format3)#
```

Syntax

```
translation-type number
```

- `number`

  Must be an integer between 0 and 255. Default is 0

Usage

Use this command to define the translation-type to be used during the global title translation process.

Example

```
translation-type 233
```
Chapter 152
GT-Format4 Configuration Mode Commands

The GT-Format4 configuration mode is a sub-mode for either the Global Title Translation Association configuration mode or the Global Title Translation Address-Map configuration mode. This sub-mode configures a set of rules used in the global title translation (GTT) process.

Mode

Exec > Global Configuration > GTT Association Configuration > GT-Format4 Configuration

configure > global title translation association instance instance_number > gt-format format_number

Entering the above command sequence results in the following prompt:

[local]host_name(config-gtt-instance-format4)#

⚠️ **Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
encoding-scheme

Configures the encoding-scheme to use during GTT.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > GTT Association Configuration > GT-Format4 Configuration

configure > global title translation association instance instance_number > gt-format format_number

Entering the above command sequence results in the following prompt:

[local]host_name(config-gtt-instance-format4)#

Syntax

encoding scheme scheme_type

scheme_type

Select one of the following encoding scheme types to determine the encoding type to be used during GTT:

• bcd-even: BCD even encoding scheme
• bcd-odd: BCD odd encoding scheme
• nw-specific: Network-specific encoding scheme
• unknown: Unknown encoding scheme

Usage
Select BCD even encoding for GTT

Example

encoding scheme bcd-even
end

Exits the configuration mode and returns to the Exec mode.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Change the mode back to the Exec mode.
exit

Exits the configuration mode and returns to the Global configuration mode.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Return to the Global configuration mode.
nature-of-address

Configures the indicator to identify the nature of the address.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > GTT Association Configuration > GT-Format4 Configuration

```bash
configure > global title translation association instance instance_number > gt-format format_number
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-gtt-instance-format4)#
```

Syntax

```
nature-of-address { international | national | subscriber }
```

---

**international**
Identifies the numbers as international.

---

**national**
Identifies the numbers as matching the national configuration.

---

**subscriber**
Identifies the numbers as subscriber numbers.

---

Usage
Configure the identify of the GT format as national.

Example

```
nature-of-address national
```
**numbering-plan**

Configures the GTT process to apply one of the numbering-plans during the GT translation process.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > GTT Association Configuration > GT-Format4 Configuration

```
configure > global title translation association instance instance_number > gt-format format_number
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-gtt-instance-format4)#
```

**Syntax**

```
numbering-plan plan_type
```

*plan_type*

Select one of the following numbering plans be employed during GTT:

- **data**: Data numbering plan
- **generic**: Generic number plan
- **isdn**: ISDN tel numbering plan
- **isdn-mobile**: ISDN mobile numbering plan
- **land-mobile**: Land mobile numbering plan
- **maritime-mobile**: Maritime mobile numbering plan
- **nw-specific**: Private network/ network-specific numbering plan
- **telex**: Telex numbering plan
- **unknown**: Unknown numbering plan

**Usage**
Select ISN telephone number plan for GTT process.

**Example**

```
numbering-plan isdn
```
translation-type

Configures the GTT process to apply a specific number for translation during the GTT process.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > GTT Association Configuration > GT-Format4 Configuration
configure > global title translation association instance instance_number > gt-format format_number

Entering the above command sequence results in the following prompt:

[local]host_name(config-gtt-instance-format4)#

**Syntax**

```bash
translation-type number
```

- `number`
  - Must be an integer between 0 and 255.
  - Default is 0.

**Usage**

Use this command to configure the translation-type to be implemented during the global title translation process.

**Example**

```bash
translation-type 231
```
Chapter 153
GTTP Server Group Configuration Mode Commands

The GTTP Server Group Configuration Mode is used to create and manage the GTTP server groups within the context or system.

GTTP server group commands facilitate the setup of the hard disk for CDR storage. They also support accounting and charging functionality within a context, and configuration of a group (list) of charging gateway function (CGF) servers on a per subscriber or per GGSN/P-GW APN level.

**Mode**

Exec > Global Configuration > Context Configuration > GTTP Server Group Configuration

```
configure > context context_name > gtpp group group_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-gtpp-group)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**

Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

exit

**Usage**
Use this command to return to the parent configuration mode.
gtpp attribute

Enables the specification of some of the optional fields in the CDRs that the GSN (GGSN or SGSN) generates and/or how the information is to be presented. Many keywords are also applicable to S-GW and P-GW CDRs.

Product
GGSN
P-GW
SAEGW
SGSN
S-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > GTPP Server Group Configuration

configure > context context_name > gtpp group group_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-gtpp-group)#

Syntax

gtpp attribute { apn-ambr [ include-for-all-bearers | include-for-default-bearer | include-for-non-gbr-bearers ] | apn-ni | apn-selection-mode | charging-characteristic-selection-mode | camel-info | cell-plmn-id | diagnostics | duration-ms | dynamic-flag | dynamic-flag-extension | furnish-charging-information | imei | imsi-unauthenticated-flag | local-record-sequence-number | losdv | ms-timezone | msisdn | node-id | node-id-suffix STRING | pdn-connection-id | pdp-address | pdp-type | pgw-plmn-id | plmn-id | rat | record-extension | record-extensions rat | served-mnai | served-pdp-pdn-address-extension | served-pdp-pdn-address-prefix-length | sgsn-change | sms { destination-number | recording-entity | service-centre } | start-time | stop-time | uli | user-csg-information } +

default gtpp attribute { apn-ambr [ include-for-all-bearers | include-for-default-bearer | include-for-non-gbr-bearers ] | apn-ni | apn-selection-mode | charging-characteristic-selection-mode | cell-plmn-id | diagnostics | duration-ms | dynamic-flag | dynamic-flag-extension | furnish-charging-information | imei | imsi-unauthenticated-flag | local-record-sequence-number | losdv | ms-timezone | msisdn | node-id | pdn-connection-id | pdp-address | pdp-type | pgw-plmn-id | plmn-id | rat | record-extension | record-extensions rat | served-mnai | served-pdp-pdn-address-extension | served-pdp-pdn-address-prefix-length | sgsn-change | sms { destination-number | recording-entity | service-centre } | start-time | stop-time | uli | user-csg-information }

no gtpp attribute { apn-ambr [ include-for-all-bearers | include-for-default-bearer | include-for-non-gbr-bearers ] | apn-ni | apn-selection-mode | charging-characteristic-selection-mode | cell-plmn-id | diagnostics | duration-ms | dynamic-flag | dynamic-flag-extension | furnish-charging-information | imei | imsi-unauthenticated-flag | local-record-sequence-number | losdv | ms-timezone | msisdn | node-id | pdn-connection-id | pdp-address | pdp-type | pgw-plmn-id | plmn-id | rat | record-extension | record-extensions rat | served-mnai | served-pdp-pdn-address-extension | served-pdp-pdn-address-prefix-length | sgsn-change | sms { destination-number | recording-entity | service-centre } | start-time | stop-time | uli | user-csg-information }
gtpp attribute

pdp-address | pdp-type |pgw-plmn-id | plmn-id |rat | recordextension | record-extensions |rat | served-mnai | served-pdp-pdn-address-extension | served-pdp-pdn-address-prefix-length | sgsn-change | served-mnai |sms {destination-number | recording-entity | service-centre} | start-time | stop-time | uli | user-csg-information

default
Resets the default attribute values for this GTPP group configuration.

no
Disables the specified optional field so that the information will not be present in generated CDRs.

apn-ambr [include-for-all-bearers | include-for-default-bearer | include-for-non-gbr-bearers]
Default: Disabled
This keyword controls the inclusion of the optional field “apn-ambr” in the PGW-CDRs in the custom24 GTPP dictionary.

Important: This keyword option will be available only if a valid license is installed. For more information, contact your Cisco account representative.

The APN Aggregate Maximum Bit Rate (AMBR) is a subscription parameter stored per APN. It limits the aggregate bit rate that can be expected to be provided across all non-GBR bearers and across all PDN connections of the same APN. Each of these non-GBR bearers potentially utilize the entire APN AMBR, e.g. when the other non-GBR bearers do not carry any traffic. The APN AMBR is present as part of QoS information.

In 15.0 and later releases, this CLI command should be configured along with the following additional options to support APN-AMBR reporting in SGW-CDRs in all GTPP dictionaries.

•include-for-all-bearers: Includes the APN-AMBR information in SGW-CDRs for all bearers (GBR and NON-GBR)
•include-for-default-bearer: Includes APN-AMBR information in SGW-CDRs only for default bearer.
•include-for-non-gbr-bearers: Includes APN-AMBR information for non-gbr-bearers.

This feature is required to enable post-processing of CDRs to verify MVNO subscribers actual QoS against invoicing systems.

Important: This CLI command and the associated options are not available for products other than S-GW and P-GW. The option “non-gbr-bearers-only” is available in S-GW and P-GW but the other options are available in S-GW only.

In the P-GW implementation, if the CLI command “gtpp attribute apn-ambr” is configured, it will be treated as “gtpp attribute apn-ambr non-gbr-bearers-only”. In case of S-GW/P-GW combo if any of the options is configured, it will be considered that the attribute is available.

apn-ni
Default: Enabled
This keyword controls the inclusion of the optional field “APN” in the x-CDRs.
**apn-selection-mode**

Default: Enabled
This keyword controls the inclusion of the optional field “APN Selection Mode” in the x-CDRs.

**camel-info**

SGSN only
Enter this keyword to include CAMEL-specific fields in SGSN CDRs. Default: Disabled

**cell-plmn-id**

SGSN only
Enter this keyword to enable the system to include the Cell PLMN ID field in the M-CDR. Default: Disabled

**charging-characteristic-selection-mode**

Default: Enabled
This keyword controls the inclusion of the optional field “Charging Characteristic Selection Mode” in the x-CDRs.

**diagnostics**

Default: Disabled
Enables the system to include the Diagnostic field in the CDR that is created when PDP contexts are released. The field will include one of the following values:

- **26** - For GGSN: if the GGSN sends “delete PDP context request” for any other reason (e.g., the operator types “clear subscribers” on the GGSN). For SGSN: The SGSN includes this cause code in the S-CDR to indicate that a secondary PDP context activation request or a PDP context modification request has been rejected due to insufficient resources.

- **36** - For GGSN: this cause code is sent in the G-CDR to indicate the PDP context has been deactivated in the GGSN due to the SGSN having sent a “delete PDP context request” to the GGSN. For SGSN, this cause code is used to indicate a regular MS or network-initiated PDP context deactivation.

- **37** - when the network initiates a QoS modification, the SGSN sends in the S-CDR to indicate that the MS initiation deactivate request message has been rejected with QoS not accepted as the cause.

- **38** - if the GGSN sends “delete PDP context request” due to GTP-C/GTP-U echo timeout with SGSN. If the SGSN sends this cause code, it indicates PDP context has been deactivated due to path failure, specifically GTP-C/GTP-U echo timeout.

- **39** - SGSN only - this code indicates the network (GGSN) has requested a PDP context reactivation after a GGSN restart.

- **40** - if the GGSN sends “delete PDP context request” due to receiving a RADIUS Disconnect-Request message.

**duration-ms**

Specifies that the information contained in the mandatory Duration field be reported in milliseconds instead of seconds (as the standards require). Default: Disabled

**dynamic-flag**

Default: Enabled
This keyword controls the inclusion of the optional field “Dynamic Flag” in the x-CDRs.
**dynamic-flag-extension**

Default: Enabled
This keyword controls the inclusion of the optional field “Dynamic Address Flag Extension” in the x-CDRs. This field is seen in the CDR when the IPv4 address is dynamically assigned for a dual PDP context. This extension field is required in the 3GPP Release 10 compliant CDRs so that the Dual Stack Bearer support is available.

**furnish-charging-information**

Default: Disabled
This keyword controls the inclusion of the optional field “pSFurnishChargingInformation” in the eG-CDRs and PGW-CDRs.

**Important:** The Furnish Charging Information (FCI) feature is applicable to all GTPP dictionaries compliant to 3GPP Rel.7 and 3GPP Rel.8 except custom43 dictionary. This keyword option will be available only if a valid license is installed. For more information, contact your Cisco account representative.

PGW-CDR and eG-CDR will contain FCI only if it is enabled at command level, i.e. using the `gtpp attribute furnish-charging-information` command in GTPP Server Group Configuration mode. Whenever FCI changes, a new Free-Format-Data (FFD) value is either appended to existing FFD or overwritten on the existing FDD depending on Append-Free-Format-Data (AFFD) flag. CDR is not generated upon FCI change.

FCI is supported in main CDR as well as in LOSDV. Whenever a trigger (volume, time, RAT, etc.) happens current available FFD at command level is added to the main body of the CDR. The same FFD at command level is added to the main body of the next CDRs until it is not appended or overwritten by next Credit-Control-Answer message at command level.

In the case of custom43 dictionary, the FCI implementation will be as follows:

- Whenever FCI changes PGW-CDR will generate CDR i.e close old bucket and will have old FCI details in the generated CDR.
- Translation for the PS-Free-Format-Data in CDR will be conversion of hexadecimal values in ASCII format (for numbers 0 to 9) to decimal values as integers.
- PS-Append-Free-Format-Data always OVERWRITE.

**imei**

Default: Disabled
For SGSN: includes the IMEI value in the S-CDR.
For GGSN: includes the IMEISV value in the G-CDR.

**imsi-unauthenticated-flag**

Default: Enabled
This keyword controls the inclusion of the optional field “IMSI Unauthenticated Flag” in the x-CDRs. When the served IMSI is not authenticated, this field “IMSI Unauthenticated Flag” if configured, will be present in the P-GW CDR record for custom35 dictionary. This field is added per 3GPP TS 32.298 v10.7.

**local-record-sequence-number**

Default: Disabled
This keyword provides both the local record sequence number and the Node ID. In the x-CDRs, this field indicates the number of CDRs generated by the node and is unique within the session manager.
The Node ID field is included in the x-CDR for any of several reasons, such as when PDP contexts are released or if partial-CDR is generated based on configuration. The field will consist of a AAA Manager identifier automatically appended to the name of the SGSN or GGSN service.

The name of the SGSN or GGSN service may be truncated, because the maximum length of the Node ID field is 20 bytes. Since each AAA Manager generates CDRs independently, this allows the Local Record Sequence Number and Node ID fields to uniquely identify a CDR.

**Important:** If this keyword is enabled and the **gtpp centralized-lrsn-creation** option is enabled with the **gtpp single-source centralized-lrsn** command, then the Node ID format changes as follows: <1-byte-AAAproxy-restart-counter> <3-byte AAAproxy instance number> <node-id-suffix>. If **gtpp centralized-lrsn-creation** is not enabled, the node-id format for CDRs generated by Sessmgr is as follows: <1-byte Sessmgr restart-value> <3-byte Sessmgr instance number> <node-id-suffix>. If **gtpp centralized-lrsn-creation** is not enabled, the node-id format for CDRs generated by ACSMG is as follows: <1-byte ACSmgr restart-value> <3-byte ACSmgr instance number> <Active charging service-name>.

**losdv**
Default: Enabled
This keyword controls the inclusion of the optional field “List of Service Data” in the x-CDRs.

**ms-timezone**
Default: Enabled
This keyword controls the inclusion of the optional field “MS-Timezone” in the x-CDRs.

**msisdn**
Default: Enabled
This keyword controls the inclusion of the optional field “MSISDN” in the x-CDRs.

**node-id**
Default: Enabled
This keyword controls the inclusion of the optional field “Node ID” in the x-CDRs.

**node-id-suffix STRING**
Default: Disabled
Specifies the configured Node-ID-Suffix to use in the NodeID field of GTPP CDRs as an alphanumeric string of 1 through 16 characters. Each Session Manager task generates a unique NodeID string per GTPP context.

**Important:** The NodeID field is a printable string of the *ndddSTRING* format: *n*: The first digit is the Sessmgr restart counter having a value between 0 and 7. *dd*: The number of sessmgr instances. Uses the specified NodeID-suffix in all CDRs. The “Node-ID” field consists of sessMgr Recovery counter (1 digit) n + AAA Manager identifier (3 digits) ddd + the configured Node-Id-suffix (1 to 16 characters) STRING. If the centralized LRSN feature is enabled, the “Node-ID” field will consist of only the specified NodeID-suffix (NodeID-prefix is not included). If this option is not configured, then GTPP group name will be used instead (For default GTPP groups, context-name will be used).

**Important:** If this node-id-suffix is not configured, the GGSN uses the GTPP context name as the Node-id-suffix (truncated to 16 characters) and the SGSN uses the GTPP group named as the node-id-suffix.
pdsn-connection-id
Default: Enabled
This keyword controls the inclusion of the optional field “PDN Connection ID” in the x-CDRs.

pdp-address
Default: Enabled
This keyword controls the inclusion of the optional field “PDP Address” in the x-CDRs.

pdp-type
Default: Enabled
This keyword controls the inclusion of the optional field “PDP Type” in the x-CDRs.

pgw-plmn-id
Default: Enabled
This keyword controls the inclusion of the optional field “PGW PLMN-ID” in the x-CDRs.

plmn-id [ unknown-use ]
Default: Enabled
For SGSN, reports the SGSN PLMN Identifier value (the RAI) in the S-CDR provided if the dictionary supports it.
For GGSN, reports the SGSN PLMN Identifier value (the RAI) in the G-CDR if it was originally provided by the SGSN in the GTP create PDP context request. It is omitted if the SGSN does not supply one.
Normally when SGSN PLMN-id information is not available, the attribute sgsnPLMNIdentifier is not included in the CDR. This keyword enables the inclusion of the sgsnPLMNIdentifier with a specific value when the SGSN PLMN-id is not available.
unknown-use hex_num: is aa hexadecimal number from 0x0 through 0xFFFFFF that identifies a foreign SGSN that has not provided a PLMN-id. For GGSN only.

rat
Default: Enabled
For SGSN: includes the RAT (identifies the radio access technology type) value in the S-CDR.
For GGSN: includes the RAT (identifies the radio access technology type) value in the G-CDR.

recordextension
Default: Disabled
This keyword controls the inclusion of the optional field “RecordExtension” in the x-CDRs.

record-extensions rat
Default: Disabled
Enables network operators and/or manufacturers to add their own recommended extensions to the CDRs according to the standard record definitions from 3GPP TS 32.298 Release 7 or higher.

served-mnai
Default: Disabled
This keyword controls the inclusion of the optional field “Served MNAI” in the x-CDRs.
served-pdp-pdn-address-extension
Default: Disabled
In support of IPv4v6 dual-stack PDP address types, this keyword causes the service to include IPv4v6 address information in the CDR. The IPv4 address goes in the Served PDP PDN Address Extension field and the IPv6 address goes in the Served PDP Address or Served PDP PDN Address field.

**Important:** This attribute will not be displayed if the GTPP dictionary is set to custom34.

served-pdp-pdn-address-prefix-length
Default: Enabled
In support of IPv6 prefix delegation, this keyword causes the service to include this field “Served PDP PDN Address” in the x-CDRs.
If this field is configured, the servedPDPPDNAddress field will support reporting the IPv6 prefix length as outlined in 3GPP 32.298. The prefix length will only be reported if:
- it is configured
- it is not the default length of 64
- it is an IPv6 or IPv4v6 call

sgsn-change
Default: Enabled
This keyword is specific to SGSN and is license restricted.
This keyword controls the inclusion of the S-CDR attribute “SGSN Change” in the S-CDRs. It is enabled by default and the attribute “SGSN Change” is included in the S-CDRs by default.

sms { destination-number | recording-entity | service-centre }
This keyword is specific to the SGSN.
Entering this keyword causes the inclusion of an SMS-related field in the SMS-MO-CDR or SMS-MT-CDR.
- **destination-number:** Includes the “destinationNumber” field in the SMS-MO-CDR or SMS-MT-CDR.
- **recording-entity:** Includes the “recordingEntity” field in the SMS-MO-CDR or SMS-MT-CDR.
- **service-centre:** Includes the “serviceCentre” field in the SMS-MO-CDR or SMS-MT-CDR.

start-time
Default: Enabled
This keyword controls the inclusion of the optional field “Start-Time” in the x-CDRs.

stop-time
Default: Enabled
This keyword controls the inclusion of the optional field “Stop-Time” in the x-CDRs.

uli
Default: Enabled
This keyword controls the inclusion of the optional field “User Location Information” in the x-CDRs.

user-csg-information
Default: Disabled
This keyword controls the inclusion of the optional field “User CSG Information” in the x-CDRs.

**Important:** Currently, UCI values are only supported for SGW-CDRs. This attribute will not be displayed if the GTPP dictionary is set to custom11, custom34, or custom35.

```
+ Indicates that this command can be entered multiple times to configure multiple attributes.
```

**Usage**

This command dictates some of the optional information fields that should be reported in CDRs generated by the GGSN. In addition, it controls how the information for some of the mandatory fields are reported. Fields described as optional by the standards but not listed above will always be present in the CDRs, except for Record Extensions (which will never be present).

**Example**

The following command disables the inclusion of the field “SGSN Change” in the S-CDR:

```
no gtpp attribute sgsn-change
```

**Example**

The following command dictates that the time provided in the Duration field of the CDR is reported in milliseconds:

```
gtpp attribute duration-ms
```
gtpp charging-agent

Configures the IP address and port of the system interface within the current context used to communicate with the CGF or the GSS.

**Product**
- GGSN
- P-GW
- SAEGW
- SGSN
- S-GW

**Privilege**
- Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > GTPP Server Group Configuration

```
configure > context context_name > gtpp group group_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-gtpp-group)#
```

**Syntax**

```
gtpp charging-agent address ip_address [ port port ]
```

```
no gtpp charging-agent
```

- **no**
  Removes a previously configured charging agent address.

- **address ip_address**
  Specifies the IP address of the interface configured within the current context that is used to transmit G-CDR records to the CGF or the GSS.
  `ip_address` is expressed in IPv4 dotted-decimal notation.

- **port port**
  Specifies the Charging Agent UDP port as an integer from 1 through 65535. If the port is not defined, the default port number 49999 will be used.

**Important:** Configuring GTPP charging-agent on port 3386 may interfere with ggsn-service configured with the same ip address.
Usage

This command can be used to establish a UDP interface to connect to the GSS or this command can establish a Ga interface to connect to the CFG. These interfaces must exist in the same context in which GTPP functionality is configured (refer to the `gtpp` commands in this chapter).

This command instructs the system as to what interface to use. The IP address supplied is also the address by which the GGSN/SGSN is known to the CGF or the GSS. Therefore, the IP address used for the Ga or UDP interface could be identical to one bound to a GGSN/SGSN service (a Gn interface).

If no GGSN/SGSN services are configured in the same context as the Ga/UDP interface, the address configured by this command is used to receive unsolicited GTPP packets.

Example

The following command configures the system to use the interface with an IP address of 192.168.13.10 as the accounting interface with port 20000 to the CGF:

```bash
    gtpp charging-agent address 192.168.13.10
    gtpp charging-agent address 192.168.13.10 port 20000
```
**gtpp data-request sequence-numbers**

Configures the range of sequence numbers to be used in the GTPP data record transfer record (DRT). Use this command to set the start value for the sequence number.

**Product**
- GGSN
- P-GW
- SAEGW
- SGSN
- S-GW

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration > Context Configuration > GTPP Server Group Configuration

```
configure > context context_name > gtpp group group_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-gtpp-group)#
```

**Syntax**

```
gtpp data-request sequence-numbers start { 0 | 1 }
```

**default gtpp data-request sequence-numbers start**

<table>
<thead>
<tr>
<th>default</th>
<th>Default is 0 (zero).</th>
</tr>
</thead>
</table>

| start { 0 | 1 } |
|----------------|
| Specifies the value of the start sequence number for the GTPP Data Record Transfer Request. Default: 0 |
| - 0: Designates the start sequence number as 0. |
| - 1: Designates the start sequence number as 1. |

**Usage**

When the GGSN/P-GW/SGSN is configured to send GTPP echo request packets, the SGSN always uses 0 as the sequence number in those packets. Re-using 0 as a sequence number in the DRT packets is allowed by the 3GPP standards; however, this CLI command ensures the possibility of inter-operating with CGFs that cannot properly handle the re-use of sequence number 0 in the echo request packets.

**Example**

The following command sets the sequence to start at 1.

```
gtpp data-request sequence-numbers start 1
```
**gtpp deadtime**

Configures the amount of time the GGSN/SGSN waits before attempting to communicate with a CGF that was previously marked as unreachable (non-responsive).

**Product**
- GGSN
- P-GW
- SAEGW
- SGSN
- S-GW

**Privilege**
Security Administrator, Administrator

**Mode**
- Exec > Global Configuration > Context Configuration > GTPP Server Group Configuration
- `configure > context context_name > gtpp group group_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-gtpp-group)#
```

**Syntax**

```
gtpp deadtime time
```

```
default gtpp deadtime
```

**default**
- `default`
  - Resets the deadtime to the default of 120 seconds.

**time**
- `time`
  - Specifies the amount of time (in seconds) that must elapse before the system attempts to communicate with a CGF that was previously unreachable.
  - `time` is an integer from 1 to 65535. Default: 120

**Usage**

If the system is unable to communicate with a configured CGF, after a pre-configured number of failures the system marks the CGF as being down.
This command specifies the amount of time that the system waits prior to attempting to communicate with the downed CGF.
Refer to the `gtpp detect-dead-server` and `gtpp max-retries` commands for additional information on the process the system uses to mark a CGF as down.

**Example**

The following command configures the system to wait 60 seconds before attempting to re-communicate with a CGF that was marked as down:

```
gtpp deadtime 60
```
gtpp dead-server suppress-cdrs

Configures the action the GGSN or the SGSN will take on CDRs generated during a communication failure between the GGSN or the SGSN and the GTPP servers.

Product
- GGSN
- P-GW
- SAEGW
- SGSN
- S-GW

Privilege
- Security Administrator, Administrator

Mode
- Exec > Global Configuration > Context Configuration > GTPP Server Group Configuration
- `configure > context context_name > gtpp group group_name`

Entering the above command sequence results in the following prompt:

```
/context_name/host_name(config-gtpp-group)#
```

Syntax

```
[ no | default ] gtpp dead-server suppress-cdrs
```

- **no**
  - Removes the suppression instruction from the configuration and sets the CDR suppression mode as disabled.

- **default**
  - Resets to the default mode: disable suppression of CDRs when GTPP server detected as “dead” or unreachable.

Usage

**For the GGSN/P-GW:** This command works in conjunction with the `gtpp detect-dead-server` to set an action when a communication failure is detected between the GGSN and a configured GTPP server. It disables the archiving of CDRs on the system when the GTPP server is unreachable or dead.

**For the GGSN, P-GW, and SGSN:** During a communication or server failure, the GGSN, P-GW, or SGSN typically retains the GTPP requests until the system buffer runs out of resources. This command enables suppression of the CDRs, so with this command the GGSN, P-GW, or the SGSN will start purging all CDRs associated with this GTPP group as soon as the GGSN/P-GW/SGSN detects that the GTPP server is down or that a communication failure has occurred. The CDRs generated, for the period while the server is down/unreachable, will also be purged.

Example

The following command configures the system to start purging CDRs when a communication failure with a server is detected:

```
gtpp dead-server suppress-cdrs
```
**gtpp detect-dead-server**

Configures the number of consecutive communication failures that could occur before the system marks a CGF as “dead” (unreachable).

**Product**
- GGSN
- P-GW
- SAEGW
- SGSN
- S-GW

**Privilege**
- Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > GTPP Server Group Configuration

```
configure > context context_name > gtpp group group_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-gtpp-group)#
```

**Syntax**

```
gtpp detect-dead-server consecutive-failures max_number
```

```
default gtpp detect-dead-server consecutive-failures
```

```
default
```

Resets the system to the default number of consecutive failures.

```
consecutive-failures max_number
```

Default: 5

Specifies the number of failures that could occur before marking a CGF as down as an integer from 0 through 1000. If 0 (zero) is the value entered, the system will mark the CGF as dead after a single instance of max-retries has been attempted with no success, regardless of configured deadtime.

**Usage**

This command works in conjunction with the **gtpp max-retries** parameter to set a limit to the number of communication failures that can occur with a configured CGF.

The **gtpp max-retries** parameter limits the number of attempts to communicate with a CGF. Once that limit is reached, the system treats it as a single failure. The **gtpp detect-dead-server** parameter limits the number of consecutive failures that can occur before the system marks the CGF as down and communicate with the CGF of next highest priority.

If all of the configured CGFs are down, the system ignores the detect-dead-server configuration and attempt to communicate with highest priority CGF again.

If the system receives a GTPP Node Alive Request, Echo Request, or Echo Response message from a CGF that was previously marked as down, the system immediately treats it as being active.
Refer to the `gtp max-retries` command for additional information.

**Example**

The following command configures the system to allow 8 consecutive communication failures with a CGF before it marks it as down:

```
gtp detect-dead-server consecutive-failures 8
```
**gtpp dictionary**

Designates specific dictionary used by GTPP for specific context.

**Product**
- GGSN
- P-GW
- SAEGW
- SGSN
- S-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > GTPP Server Group Configuration

`configure > context context_name > gtpp group group_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-gtpp-group)#
```

**Syntax**

```
gtpp dictionary { custom1 | custom10 | custom11 | custom12 | custom13 | custom14 |
custom15 | custom16 | custom17 | custom18 | custom19 | custom20 | custom21 | custom22 | custom23 | custom24 | custom25 | custom26 | custom27 | custom28 | custom29 | custom30 | custom31 | custom32 | custom33 | custom34 | custom35 | custom36 | custom37 | custom38 | custom39 | custom4 | custom40 | custom41 | custom42 | custom43 |
custom44 | custom45 | custom46 | custom47 | custom48 | custom49 | custom5 | custom50 | custom51 | custom52 | custom53 | custom54 | custom55 | custom56 | custom57 | custom58 | custom59 | custom6 | custom60 | custom7 | custom8 | custom9 | standard }
```

default gtpp dictionary

```
default
```

Configures the default dictionary.

```
custom1
```

Custom-defined dictionary. It conforms to TS 32.015 v 3.6.0 for R99. It supports the encoding of IP addresses in text format for G-CDRs.

```
custom2
```

Custom-defined dictionary.

```
custom3
```

Custom-defined dictionary. It conforms to TS 32.015 v 3.6.0 for R99 but it does support the encoding of IP addresses in binary format for CDRs.
Custom-defined dictionary. It conforms to TS 32.015 v 3.6.0 for R99 except that:
- the Data Record Format Version information element contains 0x1307 instead of 0x1308
- “QoSRequested” is not present in the LoTV containers
- “QoSnegotiated” is added only for the first container and the container after a QoS change

Custom-defined dictionaries.

Custom-defined dictionaries for GGSN only.

Custom-defined dictionary for customization of G-CDR records for GGSN only. This is compliant to 3GPP TS 32.298 (R6 v 6.5.0) for proprietary fields and encoding.

Custom-defined dictionary for customization of S-CDR records for SGSN only. This is compliant to 3GPP TS 32.298 (R6 v 6.6.0) for proprietary fields and encoding.

Custom-defined dictionaries for GGSN only.

Custom-defined dictionaries based on 3GPP 32.298 v6.4.1 for SGSN only.
- custom31: Custom-defined dictionary for S-CDR encoding. Includes a field appended for PLMN-ID.
- custom33: Custom-defined dictionary for S-CDR encoding. Includes a field appended for PLMN-ID and does not support diagnostic or SGSN-change fields.

Default: Enabled
A dictionary conforming to TS 32.215 v 4.6.0 for R4 (and also R5 - extended QoS format).

Usage

Use this command to designate specific dictionary used by GTPP for specific context.

Important: Note that the following warning message will be displayed whenever an existing GTPP dictionary is being changed or a new GTPP dictionary is configured irrespective of whether or not the calls are active on the system.
Warning: It is not recommended to change the dictionary when the system has active calls.
Are you sure? [Yes|No]: n

Important: This change will require user's input on the CLI console for GTPP dictionary configuration / change.
The following command configures the system to use custom3 dictionary to encode IP address in Binary format in G-CDRs:

```
gtpp dictionary custom3
```
gtpp duplicate-hold-time

Configures the number of minutes to hold onto CDRs that are possibly duplicates while waiting for the primary CGF to come back up.

Product
GGSN
P-GW
SAEGW
SGSN
S-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > GTPP Server Group Configuration

configure > context context_name > gtpp group group_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-gtpp-group)#

Syntax

gtpp duplicate-hold-time minutes minutes

default gtpp duplicate-hold-time

default

Resets the configuration to the default value of 60 minutes for the duplicate hold time.

minutes

When the primary CGF is down, the number of minutes to hold onto CDRs that may be duplicates. minutes must be an integer from 1 to 10080. Default is 60.

Usage

Use this command to configure how long to hold onto CDRs, that are possibly duplicates, while waiting for the primary CGF to come back up. If the GGSN determines that the primary CGF is down, CDRs that were sent to the primary CGF, but not acknowledged, are sent by the GGSN to the secondary CGF as “possibly duplicates”. When the primary CGF comes back up, the GGSN uses GTPP to determine whether the possibly duplicate CDRs were received by the primary CGF. Then the secondary CGF is told whether to release or cancel those CDRs. This command configures how long the system should wait for the primary CGF to come back up. As soon as the configured time expires, the secondary CGF is told to release all of the possibly duplicate CDRs.

Example

Use the following command to set the amount of time to hold onto CDRs to 2 hours (120 minutes):

    gtpp duplicate-hold-time minutes 120
gtpp echo-interval

Configures the frequency at which the system sends GTPP echo packets to configured CGFs.

Product
- GGSN
- P-GW
- SAEGW
- SGSN
- S-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > GTPP Server Group Configuration
configure > context context_name > gtpp group group_name

Syntax

```
gtpp echo-interval time

default | no } gtpp echo-interval

default
Resets the configuration to the default echo-interval of 60 seconds.

no
Disables the use of the echo protocol except for the scenarios described in the Usage section for this command.

time
Specifies the number of seconds for sending GTPP echo packets as an integer from 60 to 3600. Default: 60.
```

Usage
The GTPP echo protocol is used by the system to ensure that it can communicate with configured CGFs. The system initiates this protocol for each of the following scenarios:

- Upon system boot
- Upon the configuration of a new CGF server on the system using the `gtpp server` command as described in this chapter
- Upon the execution of the `gtpp test accounting` command as described in the Exec Mode Commands chapter of this reference
Upon the execution of the `gtpp sequence-numbers private-extensions` command as described in this chapter,

The echo-interval command is used in conjunction with the `gtpp max-retries` and `gtpp timeout` commands as described in this chapter.

In addition to receiving an echo response for this echo protocol, if we receive a GTPP Node Alive Request message or a GTPP Echo Request message from a presumed dead CGF server, we will immediately assume the server is active again.

The alive/dead status of the CGFs is used by the AAA Managers to affect the sending of CDRs to the CGFs. If all CGFs are dead, the AAA Managers will still send CDRs, (refer to the `gtpp deadtime` command), albeit at a slower rate than if a CGF were alive. Also, AAA Managers independently determine if CGFs are alive/dead.

**Example**

The following command configures an echo interval of 120 seconds:

```
gtpp echo-interval 120
```
**gtpp egcdr**

Configures the eG-CDR and P-CDR (P-GW CDR) parameters and triggers.

**Product**
- GGSN
- P-GW
- SAEGW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > GTPP Server Group Configuration

```
configure > context context_name > gtpp group group_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-gtpp-group)#
```

**Syntax**

```
gtpp egcdr { closure-reason admin-disconnect | management-intervention | normal-release } | final-record { [ include-content-ids | all | only-with-traffic ] } | closing-cause { same-in-all-partials | unique } ] | losdv-max-containers max_losdv_containers | lotdv-max-containers max_lotdv_containers | rulebase-max-length rulebase_name_max_length | service-data-flow threshold { interval interval | volume { downlink bytes | uplink bytes } | total bytes | uplink bytes | downlink bytes } | service-idle-timeout { 0 | service_idle_timeout } }
```

```
default gtpp egcdr { closure-reason admin-disconnect | final-record include-content-ids | only-with-traffic closing-cause same-in-all-partials | losdv-max-containers | lotdv-max-containers | service-idle-timeout 0 }
```

```
no gtpp egcdr { rulebase-max-length | service-data-flow threshold { interval | volume { downlink | uplink } | total | uplink | downlink } } }
```

---

**Important:** This behavioral change is limited to PGW-CDR Release 8 dictionaries only.

**closing-reason:** Configures the record closing reason for PGW-CDR.

**management-intervention:** Specifies to send Management-Intervention as causeForRecordClosing in PGW-CDRs. By default, Management-Intervention will be sent as the record closure reason for PGW-CDRs.
• **normal-release**: Specifies to send Normal Release as causeForRecordClosing in PGW-CDRs.

```plaintext
final-record [ [ include-content-ids { all | only-with-traffic } ] [ closing-cause { same-in-allpartials | unique } ] ]
```

Enables configuration of the final eG-CDR/P-CDR.

• **include-content-ids**: Controls which content-ids are being included in the final eG-CDR/P-CDR.
  - **all**: Specifies that all content-ids be included in the final eG-CDR/P-CDRs.
  - **only-with-traffic**: Specifies that only content-ids with traffic be included in the final eG-CDR/P-CDRs.

• **closing-cause**: Configures closing cause for the final eG-CDR/P-CDR.
  - **same-in-allpartials**: Specifies that the same closing cause is to be included for multiple final eG-CDR/P-CDRs.
  - **unique**: Specifies that the closing cause for final eG-CDR/P-CDRs is to be unique.

```plaintext
losdv-max-containers max_losdv_containers
```

Specifies the maximum number of List of Service Data Volume (LoSDV) containers in one eG-CDR/P-CDR.

*max_losdv_containers* must be an integer from 1 through 255.
Default: 10

```plaintext
lotdv-max-containers max_lotdv_containers
```

Specifies the maximum number of List of Traffic Data Volume (LoTDV) containers in one eG-CDR/P-CDR.

*max_lotdv_containers* must be an integer from 1 through 8.
Default: 8

```plaintext
rulebase-max-length rulebase_name_max_length
```

Specifies the maximum character length of charging rulebase name in LOSDVs of eG-CDR/P-GW-CDR.

*rulebase_name_max_length* must be an integer from 0 through 63. Zero (0) means the rulebase name is added as-is.
Default: None. That is, full (un-truncated) charging rulebase name will go in LOSDVs of eG-CDR/P-GW-CDR.

```plaintext
service-data-flow threshold { interval interval | volume { downlink bytes [ uplink bytes ] | total bytes | uplink bytes [ downlink bytes ] } }
```

Configures the thresholds for closing a service data flow container within an eG-CDR/P-CDR.

• **interval interval**: Specifies the time interval (in seconds) to close the eG-CDR/P-CDR if the minimum time duration thresholds for service data flow containers satisfied in flow-based charging. The interval is an integer from 60 through 40000000. Default: Disabled

• **volume { downlink bytes [ uplink bytes ] | total bytes | uplink bytes [ downlink bytes ] }**: Specifies the volume octet counts for the generation of the interim eG-CDR/P-CDRs to the service data flow container in FBC.
  - **downlink bytes**: Specifies the limit for the number of downlink octets after which the eG-CDR/P-CDR is closed.
  - **total bytes**: Specifies the limit for the total number of octets (uplink+downlink) after which the eG-CDR/P-CDR is closed.
  - **uplink bytes**: Specifies the limit for the number of uplink octets after which the eG-CDR/P-CDR is closed.
bytes must be an integer from 10000 through 400000000.

A service data flow container has statistics for an individual content ID. When the threshold is reached, the service data flow container is closed.

In 12.3 and earlier releases, when the CLI command `gtpp egcdr service-data-flow threshold interval` was configured to ‘n’ seconds, the difference between “timeOfFirstUsage” and “timeOfReport” of LOSDV was always ‘n’ seconds for the LOSDVs closed due to “service-data-flow” threshold. Here, changeTime of LOSDV was reported incorrectly. It was always timeOfFirstUsage + ‘n’. This does not hold true when the traffic for a particular content ID was not continuous.

In StarOS release 14.0 and later, when the command `gtpp egcdr service-data-flow threshold interval` is configured to ‘n’ seconds, the difference between “timeOfFirstUsage” and “timeOfReport” of LOSDV can be any value between 1 and ‘n’ seconds depending on the continuity of traffic. If the traffic is not continuous, the difference is less than ‘n’ seconds. And if the traffic is continuous the difference will be ‘n’ seconds. When this CLI command is configured in the GTPP Server Group Configuration mode, each LOSDV will be closed at configured regular interval after the arrival of first packet.

**service-idle-timeout { 0 | service_idle_timeout}**

 Specifies a time period during which if no data is reported for a service flow, the service container is closed and added to eG-CDR/P-CDR (as part of LOSDV container list) with service condition change as ServiceIdleOut.

0: Specifies there is no service-idle-timeout trigger.

*service_idle_timeout* is an integer from 10 through 86,400. Default: 0

**Usage**

Use this command to configure individual triggers for eG-CDR/P-CDR generation.

**Example**

Use the following command to set the maximum number of LoSDV containers to 7:

```
gtpp egcdr losdv-max-containers 7
```
**gtpp error-response**

Configures the response when the system receives an error response after transmitting a DRT (data record transfer) request.

**Product**

GGSN

P-GW

SAEGW

SGSN

S-GW

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > GTPP Server Group Configuration

```
configure > context context_name > gtpp group group_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-gtpp-group)#
```

**Syntax**

```
gtpp error-response { discard-cdr | retry-request }
```

**default gtpp error-response**

- **default**
  
  Resets the system’s configuration to the default value for error-response. Default is retry-request.

- **discard-cdr**
  
  Purges the request upon receipt of an error response and not to retry.

- **retry-request**
  
  Retries sending a DRT after receiving an error response. This is the default behavior.

**Usage**

This command configures the system’s response to receiving an error message after sending a DRT request.

**Example**

```
gtpp error-response discard-cdr
```
**gtpp max-cdrs**

Configures the maximum number of charging data records (CDRs) to be included in a packet.

**Product**
- GGSN
- P-GW
- SAEGW
- SGSN
- S-GW

**Privilege**
- Security Administrator, Administrator

**Mode**

```
Exec > Global Configuration > Context Configuration > GTPP Server Group Configuration
configure > context context_name > gtpp group group_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-gtpp-group)#
```

**Syntax**

```
gtpp max-cdrs max_cdrs [ wait-time wait_time ]
default gtpp max-cdrs
```

- **default**
  Sets the default configuration.

- **max_cdrs**
  Specifies the maximum number of CDRs to insert in a single packet as an integer from 1 through 255.
  Default: 1

- **wait-time wait_time**
  Specifies the number of seconds the GSN waits to send the packet while accumulating CDRs as defined by `max-cdrs`. If the `wait-time` interval expires before `max-cdrs` is reached, this keyword over-rides and the packet is sent. Default: Disabled
  `wait_time` is an integer from 1 through 300.

**Important:** The `wait-time` interval can only be enabled if the value for `max-cdrs` is greater than 1.

**Usage**

The system places CDRs into a packet until either `max-cdrs` is met, `wait-time` times out, or the maximum PDU size, configured by the `gtpp max-pdu-size` command, is met.

The `gtpp max-pdu-size` and the `wait-time` parameters take priority over `max-cdrs`. 
**Important:** This command’s configuration is ignored if CDRs are stored on an SMC hard disk.

**Example**

The following command configures the system to place a maximum of 10 CDRs in a single GTPP packet with a wait-time of 30 seconds:

```
gtp max-cdrs 10 wait-time 30
```
gtpp max-pdu-size

Configures the maximum payload size of a single GTPP packet that could be sent by the system.

**Product**
- GGSN
- P-GW
- SAEGW
- SGSN
- S-GW

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration > Context Configuration > GTPP Server Group Configuration
- configure > context context_name > gtpp group group_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-gtpp-group)#
```

**Syntax**

- `gtpp max-pdu-size pdu_size`
- `default gtpp max-pdu-size`

**Usage**

The GTPP packet contains headers (layer 2, IP, UDP, and GTPP) followed by the CDR. Each CDR contains one or more volume containers. If a packet containing one CDR exceeds the configured maximum payload size, the system creates and send the packet containing the one CDR regardless. The larger the packet data unit (PDU) size allowed, the more volume containers that can be fit into the CDR. The system performs standard IP fragmentation for packets that exceed the system’s maximum transmission unit (MTU).

**Important:** The maximum size of an IPv4 PDU (including the IPv4 and subsequent headers) is 65,535. However, a slightly smaller limit is imposed by this command because the system’s max-pdu-size doesn't include the IPv4 and UDP headers, and because the system may need to encapsulate GTPP packets in a different/larger IP packet (for sending to a backup device).
Example

The following command configures a maximum PDU size of 2048 octets:

```
gtp max-pdu-size 2048
```
gtpp max-retries

Configures the maximum number of times the system attempts to communicate with an unresponsive CGF.

Product
GGSN
P-GW
SAEGW
SGSN
S-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > GTPP Server Group Configuration
configure > context context_name > gtpp group group_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-gtpp-group)#

Syntax

gtpp max-retries max_attempts

default gtpp max-retries

Usage

This command works in conjunction with the gtpp detect-dead-server and gtpp timeout parameters to set a limit to the number of communication failures that can occur with a configured CGF. When the value specified by this parameter is met, a failure is logged. The gtpp detect-dead-server parameter specifies the number of consecutive failures that could occur before the server is marked as down. In addition, the gtpp timeout command controls the amount of time between re-tries. If the value for the max-retries is met, the system begins storing CDRs in Random Access Memory (RAM). The system allocates memory as a buffer, enough to store one million CDRs for a fully loaded chassis (a maximum of one outstanding CDR per PDP context). Archived CDRs are re-transmitted to the CGF until they are acknowledged or the system’s memory buffer is exceeded.

Example

The following command configures the maximum number of re-tries to be 8.
gtpp max-retries 8
gtpp mbms bucket

Configures the traffic data volume (bucket) limit of charging buckets due to QoS changes of tariff time that can occur before a G-MBMS-CDR should be closed.

Product
GGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > GTPP Server Group Configuration

configure > context context_name > gtpp group group_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-gtpp-group)#

Syntax

gtpp mbms buckets number
[ no ] gtpp mbms buckets

no

Disables the configured traffic data volume bucket limits trigger for G-MBMS-CDR generation for MBMS user service data.

number

Specifies the number of statistics container changes due to QoS changes or tariff time that can occur before a G-MBMS-CDR should be closed as an integer from 1 through 4. Default: 4

Usage

Use this command to configure the traffic data volume (bucket) based G-MBMS-CDR generation triggers for MBMS user data service.

Example

The following command configures the bucket-based trigger to generate G-MBMS-CDRs after changes in 2 container:

gtpp mbms buckets 2
**gtpp mbms interval**

Configures the interval duration for interval-based triggers for GTPP MBMS Charging Data Record (G-MBMS-CDR) generation.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > GTPP Server Group Configuration

```
configure > context context_name > gtpp group group_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-gtpp-group)#!
```

**Syntax**

```
gtpp mbms interval duration_sec

no gtpp mbms interval
```

- **no**
  
  Disables the interval-based trigger for G-MBMS-CDR generation for MBMS user service data.

- **duration_sec**
  
  Specifies the normal time duration (in seconds) that must elapse before closing an accounting record provided that any or all of the following conditions occur:
  
  - Downlink traffic volume is reached within the time interval
  - Tariff time based trigger occurred within the time interval
  - Data volume (up and downlink) bucket trigger occurred within the time interval

  **duration_sec** is an integer from 60 through 40,000,000. Default: Disabled

**Usage**

Use this command to configure the G-MBMS-CDR generation triggers for MBMS user data service.

**Example**

The following command configures the interval-based trigger to generate G-MBMS-CDRs in every 60 seconds:

```
gtpp mbms interval 60
```
gtpp mbms tariff

Configures the tariff slots for tariff-based triggers for GTPP MBMS Charging Data Record (G-MBMS-CDR) generation.

Product
GGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > GTPP Server Group Configuration
configure > context context_name > gtpp group group_name

Entering the above command sequence results in the following prompt:
[context_name]host_name(config-gtpp-group)#

Syntax

gtpp mbms tariff time1 mins hours [ time2 mins hours [ time3 mins hours [ time4 mins hours ] ] ]

no gtpp mbms tariff

Specifies time-of-day time values to close the current statistics container (but not necessarily the accounting record). Default: Disabled

**Important:** The system assumes that the billing system uses the day/date to determine if the statistics container represents an actual tariff period.

For each of the different tariff times, the following parameters must be configured:

- **mins:** Minute of the hour, an integer from 0 through 59.
- **hours:** Hour of the day, an integer from 0 through 23.

Usage
Use this command to configure the tariff-time-based triggers for G-MBMS-CDR generation in MBMS user data service.

Example
The following command configures the tariff-time-based trigger to generate G-MBMS-CDRs every day at 11 hours and 30 min:

gtpp mbms tariff time1 30 11
gtpp mbms volume

Configures the download traffic data volume based trigger for GTPP MBMS Charging Data Record (G-MBMS-CDR) generation.

Product
GGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > GTPP Server Group Configuration

configure > context context_name > gtpp group group_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-gtpp-group)#

Syntax

gtpp mbms volume download_bytes

no gtpp mbms volume

no

Disables the configured download traffic data volume based trigger for G-MBMS-CDR generation for MBMS user service data.

volume download_bytes

Specifies the threshold of downlink data volumes that (in bytes) must be met before a G-MBMS-CDR should be closed as an integer from 100000 through 400000000. Default: Disabled

Usage

Use this command to configure the traffic data volume (download) based G-MBMS-CDR generation triggers for MBMS user data service.

Example

The following command configures the traffic data volume (download) limit to trigger to generate G-MBMS-CDRs after reaching 150,000 octets:

    gtpp mbms volume download_bytes
gtpp redirection-allowed

Configures the system to allow/disallow the redirection of CDRs when the primary CGF is unavailable.

**Product**
- GGSN
- P-GW
- SAEGW
- SGSN
- S-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > GTPP Server Group Configuration

```
configure > context context_name > gtpp group group_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-gtpp-group)#
```

**Syntax**

```
[ default | no ] gtpp redirection-allowed
```

- **default**
  
  Resets the system to allow redirection of CDRs.

- **no**
  
  Removes the redirection definition from the configuration.

**Usage**

This command allows operators to better handle erratic network links, without having to remove the configuration of the backup server(s) via the **no gtpp server** command. This functionality is enabled by default.

If the **no gtpp redirection-allowed** command is executed, the system only sends CDRs to the primary CGF. If that CGF goes down, the system will buffer the CDRs in memory until the CGF comes back or until the system runs out of buffer memory. In addition, if the primary CGF announces its intent to go down (with a GTPP Redirection Request message), the system responds to that request with an error response.

**Example**

The following command configures the system to allow the redirection of CDRs when the primary CGF is unavailable:

```
default gtpp redirection-allowed
```
gtpp redirection-disallowed

This command has been obsoleted and is replaced by the gtpp redirection-allowed command.
gtpp server

Configures the charging gateway function (CGF) accounting server(s) with in GTPP server group that the system is to communicate with.

**Product**

GGSN
P-GW
SAEGW
SGSN
S-GW

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > GTPP Server Group Configuration

configure > context context_name > gtpp group group_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-gtpp-group)#
```

**Syntax**

```
gtpp server ip_address [ max msgs ] [ priority priority ] [ udp-port port ] [ node-alive { enable | disable } ] [ -noconfirm ]
```

```
no gtpp server ip_address [ udp-port port ]
```

**no**

Deletes a previously configured CGF.

**ip_address**

Specifies the IP address of the CGF in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

**max msgs**

Specifies the maximum number of outstanding or unacknowledged GTPP packets (from any one AAA Manager task) allowed for this CGF before the system begins buffering the packets.

msgs can be configured to an integer from 1 to 256. Default: 256

**priority priority**

Default: 1000

Specifies the relative priority of this CGF as an integer from 1 through 1000. When multiple CGFs are configured, the priority is used to determine which CGF server to send accounting data to. When configuring two or more servers with the same priority you will be asked to confirm that you want to do this.

If you use the -noconfirm option, you are not asked for confirmation and multiple servers could be assigned the same priority.
GTPP Server Group Configuration Mode Commands

GTPP Server Group Configuration Mode Commands

udp-port <port>

Specifies the UDP port over which the GGSN communicates with the CGF, as an integer from 1 through 65535. Default: 3386

node-alive { enable | disable }

Enable or disables GGSN sending Node Alive Request to a GTPP Server (such as CGF). This configuration can be done per GTPP Server. Default: Disable.

-noconfirm

Executes this command without any additional prompt and confirmation from the user.

Usage

Use this command to configure the CGF(s) that the system sends CDR accounting data to.

Multiple CGFs can be configured using multiple instances of this command subject to the following limits:

- Up to 4 CGFs can be configured in one GTPP server group
- Total of 32 CGFs can be configured per context.

Each configured CGF can be assigned a priority. The priority is used to determine which server to use for any given subscriber based on the routing algorithm that has been implemented. A CGF with a priority of “1” has the highest priority.

Important: The configuration of multiple CGFs with the same IP address but different port numbers is not supported.

Each CGF can also be configured with the maximum allowable number of unacknowledged GTPP packets. Since multiple AAA Manager tasks could be communicating with the same CGF, the maximum is based on any one AAA Manager instance. If the maximum is reached, the system buffers the packets Random Access Memory (RAM). The system allocates memory as a buffer, enough to store one million CDRs for a fully loaded chassis (a maximum of one outstanding CDR per PDP context).

Example

The following command configures a CGF with an IP address of 192.168.2.2 and a priority of 5.

gtpp server 192.168.2.2 priority 5

The following command deletes a previously configured CGF with an IP address of 100.10.35.7:

no gtpp server 100.10.35.7
gtpp source-port-validation

Configures whether the system validates the UDP source port in received GTPP messages.

Product

  GGSN
  P-GW
  SAEGW
  SGSN
  S-GW

Privilege

  Security Administrator, Administrator

Mode

Exec > Global Configuration > Context Configuration > GTPP Server Group Configuration

configure > context context_name > gtpp group group_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-gtpp-group)#

Syntax

[ default | no ] gtpp source-port-validation

  default
  Restores this parameter to its default setting of enabled.

  no
  Validates the IP source address but not the UDP source port.

Usage

This command configures whether the system validates the UDP source port in received GTPP messages.

Example

The following command disables UDP port validation:

  no gtpp source-port-validation
gtpp storage-server

Configures information for the GTPP back-up storage server.

Product
- GGSN
- P-GW
- SAEGW
- SGSN
- S-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > GTPP Server Group Configuration

configure > context context_name > gtpp group group_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-gtpp-group)#

Syntax

[ no ] gtpp storage-server  ip_address port port_num

no
Removes a previously configured back-up storage server.

ip_address
The IP address of the back-up storage server expressed in IPv4 dotted-decimal notation.

port port_num
Specifies the UDP port number over which the GGSN communicates with the back-up storage server. Default: 3386

Usage
This command identifies the connection to the GSS. One backup storage server can be configured per GTPP group.

Example
The following command configures a GSS with an IP address of 192.168.1.2:

    gtpp storage-server 192.168.1.2
gtpp storage-server local file

Configures the parameters for GTPP files stored locally on the GTPP storage server.

Product
GGSN
IPSG
PDG/TTG
P-GW
SAEGW
SGSN
S-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > GTPP Server Group Configuration

configure > context context_name > gtpp group group_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-gtpp-group)#

Syntax

```

default gtpp storage-server local file { compression | format | name { format | prefix } | purge-processed-files | rotation { cdr-count | time-interval | volume } start-file-seq-num }

no gtpp storage-server local file { purge-processed-files | push | rotation { cdr-count | time-interval } }
```

```
no

Removes a previously configured parameters for local storage of CDR files on HDD on SMC card.
```

```
compression { gzip | none }

Configures the type of compression to be used on the files stored locally.
gzip – Enables Gzip file compression.
none – Disables Gzip file compression -this is the default value.
```
format custom1 .. 8

Configures the file format to be used to format files to be stored locally.

**custom1** — File format custom1 - this is the default file format.

**custom2 to custom5** Customer specific CDR file formats.

**custom6** — File format custom6 with a block size of 8K for CDR files.

**custom7** — File format custom7 is a customer specific CDR file format.

**custom8** — File format custom8 is a customer specific CDR file format. It uses node-id-suffix_date_time_fixed-length-seq-num.u format for file naming where:

- **date** is date in MMDDYY (01132010) for mat
- **time** is time in HHMMSS (023508) format
- **fixed-length-seq-num** is the fixed length of the sequence number for a specific file having a 6-digit counter starting from 000001 and ending at 999999. When file sequence reaches 999999, the sequence is reset to 000001.

name format string

Allows the format of the CDR filenames to be configured independently so that the name format contains the file name with conversion specifications.

**string** — is an alphanumeric string of 1 through 127 characters. It must begin with the % (percent sign).

- **%y** = year as a decimal number without century (range 00 to 99).
- **%Y** = year as a decimal number with century.
- **%m** = month as a decimal number (range 01 to 12).
- **%d** = day of the month as a decimal number (range 01 to 31).
- **%H** = hour as a decimal number 24-hour format (range 00 to 23).
- **%h** = hour as a decimal number 12-hour format (range 01 to 12).
- **%M** = minute as a decimal number (range 00 to 59).
- **%S** = second as a decimal number (range 00 to 60). (The range is up to 60 to allow occasional leap seconds.)
- **%Q** = file sequence number. Field width may be specified between the % and the Q. If the natural size of the field is smaller than this width, then the result string is padded (on the left) to the specified width with 0s
- **%N** = No of CDRs in the file. Field width may be specified between the % and the N. If the natural size of the field is smaller than this width, then the result string is padded (on the left) to the specified width with 0s
- **%%%** = This field is used to add % to the CDR file name.

**max-file-seq-no**: This can be configured optionally. It indicates the maximum value of sequence number in file name (starts from 1). Once the configured max-file-seq-no limit is reached, the sequence number will restart from 1. If no max-file-seq-no is specified then file sequence number ranges from 1-4294967295.

By default the above keyword is not configured (default gtpp storage-server local file name format). In which case the CDR filenames are generated based on the file format as before (maintains backward compatibility).
**name prefix prefix**

Defines the prefix to be used for the file name. By default the file name prefix would be “GTPP-group-name + VPN-ID”. It is possible to have a NULL value prefix where the system would enter a default, which would be *group vpn*, *prefix* - is an alphanumeric string of 1 through 64 characters, Do not enter a value (NULL).

**purge-processed-files [ file-name-pattern file_pattern | purge-interval purge_dur ]**

Enables the GSN to periodically (every 4 minutes) delete locally processed (*.p) CDR files from the HDD on the SMC card. Default: Disabled

This keyword also deletes the processed push files (tx.*,under $CDR_PATH/TX/tk.*) a well when purging is enabled instead of "*.p:*.P".

**Important:** This option is available only when GTPP server storage mode is configured for local storage of CDRs with the *gtpp storage-server mode local* command.

Optional keyword *file-name-pattern file_pattern* provides an option for user to control the pattern of files. *file_pattern* must be mentioned in "*.p:*.P:tx.*" format in a string of size 1 through 127, which is also the default format. Wildcards * and: (synonymous to |) are allowed.

Optional keyword *purge-interval purge_dur* provides an option for user to control the purge interval duration (in minutes). *purge_dur* must be an integer from 1 through 259200. Default value 60.

**push { encrypted-url encrypted_url | url url } [ encrypted-secondary-url encrypted_url | secondary-url url ] [ via-local-context ]**

Enables push method to transfer local CDR files to remote system.

encrypted-url: Defines use of an encrypted url.

encrypted_url must be an alphanumeric string of 1 through 8192 characters in SFTP format.

url: Location where the CDR files are to be transferred.

url must be an alphanumeric string of 1 through 1024 characters in the format: scheme://user:password@host

encrypted-secondary-url: Defines use of an encrypted secondary url.

encrypted_url must be an alphanumeric string of 1 through 8192 characters in SFTP format.

secondary-url: Secondary location where the CDR files are to be transferred, in case primary is unreachable.

url must be an alphanumeric string of 1 through 1024 characters in the format: scheme://user:password@host

**Important:** When a file transfer to primary fails four times, the transfer of files will automatically be failed over to the secondary server. The transfer will switch back to the original primary after 30 minutes, or if there are four transfer failures to the secondary server.

via-local-context: Pushes the CDR files via SPIO in the local context.

Default: Pushes via the group's context.

**Important:** If the push is done through gtpp context, then the push rate is lesser compared to via local context as the HDD is attached to the local context.
rotation { cdr-count count | time-interval time [ force-rotation ] | volume size }

Specifies rotation related configuration for GTPP files stored locally.

cdr-count count: Configures the CDR count for the file rotation as an integer from 1000 through 65000. Default value 10000.

time-interval time: Configures the time interval for file rotation (in seconds) as an integer from 30 through 86400. Default: 3600 (1 hour).

force-file-rotation: Forces CDR file-rotation at a specified interval configured via the time-interval keyword, even if no CDRs were generated. By default this keyword is Disabled.

volume size: Configures the file volume (in megabytes) for file rotation as an integer from 2 through 40. This trigger can not be disabled. Default: 10

start-file-seq-num seq_num | recover-file-seq-num

Default: disabled

Enables the continuous file sequence number function. start-file-seq-num specifies the lowest number to be used as a file sequence number in the case of an aaaproxy or a chassis restart/reboot.

seq_num is an integer from 1 to 4294967295. Entering a value of 1 disables the recover file sequence number function. Entering any other number, for example 10, would instruct the system to always start from 10 as the file sequence number in the event of an aaaproxy or chassis reload.

When files are moved, the file sequence numbers are synced and stored in both RAM and the hard disk drive (HDD). recover-file-seq-num instructs the system to recover the last (largest) stored file sequence number, in the event of an aaaproxy/chassis restart/reboot, to continue file sequence numbering rather than resetting the file sequence numbering to the lowest start file sequence number.

Usage

This command configures the parameters for storage of GTPP packets as files on the local server - meaning the hard disk drive (HDD).

Example

The following command configures rotation for every 1.5 hours for locally stored files.

```
gtpp storage-server local file rotation time-interval 5400
```

Configuring file name format along with max-file-seq-no:

```
gtpp storage-server local file name format processed_2g_%Y%m%d_%5Q_%N.cdr max-file-seq-no 2345
```

Configuring file name prefix with a NULL value:

```
gtpp storage-server local file name prefix NULL
```

Configure the file name pattern and purge interval to setup file purging from the HDD:

```
gtpp storage-server local file purge-processed-files file-name-pattern *.z purge-interval 4
```
gtpp storage-server max-retries

Configures the maximum number of times the system attempts to communicate with an unresponsive GTPP back-up storage server.

**Product**
- GGSN
- P-GW
- SAEGW
- SGSN
- S-GW

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration > Context Configuration > GTPP Server Group Configuration
- configure > context context_name > gtpp group group_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-gtpp-group)#
```

**Syntax**

```
[ default ] gtpp storage-server max-retries max_attempts
```

- **default**
  - Restores the system to the default value of 2 retry attempts.

- **max_attempts**
  - Specifies the number of times the system attempts to communicate with a GTPP back-up storage server that is not responding as an integer from 1 to 15. Default: 2

**Usage**

This command works in conjunction with the **gtpp storage-server timeout** parameters to set a limit to the number of communication failures that can occur with a configured GTPP back-up storage server. The **gtpp storage-server timeout** command controls the amount of time between retries. Refer to the description of this command for additional information.

**Example**

The following command configures the maximum number of re-tries to be 8.

```
gtpp storage-server max-retries 8
```
gtpp storage-server mode

Configures the storage mode (local, remote or streaming for CDRs) to be used. Local storage mode is available with ASR 5000 platforms only.

Product
GGSN
P-GW
SAEGW
SGSN
S-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > GTPP Server Group Configuration

configure > context context_name > gtpp group group_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-gtpp-group)#

Syntax

```plaintext
gtpp storage-server mode { local | remote | streaming }
default gtpp storage-server mode
```

default

Returns the GTPP group configuration to the default “remote” value for the GTPP storage server mode.

local

Specifies the use of the hard disk for storing CDRs. Default: Disabled

---

**Important:** This option is available with ASR 5000 platforms only.

remote

Specifies the use of an external server for storing CDRs. This is the default value.

---

**Important:** When the external server is down, the Session Managers will start buffering up to a maximum of 26400 CDRs or a total of 120 MB worth of CDRs, whichever limit reaches first. The maximum CDR limit specified is per the session manager. The chassis level limit varies depending on the number of session manager instances and number of active cards.
streaming

Specifies the use of HDD to store CDRs in case if CGF fails and then stream the CDRs to the CGF when CGF is up. Streaming can be done in a First-In-First-Out (FIFO) mode. Default: streaming (FIFO)

streaming: This keyword allows the operator to configure “streaming” mode of operation for GTPP group. When this keyword is supplied the CDRs will be stored in following fashion:

- When GTPP link is active with CGF, CDRs are sent to a CGF via GTPP and local hard disk is NOT used as long as every record is acknowledged in time.

- If the GTPP connection is considered to be down, all streaming CDRs will be saved temporarily on the local hard disk and once the connection is restored, unacknowledged records will be retrieved from the hard disk and sent to the CGF.

In the streaming mode, when the CGF becomes active, CDRs in HDD are streamed in a First-In-First-Out order. In this mode, newly generated CDRs are routed to CGF via HDD.

Usage

This command configures whether the CDRs should be stored on the hard disk of the SMC or remotely, on an external server.

Example

The following command configures use of a hard disk for storing CDRs.

```
gtpp storage-server mode local
```
gtpp storage-server timeout

Configures the amount of time that must pass with no response before the system re-attempts to communicate with the GTPP back-up storage server.

Product
- GGSN
- P-GW
- SAEGW
- SGSN
- S-GW

Privilege
- Security Administrator, Administrator

Mode
- Exec > Global Configuration > Context Configuration > GTPP Server Group Configuration
  - configure > context context_name > gtpp group group_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-gtpp-group)#
```

Syntax

```
[ default ] gtpp storage-server timeout duration
```

- **default**
  - Restores the timeout duration to the default of 30 seconds.

- **duration**
  - Specifies the maximum amount of time (in seconds) that the system waits for a response from the GTPP back-up storage server before assuming the packet is lost.
  - `duration` is an integer from 30 through 120. Default: 30

Usage

This command works in conjunction with the `gtpp storage-server max-retries` command to establish a limit on the number of times that communication with a GTPP back-up storage server is attempted before a failure is logged.

This parameter specifies the time between retries.

Example

The following command configures a retry timeout of 60 seconds:

```
gtpp storage-server timeout 60
```
gtpp suppress-cdrs zero-volume

Suppresses the CDRs with zero byte data count, so that the OCG node is not overloaded with a flood of CDRs. By default this mode is “disabled”.

Important: The Zero Volume CDR Suppression is a license-controlled feature. For more information, contact your Cisco account representative.

Product
- GGSN
- P-GW
- SAEGW
- SGSN
- S-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > GTPP Server Group Configuration
configure > context context_name > gtpp group group_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-gtpp-group)#

Syntax

gtpp suppress-cdrs zero-volume { final-cdr | internal-trigger-cdr | external-trigger-cdr } +

{ default | no } gtpp suppress-cdrs zero-volume

default | no
Disables the CDR suppression mode. By default this command is disabled and system will not suppress any CDR.

final-cdr
Suppresses only the Final Zero Volume CDRs i.e. the CDRs that are generated when the session ends.

internal-trigger-cdr
Supresses Zero Volume interim CDRs that are generated due to internal triggers such as volume limit, time limit, tariff change or user generated interims through the CLI commands.

external-trigger-cdr
Supresses Zero Volume interim CDRs that are generated due to external triggers such as QoS Change, RAT change and so on.
gtpp suppress-cdrs zero-volume

Usage

Use this command to suppress the CDRs (G-CDRs, eG-CDR, PGW-CDRs, SGW-CDRs, SGSN CDRs) with zero-volume session due to any reason. This feature allows the customers to suppress the CDRs with zero byte data count, so that the OCG node is not overloaded with a flood of CDRs.

The CDRs can be categorized as follows:

- **final-cdr**: These CDRs are generated when the session ends.
- **internal-trigger-cdr**: These CDRs are generated due to internal triggers such as volume limit, time limit, tariff change or user generated interims through the CLI commands.
- **external-trigger-cdr**: These CDRs are generated due to external triggers such as QoS Change, RAT change and so on. All triggers which are not considered as final-cdrs or internal-trigger-cdrs are considered as external-trigger-cdrs.

Customers can select the CDRs they want to suppress. This feature is disabled by default to ensure backward compatibility.

Example

The following command configures the system to suppress Zero Volume Final CDRs, interim CDRs due to internal and external triggers:

```
gtpp suppress-cdrs zero-volume final-cdr internal-trigger-cdr external-trigger-cdr
```
**gtpp suppress-cdrs zero-volume-and-duration**

Suppresses the CDRs created by session having zero duration and/or zero volume. By default this mode is “disabled”.

**Product**
- GGSN
- P-GW
- SAEGW
- S-GW

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration > Context Configuration > GTPP Server Group Configuration
  ```
  configure > context context_name > gtpp group group_name
  ```

**Syntax**
- `gtpp suppress-cdrs zero-volume-and-duration { gcdrs [ egcdrs ] | egcdrs [ gcdrs ] }
- default gtpp suppress-cdrs zero-volume-and-duration

- **default**
  - Disables the CDR suppression mode.

- **gcdrs [ egcdrs ]**
  - Specifies that this command will handle G-CDRs before eG-CDR/P-CDRs.

- **egcdrs [ gcdrs ]**
  - Specifies that this command will handle eG-CDR/P-CDRs before G-CDRs.

**Usage**
Use this command to suppress the CDRs (G-CDRs and eG-CDR/P-CDRs) which were created due with zero-duration session and zero-volume session due to any reason. By default this command is disabled and system will not suppress any CDR.

**Example**
The following command configures the system to suppression the eG-CDR/P-CDRs created for a zero duration session or zero volume session:

```
gtpp suppress-cdrs zero-volume-and-duration egcdrs gcdrs
```
gtpp timeout

Configures the amount of time that must pass with no response before the system re-attempts to communicate with the CGF.

Product
GGSN
P-GW
SAEGW
SGSN
S-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > GTPP Server Group Configuration

Syntax
[ default ] gtpp timeout time

default
Resets the systems GTPP timeout value to 20 seconds.

time
Specifies the maximum amount of time (in seconds) the system waits for a response from the CGF before assuming the packet is lost.
time is an integer from 1 through 60. Default: 20

Usage
This command works in conjunction with the gtpp max-retries command to establish a limit on the number of times that communication with a CGF is attempted before a failure is logged.
This parameter specifies the time between retries.

Example
The following command configures a retry timeout of 30 seconds:

    gtpp timeout 30
**gtpp transport-layer**

Selects the transport layer protocol for Ga interface for communication between AGW (GSNs) and GTPP servers.

**Product**

GGSN
P-GW
SAEGW
SGSN
S-GW

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > GTPP Server Group Configuration

configure > context context_name > gtpp group group_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-gtpp-group)#
```

**Syntax**

```
gtpp transport-layer { tcp | udp }
```

```
default gtpp transport-layer
```

**Usage**

Use this command to select the TCP or UDP as the transport layer protocol for Ga interface communication between GTPP servers and AGWs (GSNs).

**Example**

The following command enables TCP as the transport layer protocol for the GSN’s Ga interface.

```
gtpp transport-layer tcp
```
gtpp trigger

Disables GTPP trigger conditions that cause either partial CDR record closure or opening of a new CDR record container. GTPP Triggers are specified in 3GPP TS 32.251 v6.6.0. All GTPP trigger changes take effect immediately, except *volume-limit*.

**Product**
- ECS
- GGSN
- P-GW
- SAEGW
- SGSN
- S-GW

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration > Context Configuration > GTPP Server Group Configuration
- `configure > context context_name > gtpp group group_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-gtpp-group)#
```

**Syntax**

```

default gtpp trigger


default

Sets the specified trigger condition back to the default setting. All trigger conditions are enabled by default.

no

Disables the specified trigger condition.
GTPP Server Group Configuration Mode Commands

gtpp trigger

---

apn-ambr-change [ default-bearer-only | all-non-gbr-bearers | all-bearers ]

Default: Disabled
Enables APN AMBR trigger only for default-bearer or for all bearers for that PDN or selectively for apn-non-gbr bearers.

---

**Important:** This keyword option will be available only if a valid license is installed. For more information, contact your Cisco account representative.

The APN Aggregate Maximum Bit Rate (AMBR) is a subscription parameter stored per APN. It limits the aggregate bit rate that can be expected to be provided across all non-GBR bearers and across all PDN connections of the same APN. Each of these non-GBR bearers potentially utilize the entire APN AMBR, e.g. when the other non-GBR bearers do not carry any traffic.

In 15.0 and later releases, this CLI command should be configured along with the following additional options to enable APN-AMBR trigger for SGW-CDRs in all GTPP dictionaries.

- **default-bearer-only**: Adds container only to default bearer.
- **all-non-gbr-bearers**: Adds container to all non-gbr-bearers.
- **all-bearers**: Adds containers for all bearers.

---

**Important:** This CLI command and the associated options are not available for products other than S-GW and P-GW.

The first container of each CDR includes apn-ambr fields along with QoS. In the following containers this field is present if previous change condition is "QoS change" or "APN AMBR Change".

---

cell-update

Enables the cell update trigger for S-CDRs, if the dictionary specified in the **gtpp dictionary** configuration includes support for cell update. This trigger is available only for 2G. Currently, custom18 dictionary supports the cell update trigger.

---

dcca

This keyword enables or disables the addition of LOSDV in PGW-CDR for the following DCCA generated triggers.

- Time Threshold Reached
- Volume Threshold Reached
- Service Specific Unit Threshold Reached
- Time Exhausted
- Volume Exhausted
- Validity Timeout
- Reauthorization Request
- Continue Ongoing Session
- Retry And Terminate Ongoing Session
- Terminate Ongoing Session
GTPP Server Group Configuration Mode Commands

- Service Specific Unit Exhausted
- Envelope Closure

**direct-tunnel**
Enables the direct tunnel trigger for CDRs.

**egcdr max-losdv**
Enables the trigger for an eG-CDR/P-CDR if the List of Service Data Volume (LoSDV) containers crosses the configured limit for LOSDV containers. Default: Disabled

**ggsn-preservation-mode-change**
This keyword is for GGSN only. This trigger enables the preservation-mode-change trigger for G-CDR.

**inter-plmn-sgn-change**
This keyword is for GGSN only. Disabling this trigger ignores an Inter-PLMN SGSN change and doesn't release a G-CDR. Default: Enabled

**ms-timezone-change**
This keyword is specific to GGSN. No partial record closure for a time zone change occurs when this trigger is disabled. MS time zone change should be applicable only for 3GPP R6 based GTPP dictionaries. Default: Enabled

**plmn-id-change**
This trigger keyword is specific to the 2G SGSN and is proprietary (non-standard). Enables the PLMNID change trigger for S-CDRs if the dictionary specified in the `gtpp dictionary` configuration supports the PLMNID change. If enabled, the SGSN generates a partial S-CDR when the MS changes the PLMN while under the same SGSN (intra-system intra-SGSN PLMN-ID handover). Currently, custom18 dictionary supports this trigger. Default: Disabled

**qos-change**
Enables the QoS-change trigger for CDRs. Disabling this trigger ignores a QoS-change and does not open a new CDR for it. Default: Enabled

When QoS changes are observed, the system generates only containers. However, when the max-container condition is reached, an interim CDR is generated.

**rat-change**
Enables or disables the partial record closure for a RAT change. If disabled, no partial record closure for a RAT change occurs. RAT change should be applicable only for 3GPP R6 based GTPP dictionaries. Default: Enabled

In SGSN, RAT change trigger (2G<->3G) means inter-service handoff (SGSN service <-> GPRS service). If this trigger is enabled, after the RAT change interim CDR is generated. After this RAT change CDR, CDR thresholds such as volume/time etc. and GTPP Group are applicable from new service. If RAT change trigger is disabled, the CDR thresholds and GTPP group etc. will not change and will continue to use from old service.

After the RAT change, the System Type field in CDR changes to indicate the new system type. If this trigger is disabled, then the next CDR generated will indicate System Type, but the data count in the CDR does not
necessarily belong to the system type indicated in CDR; instead, it may belong to both 2G and 3G as CDR is not closing when handover takes place.

**Important:** The System Type field in CDR-related change is not applicable to customized CDR formats, which does not use the System Type field.

```text
generate { cdr | container }: Sets generation of CDR or just a Container on a RAT change.

cdr: Generates a CDR on a RAT-change.

container: Generates a container only on a RAT-change.
```

**routing-area-update**

Enables the routing-area-update trigger for CDRs.

**service-idle-out**

This keyword enables or disables the addition of LOSDV in PGW-CDR when a service idles out.

Note that the CDR module receives service idle out trigger from DCCA module when the quota hold timer expires, or from ACS manager when rulebase has a service idle out configuration.

```text
serving-node-change-limit [ also-intra-sgsn-multiple-address-group-change ]
```

This keyword is enabled for P-GW, S-GW, and GGSN. However, the `also-intra-sgsn-multiple-address-group-change` is enabled only for GGSN. Default: Enabled

Disabling this trigger ignores an SGSN change and does not add the SGSN IP address into the SGSN address list of the CDR. This helps to reduce the release of CDRs due to SGSN changes crossing the configured limit.

**also-intra-sgsn-multiple-address-group-change:** This keyword includes Intra-SGSN group changes as an SGSN change.

```text
sgsn-change-limit [ also-intra-sgsn-multiple-address-group-change ]
```

This keyword is obsolete and is available to maintain the backward compatibility for existing customers. The new keyword for `sgsn-change-limit` is `serving-node-change-limit`. Default: Enabled

Disabling this trigger ignores an SGSN change and does not add the SGSN IP address into the SGSN address list of the CDR. This helps to reduce the release of CDRs due to SGSN changes crossing the configured limit.

**also-intra-sgsn-multiple-address-group-change:** This keyword includes Intra-SGSN group changes as an SGSN change.

**tariff-time-change**

When this trigger is disabled, container closure does not happen for a tariff-time change. Default: Enabled

This trigger is applicable for G-MB-CDRs for MBMS session too.

**time-limit**

When this trigger is disabled, no partial record closure occurs when the configured time limit is reached. Default: Enabled

This trigger is applicable for G-MB-CDRs for MBMS session too.

**uli-change**

Enables the user location update trigger for eG-CDRs/PGW-CDRs/SGW-CDRs, if the dictionary specified in the GTPP dictionary configuration includes support for user location update trigger. Default: Enabled
volume-limit

When this trigger is disabled no partial record closure occurs when volume limit is reached. Default: Enabled

This trigger is applicable for G-MB-CDRs for MBMS session too.

Usage

Use this command to disable or enable GTTP triggers that can cause partial CDR record closure or cause a new CDR to be created.

Example

The following command disables partial record closure when a configured time limit is reached:

```
gtp trigger time-limit
```

The following command re-enables partial record closure when a configured time limit is reached:

```
no gtp trigger time-limit
```
Chapter 154
GTP-U Service Configuration Mode Commands

The GTP-U Service Configuration Mode is used to manage parameters applied to incoming GTP-U packets.

Mode

Exec > Global Configuration > Context Configuration > GTP-U Service Configuration

configure > context context_name > gtpu-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-gtpu-service)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
bind

Configures the IP address to use for GTP-U data packets.

Product

ePDG
GGSN
P-GW
SAEGW
SGSN
S-GW

Privilege

Administrator

Mode

Exec > Global Configuration > Context Configuration > GTP-U Service Configuration

configure > context context_name > gtpu-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-gtpu-service)#

Syntax

[  no  ] bind { ipv4-address ipv4_address [ crypto-template crypto_template ] [ ike-bind-address { ipv4_address } ] [ ipv6-address ipv6_address ] | ipv6-address ipv6_address [ crypto-template crypto_template ] [ ike-bind-address { ipv6_address } ] [ ipv4-address ipv4_address ] }

no

removes a configured IP address from this service.

ipv4-address ipv4_address

Binds this service to the IPv4 address of a configured interface.

ipv4_address must be entered using IPv4 dotted-decimal notation.

bearer-type non-ims-media | ims-media | all

Specifies the type of bearer to be associated with the bind address. Default behavior is for that the address will be used for all bearer types.

non-ims-media Configures bind address for non-ims media only.

ims-media Configures bind address for ims-media traffic only.

all configures bind address to handle all types of bearer traffic. This is the default setting.

ipv6-address ipv6_address

Binds this service to the IPv6 address of a configured interface.

ipv6_address must be entered using IPv6 colon-separated-hexadecimal notation.
**crypto-template crypto_template**

Configures crypto template for IPSec, which enables IPSec tunneling for this GTP-U address. Must be followed by the name of an existing crypto template. 
`crypto_template` must be an alphanumeric string of 1 through 127 characters.

**ike-bind-address ip_address**

Configures an IKE bind address. Must be followed by IPv4 or IPv6 address; IP address type must be the same as the GTP-U address type.

`ipv4_address` must be entered using IPv4 dotted-decimal notation.

`ipv6_address` must be entered using IPv6 colon-separated-hexadecimal notation.

**bearer-type non-ims-media | ims-media | all**

Specifies the type of bearer to be associated with the bind address. Default behavior is for that the address will be used for all bearer types.

`non-ims-media` configures bind address for non-ims media only.

`ims-media` configures bind address for ims-media traffic only.

`all` configures bind address to handle all types of bearer traffic. This is the default setting.

**Usage**

Use this command to bind the service to an interface for sending/receiving GTP-U packets.

**Important:** A GTP-U service can support a maximum of 12 GTP-U endpoints/interfaces.

**Example**

The following command configures the IPv4 address for this GTP-U service as 10.2.3.4:

```
bind ipv4-address 10.2.3.4
```
echo-interval

Configures the rate at which GPRS Tunneling Protocol (GTP) v1-U echo packets are sent.

Product
- ePDG
- GGSN
- P-GW
- SAEGW
- SGSN
- S-GW

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > GTP-U Service Configuration
configure > context context_name > gtpu-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-gtpu-service)#

Syntax

```
echo-interval seconds [ dynamic [ smooth-factor multiplier ] ]
{ default | no } echo-interval
```

- **default**
  Disables the configured echo-interval setting.

- **no**
  Removes the configured echo-interval setting.

- **seconds**
  Specifies the number of seconds between the sending of a GTP-Uv1 echo packet. `seconds` must be an integer from 60 through 3600. Default: 60

- **dynamic [ smooth-factor multiplier ]**
  Enables the dynamic echo timer for the GTP-U service.
  
  `smooth-factor multiplier`: Introduces a multiplier into the dynamic echo timer as an integer from 1 through 5. Default: 2

Usage

Use this command to configure the rate at which GTP-Uv1 echo packets are sent.

Example

```
```
The following command sets the rate between the sending of echo packets at 120 seconds:

```
echo-interval 120
```
echo-retransmission-timeout

Configures the timeout for GTP-U echo message retransmissions for this service.

Product
- ePDG
- GGSN
- P-GW
- SAEGW
- SGSN
- S-GW

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > GTP-U Service Configuration

configure > context context_name > gtpu-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-gtpu-service)#

Syntax

echo-retransmission-timeout seconds

default echo-retransmission-timeout

default

Returns the command to its default setting of 5.

seconds

Default: 5

Configures the echo retransmission timeout, in seconds, for the GTP-U service as an integer ranging from 1 to 20.

Usage

Use this command to configure the amount of time, in seconds, before the GTP-U service transmits another echo request message. The value set in this command is used, as is, for the default echo. If dynamic echo is enabled (echo-interval dynamic) the value set in this command serves as the dynamic minimum (if the RTT multiplied by the smooth factor is less than the value set in this command, the service uses this value).

Example

The following command sets the retransmission timeout for echo messages to 2 seconds:

echo-retransmission-timeout 2
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

exit

Usage
Use this command to return to the parent configuration mode.
extension-header

Configures the addition of an extension header in the GTP-U packet header, allowing for error indication messages.

Product
GGSN
P-GW
SAEGW
SGSN
S-GW

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > GTP-U Service Configuration

configure > context context_name > gtpu-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-gtpu-service)#

Syntax

[ default | no ] extension-header source-udp-port

default

Returns the command to its default setting of disabled.

no

Disables the feature.

source-udp-port

Configures extension header type UDP Port support in GTP-U header for GTP-U Error Indication messages.

Usage

Use this command to configure the addition of an extension header in the GTP-U packet to allow for error indication messages

Example

The following command enables the inclusion of an extension header to allow for error indication messages:

extension-header source-udp-port
### ip qos-dscp

Configures the quality of service (QoS) differentiated service code point (DSCP) per-hop behavior (PHB) to be marked on the outer header of signalling packets originating from the LTE component.

**Product**
- ePDG
- P-GW
- SAEGW
- S-GW

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > GTP-U Service Configuration

*configure > context context_name > gtpu-service service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-gtpu-service)#
```

**Syntax**

```
ip qos-dscp { af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef }
```

- **default**
  Sets/restores default value.

- **no**
  Disables DSCP marking.

**af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef**

Specifies the IP QoS DSCP PHB to be marked on the outer header of signalling packets originating from the LTE component. This is a standards-based feature (RFC 2597 and RFC 2474).

Note that CS (class selector) mode options below are provided to support backward compatibility with the IP precedence field used by some network devices. CS maps one-to-one to IP precedence, where CS1 is IP precedence value 1. If a packet is received from a non-DSCP aware router that used IP precedence markings, then the DSCP router can still understand the encoding as a Class Selector code point.

The following forwarding types are supported:

- **af11**: Designates the use of Assured Forwarding 11 PHB.

  This is the default setting.

- **af12**: Designates the use of Assured Forwarding 12 PHB.

- **af13**: Designates the use of Assured Forwarding 13 PHB.
• **af21**: Designates the use of Assured Forwarding 21 PHB.
• **af22**: Designates the use of Assured Forwarding 22 PHB.
• **af23**: Designates the use of Assured Forwarding 23 PHB.
• **af31**: Designates the use of Assured Forwarding 31 PHB.
• **af32**: Designates the use of Assured Forwarding 32 PHB.
• **af33**: Designates the use of Assured Forwarding 33 PHB.
• **af41**: Designates the use of Assured Forwarding 41 PHB.
• **af42**: Designates the use of Assured Forwarding 42 PHB.
• **af43**: Designates the use of Assured Forwarding 43 PHB.
• **be**: Designates the use of Best Effort forwarding PHB.
• **cs1**: Designates the use of Class Selector code point “CS1”.
• **cs2**: Designates the use of Class Selector code point “CS2”.
• **cs3**: Designates the use of Class Selector code point “CS3”.
• **cs4**: Designates the use of Class Selector code point “CS4”.
• **cs5**: Designates the use of Class Selector code point “CS5”.
• **cs6**: Designates the use of Class Selector code point “CS6”.
• **cs7**: Designates the use of Class Selector code point “CS7”.
• **ef**: Designates the use of Expedited Forwarding PHB typically dedicated to low-loss, low-latency traffic.

The assured forwarding behavior groups are listed in the table below.

<table>
<thead>
<tr>
<th></th>
<th>Class 1</th>
<th>Class 2</th>
<th>Class 3</th>
<th>Class 4</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Low Drop</strong></td>
<td>AF11</td>
<td>AF21</td>
<td>AF31</td>
<td>AF41</td>
</tr>
<tr>
<td><strong>Medium Drop</strong></td>
<td>AF12</td>
<td>AF22</td>
<td>AF32</td>
<td>AF42</td>
</tr>
<tr>
<td><strong>High Drop</strong></td>
<td>AF13</td>
<td>AF23</td>
<td>AF33</td>
<td>AF43</td>
</tr>
</tbody>
</table>

Traffic marked with a higher class is given priority during congestion periods. If congestion occurs to traffic with the same class, the packets with the higher AF value are dropped first.

**Usage**

Use this command to implement DSCP marking only for GTP-U ECHO Request and Response messages.

**Example**

Use the following command to set the use of Best Effort forwarding PHB:

```
ip qos-dscp be
```
ipsec-allow-error-ind-in-clear

Configures whether error-indication is dropped or sent without IPSec tunnel.

Product
S-GW
SAEGW
SGSN

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > GTP-U Service Configuration

configure > context context_name > gtpu-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-gtpu-service)#

Syntax

[ default | no ] ipsec-allow-error-ind-in-clear

- default
  Error-indication is dropped if no IPSec tunnel is present for that peer.

- no
  Disables the feature.

Usage

Use this command to determine whether error-indication is dropped or sent without an IPSec tunnel. On receiving data packets for a session that does not exist, error-indication needs to be sent back to the peer. If there is no IPSec tunnel present with that peer, error-indication may be either dropped or sent without any IPSec tunnel.

Example

The following command allows error-indication to be sent without any IPSec tunnel:

ipsec-allow-error-ind-in-clear
ipsec-tunnel-idle-timeout

Configures the IPSec tunnel idle timeout after which IPSec tunnel deletion is triggered.

**Product**
S-GW
SAEGW
SGSN

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > GTP-U Service Configuration

```
configure > context context_name > gtpu-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-gtpu-service)#
```

**Syntax**

```
ipsec-tunnel-idle-timeout seconds

default ipsec-tunnel-idle-timeout
```

**seconds**
Default: 60
Specifies the number of seconds an IPSec tunnel is idle before tunnel deletion is triggered. **seconds** must be an integer from 10 through 600.

**default**
Returns the command to its default setting of 60.

**Usage**

When there are no bearers on a particular IPSec tunnel, GTPUMGR initiates the delete for that tunnel. This timer helps to avoid unnecessary IPSec tunnel deletions for an idle tunnel.

**Example**

The following command sets the IPsec tunnel idle timeout to 100 seconds:

```
ipsec-tunnel-idle-timeout 100
```
max-retransmissions

Configures the maximum retry limit for GTP-U echo retransmissions.

Product
- ePDG
- GGSN
- P-GW
- SAEGW
- SGSN
- S-GW

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > GTP-U Service Configuration
configure > context context_name > gtpu-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-gtpu-service)#

Syntax

max-retransmissions num
no max-retransmissions

num

Default: 4
Specifies the number of GTP-U echo message retransmissions allowed before triggering a path failure error condition. num must be an integer from 0 through 15.

no

Disables the feature.

Usage

Use this command to set the maximum number of GTP-U echo message retransmissions in order to define a limit that triggers a path failure error.

Example

The following command sets the maximum GTP-U echo message retransmissions for this service to 10:

max-retransmissions 10
path-failure clear-trap

Configures a trigger for clearing the path failure trap.

**Product**
- ePDG
- GGSN
- P-GW
- SAEGW
- SGSN
- S-GW

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > GTP-U Service Configuration

```
configure > context context_name > gtpu-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-gtpu-service)#
```

**Syntax**

```
path-failure clear-trap gtp echo
```

[ default | no ] path-failure clear-trap

---

gtp echo

Sets the clearing trigger/trap to detect a failure upon reaching the maximum number of GTP-U echo message retransmissions.

---

default

Resets the command to its default setting of enabled.

---

no

Disables the feature.

**Usage**

Use this command to set the detection policy for path failures. By default, path failure trap is cleared on receiving first control plane message for that GTP-U peer allocation.

**Example**

The following command sets the clearing trigger to detect failures upon reaching the maximum number of GTP-U echo message retries:

```
path-failure clear-trap gtp echo
```
path-failure detection-policy

Configures a path failure detection policy on GTP-U echo messages that have been retransmitted the maximum number of retry times.

Product
- ePDG
- GGSN
- P-GW
- SAEGW
- SGSN
- S-GW

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > GTP-U Service Configuration
configure > context context_name > gtpu-service service_name

Entering the above command sequence results in the following prompt:

[context_name] host_name(config-gtpu-service)#

Syntax

path-failure detection-policy gtp echo

[ default | no ] path-failure detection-policy

<table>
<thead>
<tr>
<th>Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>gtp echo</td>
</tr>
</tbody>
</table>
Sets the detection policy to detect a failure upon reaching the maximum number of GTP-U echo message retransmissions.

<table>
<thead>
<tr>
<th>Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
</tr>
</tbody>
</table>
Resets the command to its default setting of enabled.

<table>
<thead>
<tr>
<th>Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
</tr>
</tbody>
</table>
Disables the feature.

Usage

Use this command to set the detection policy for path failures.

Example

The following command sets the path failure detection policy to detect failures upon reaching the maximum number of GTP-U echo message retries:

path-failure detection-policy gtp echo
retransmission-timeout

Configures retransmission timeout for GTPU echo message retransmissions for this service.

**Important:** In release 14.0 and later versions, this command is replaced by the `echo-retransmission-timeout` command.

**Product**
- ePDG
- GGSN
- P-GW
- SAEGW
- S-GW

**Privilege**
Administrator

**Mode**
- Exec > Global Configuration > Context Configuration > GTP-U Service Configuration
  - configure > context context_name > gtpu-service service_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-gtpu-service)#
```

**Syntax**

```
retransmission-timeout seconds
```

**default retransmission-timeout**

```
default
```

Returns the command to its default setting of 5.

```
default
```

**seconds**

```
default
```

Default: 5

Specifies the number of seconds between the re-sending of GTP-U echo messages. `seconds` must be an integer from 1 through 20.

**Usage**

Use this command to set the number of seconds between the retransmission of GTP-U echo messages.

**Example**

The following command sets the number of seconds between the sending of GTP-U echo messages to 7:

```
retransmission-timeout 7
```
sequence-number

Enables addition of the sequence number to every GTP-U packet. Default is disabled.

Product

GGSN
HSGW
P-GW
SAEGW
SGSN
S-GW

Privilege

Administrator

Mode

Exec > Global Configuration > Context Configuration > GTP-U Service Configuration

configure > context context_name > gtpu-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-gtpu-service)#

Syntax

[ no ] sequence-number

no

Disables addition of the sequence number to every GTP-U packet.

Usage

Use this command to enable/disable addition of the sequence number to every GTP-U packet coming from Gi interface and going towards Gn/Gp interface. If GTP-U packets are received out of sequence, sequence numbers would allow the packets to be reordered.

Example

The following command enables addition of the sequence number to every GTP-U packet:

`sequence-number`
udp-checksum

Inserts UDP-checksum in the UDP header of GTP-U packet.

Product
GGSN
HNB-GW
P-GW
SGSN
S-GW

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > GTP-U Service Configuration

configure > context context_name > gtpu-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-gtpu-service)#

Syntax

udp-checksum { no-optimize | optimize }
[ default | no ] udp-checksum

default
Through releases 14.0: Enables the UDP checksum, but no optimization is attempted. Releases 15.0 and later: Enables the UDP checksum, and attempts optimization of the UDP checksum in UDP header of GTPU packet using the inner payload transport checksum.

no
Outer UDP checksum is marked as 'ZERO,' effectively disabling UDP checksum. Applicable only for IPv4 data.

no-optimize
No optimization attempt over UDP checksum in UDP header of GTP-U packet.

optimize
Attempts optimization of UDP checksum in UDP header of GTP-U packet using inner payload transport checksum.

Usage
This command is used for enabling optimization of UDP checksum in UDP header of the GTP-U packet. An option to completely disable the UDP checksum of GTP-U packet is also introduced.

Example
The following command enables the optimization of UDP checksum in UDP header of the GTP-U packet:

```
udp-checksum optimize
```
Chapter 155
HA Proxy DNS Configuration Mode Commands

The HA Proxy DNS Configuration Mode is used to create rules for Home Agent (HA) proxy DNS intercept lists that redirect packets with unknown foreign DNS addresses to a home network DNS server.

**Important:** HA Proxy DNS Intercept is a license-enabled feature.

**Mode**

Exec > Global Configuration > Context Configuration > Proxy DNS Configuration

```
configure > context context_name > proxy-dns intercept-list list_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-proxy-dns-intercept-list)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
**end**

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
```
end
```

**Usage**
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Use this command to return to the parent configuration mode.
**pass-thru**

Sets IP addresses that should be allowed through the proxy DNS intercept feature.

**Product**
HA

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Proxy DNS Configuration

```
configure > context context_name > proxy-dns intercept-list list_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-proxy-dns-intercept-list)#
```

**Syntax**

```
[ no ] pass-thru ip_address [ /ip_mask ]
```

- `no`
  Removes the DNS IP address from the pass-thru rule.

- `pass-thru ip_address [ /ip_mask ]`
  Specifies an DNS IP address that is allowed through the intercept feature.
  
  `ip_address[/ip_mask]`: Specifies the IP address and network mask bits. `ip_address[/ip_mask]` is specified using IPv4 dotted decimal or IPv6 colon-separated-hexadecimal notation. The mask bits are a numeric value which is the number of bits in the subnet mask (CIDR notation).

**Usage**

Use this command to identify DNS IP addresses that should be allowed through the intercept feature. For a more detailed explanation of the proxy DNS intercept feature, see the `proxy-dns intercept-list` command in the Context Configuration Mode Commands chapter. A maximum of 16 intercept rules (either `redirect` or `pass-thru`) are allowed for each intercept list.

**Important:** To allow packets through that do not match either the `pass-thru` or `redirect` rules, set a `pass-thru` rule address as: 0.0.0.0/0. If a packet does not match either the `pass-thru` or `redirect` rule, the packet is dropped.

**Example**

The following command allows a foreign network’s DNS with an IP address of 10.2.55.12 to avoid being redirected:

```
pass-thru 10.2.55.12
```
redirect

Redirects DNS IP addresses from foreign networks matching an IP address in this command to a home network DNS.

Product:
HA

Privilege:
Security Administrator, Administrator

Mode:
Exec > Global Configuration > Context Configuration > Proxy DNS Configuration

configure > context context_name > proxy-dns intercept-list list_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-proxy-dns-intercept-list)#

Syntax:

[ no ] redirect any [ primary-dns ip_address [ secondary-dns ip_address ] ]

no

Removes the DNS IP address from the redirect rule.

primary-dns ip_address

Specifies the IP address of the primary home network DNS.

ip_address is specified using IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

secondary-dns ip_address

Specifies the IP address of the secondary home network DNS.

ip_address is specified using IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

Usage:

Use this command to identify DNS IP addresses from foreign networks that are to be redirected to the home DNS. For a more detailed explanation of the Proxy DNS feature, see the proxy-dns intercept-list command in the Context Configuration Mode Commands chapter. A maximum of 16 intercept rules (either redirect or pass-thru) are allow for each intercept list.

Since this command is configured in the source context, the destination context containing the path to the home network DNS is identified using the Context Configuration Mode command ip dns-proxy source-address.

Important: If a packet does not match the pass-thru or redirect rule, the packet is dropped. If primary-dns or secondary-dns is not configured, DNS messages are redirected to the primary-dns-server (or the secondary-dns-server) configured for the subscriber OR inside the context.

Example:

The following command identifies a foreign network DNS with an IP address of 10.2.55.12 and redirects it to a primary home network DNS with an IP address of 10.3.4.5:
predirect 10.2.55.12 primary-dns 10.3.4.5
Chapter 156
HA Service Configuration Mode Commands

The HA Service Configuration Mode is used to create and manage the Home Agent (HA) services within the current context.

**Mode**

Exec > Global Configuration > Context Configuration > HA Service Configuration

```
configure > context context_name > ha-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ha-service)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
a11-signalling-packets

Applies Differentiated Services Code Point (DSCP) marking for IP headers carrying outgoing signalling packets.

**Product**
HA

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > HA Service Configuration

`configure > context context_name > ha-service service_name`

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-ha-service)#`

**Syntax**

```
all-signalling-packets ip-header-dscp ip-header-dscp{ default | no } all-signalling-packets ip-header-dscp
```

**no**

Disables DSCP marking for IP header encapsulation for the HA service.

**default**

Configures DSCP marking for IP header encapsulation for a specific HA service.

**ip-header-dscp**

Is a hexadecimal number between 0x0 and 0x3F.

**Usage**

The following command is used to apply DSCP marking for IP header carrying outgoing signalling packets.

**Example**

The following command applies DSCP marking for IP header carrying outgoing signalling packets.

```
all-signalling-packets ip-header-dscp 0x2f
```
aaa

Configures the sending of subscriber session AAA accounting by the HA service.

Product
HA

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > HA Service Configuration

configure > context context_name > ha-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ha-service)#

Syntax

aaa { accounting [ roaming ] | group string }

no aaa { accounting | group }

default aaa accounting

  no
  Enables AAA accounting for the HA service.

  default
  Configures AAA parameters for specific HA service

  accounting
  accounting Enables the sending of AAA accounting information for subscriber sessions by the Home Agent (HA), by default is enabled.
  roaming Enables the sending of AAA accounting information for subscriber sessions by the Home Agent (HA) only for roaming subscribers.

  group
  group configures aaa group for ha-service, group has lower priority than subscriber/apn config.
  string: size ranges between 1 and 63.

Usage

Enabling the HA service will send all accounting data (start, stop, and interim) to the configured AAA servers.

The chassis is shipped from the factory with the AAA accounting enabled.
Important: In order for this command to function properly, AAA accounting must be enabled for the context in which the HA service is configured using the aaa accounting subscriber radius command.

Example

The following command disables aaa accounting for the HA service:

```
no aaa accounting
```
access-network

Configures a specific access network configuration.

**Product**
HA

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > HA Service Configuration

```
configure > context context_name > ha-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ha-service)#
```

**Syntax**

```
access-network accounting identifier access_network_accounting_identifier
no access-network accounting identifier
```

**no**
Disables a specific access network configuration.

**accounting**
Specifies an access network configuration for accounting

**identifier**
Specifies an access network accounting identifier

**access_network_accounting_identifier**
This is an alphanumeric string of 1 through 128 characters.

**Usage**
This command is used to configure an access network for accounting.

**Example**
The following command configures an access network for accounting with the identifier *idnt*:

```
access-network accounting identifier idnt
```
associate

Associates an HA-service with a QoS policy.

Product
HA

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > HA Service Configuration

configure > context context_name > ha-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ha-service)#

Syntax

associate qci-qos-mapping string

no associate qci-qos-mapping

no

Disables the association of an HA-service with a QoS policy.

qci-qos-mapping string

Maps a QoS Class Identifier (QCI) for this HA service.

string is an alphanumeric string of 1 through 63 characters.

Usage

This command associates an HA-service with a QoS policy.

Example

The following command associates an HA-service with a QCI map01:

associate qci-qos-mapping map01
authentication

Configures authentication parameters for a specific HA service within a context.

Product
HA
ASN-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > HA Service Configuration

configure > context context_name > ha-service service_name

Entering the above command sequence results in the following prompt:

[context_name] host_name(config-ha-service)#

Syntax

authentication { aaa-distributed-mip-keys [ disabled | optional | required ] | dmu
refresh-key | imsi-auth] mn-aaa { allow-noauth | always| dereg-noauth | noauth | renew
reg-noauth | renew-and-dereg-noauth } | mn-ha { allow-noauth | always } | pmip-auth | stale-key-disconnect }

no authentication { imsi-auth | pmip-auth }

default authentication { aaa-distributed-mip-keys | dmu-refresh-key | imsi-auth | mn-aaa | mn-ha | pmip-auth | stale-key-disconnect }

no
Disables the parameter.

default
Resets the specified option to its default setting.

aaa-distributed-mip-keys [ disabled | optional | required ]
Configures use of AAA distributed MIP keys for authenticating RRQ for WiMAX HA calls.
Default is disabled.

disabled: Disables using AAA distributed WiMAX Mobile IP (MIP) keys for authenticating MIP RRQ.
optional: Uses AAA distributed WiMAX MIP keys for authenticating RRQ with fallback option to use static/3GPP2 based MIP keys.
required: AAA distributed WiMAX MIP keys for authenticating MIP RRQ are mandatory

dmu-refresh-key
Typically, when a Dynamic Mobile IP Update (DMU) resets, the next MIP re-registration causes MN-HA authorization failure and the HA rejects the MIP RRQ. This parameter enables the HA to retrieve the MN-HA key again from the AAA during the call and to use the freshly retrieved key value to recheck authentication. Default is disabled.
**imsi-auth**

Enable uses the International Subscriber Mobile identity (IMSI) to determine if MN-AAA or MN-FAC extensions are not present in the RRQ.
Default is disabled.

```
imsi-auth
```

**mn-aaa { allow-noauth | always | dereg-noauth | noauth | renew-reg-noauth | renew-and-dereg-noauth }**

Specifies how mobile node-to-AAA authentication extension in registration requests from the mobile node should be handled by the HA service.
Default is always.

- **allow-noauth**: Specifies that the HA service does not require authentication for every mobile node registration request. However, if the mn-aaa extension is received, the HA service will authenticate it.
- **always**: Specifies that the HA service will perform authentication each time a mobile node registers.
- **dereg-noauth**: Disables authentication request upon de-registration.
- **noauth**: Specifies that the HA service will not look for mn-aaa extension and will not authenticate it.
- **renew-reg-noauth**: Specifies that the HA service will not perform authentication for mobile node re-registrations. Initial registration and de-registration will be handled normally.
- **renew-and-dereg-noauth**: Disables authentication request upon re-registration and de-registration.

```
mn-aaa { allow-noauth | always | dereg-noauth | noauth | renew-reg-noauth | renew-and-dereg-noauth }
```

**mn-ha { allow-noauth | always }**

Specifies whether the HA service looks for an MN-HA authentication extension in the RRQ.
Default is always.

- **allow-noauth**: Allows a request that does not contain the auth extension.
- **always**: A request should always contain the auth extension to be accepted.

```
mn-ha { allow-noauth | always }
```

**pmip-auth**

Specifies whether the HA service looks for an MN-HA authentication extension in the RRQ.
Default is always.

- **allow-noauth**: Allows a request that does not contain the auth extension.
- **always**: A request should always contain the auth extension to be accepted.

```
pmip-auth
```

**stale-key-disconnect**

If MN-HA auth fails for MIP renew and dereg, disconnects the call immediately.
Disabled by default.

```
stale-key-disconnect
```

**Usage**

The **authentication** command, combined with a keyword, can be used to specify how the system will perform authentication of registration request messages.

**Example**

The following command configures the HA service to always perform mobile node authentication for every registration request.
```
authentication mn-aaa always
```

The following command configures the HA service to always look for an MN-HA authentication extension in the RRQ.
```
authentication mn-ha always
```
bind

Binds the HA service to a logical IP interface serving as the Pi interface and specifies the maximum number of subscribers that can access this service over the interface.

**Product**
HA

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > HA Service Configuration
```
configure > context context_name > ha-service service_name
```

Entering the above command sequence results in the following prompt:
```
[context_name]host_name(config-ha-service)#
```

**Syntax**
```
bind address address|range_address ip_mask | range_address/bitmask [ max-subscribers count ]
```
```
no bind address
```

**address**
Specifies the IP address (address) of the interface configured as the Pi interface. *address* is specified in IPv4 dotted-decimal notation.

**range_address ip_mask | range_address/bitmask**
Specifies the pool of IP addresses (IPv4) of the interface configured as the Pi interface with an enterprise HA (EHA). *ip_mask* and *bit_mask* specify the number of subnet bits, representing the subnet mask in CIDR notation and must be a value between 1 to 32. *range_address* is a preconfigured range of IPv4 addresses in Loopback Interface Configuration Mode to enable the Enterprise HA support with enhanced capacity and configured

**max-subscribers count**
Default: 2500000
Specifies the maximum number of subscribers that can access this service on this interface. *count* can be configured to an integer from 0 through 4000000.

**Important:** The maximum number of subscribers supported is dependant on the license key installed and the number of active packet processing cards installed in the system.
Usage

Associate the HA service to a specific logical IP address. The logical IP address or interface takes on the characteristics of a Pi interface. Only one interface can be bound to a service. The interface should be configured prior to issuing this command. This command also sets a limit as to the number of simultaneous subscribers sessions that can be facilitated by the service/interface at any given time.

When configuring the `max-subscribers` option, be sure to consider the following:

- The total number of interfaces that you will configuring for use as Pi interfaces
- The maximum number of subscriber sessions that all of these interfaces may handle during peak busy hours
- The average bandwidth for each of the sessions
- The type of physical port to which these interfaces will be bound

Taking these factors into account and distributing your subscriber session across all available interfaces will allow you to configure your interfaces to optimally handle sessions without degraded performance.

IP range support is provided through `ranged_address` value. This value enables the pool of IPv4 addresses to support Enterprise HA on HA service to connect enhanced number of enterprise nodes. Refer HA Administration Guide for more information.

Use the `no bind address` command to delete a previously configured binding.

Example

The following command would bind the logical IP interface with the address of 192.168.3.1 to the HA service and specifies that a maximum of 600 simultaneous subscriber sessions can be facilitated by the interface/service at any given time.

```
bind address 192.168.3.1 max-subscribers 600
```

The following command disables a binding that was previously configured:

```
no bind address
```

The following command binds the range of IP addresses with HA service to be used with Enterprise HA support:

```
bind address 10.2.3.0/24
```
encapsulation

Configures Mobile IP (MIP) encapsulation types supported for a specific HA service.

**Product**
HA

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > HA Service Configuration

```
configure > context context_name > ha-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ha-service)#
```

**Syntax**

```
[ no ] encapsulation allow { gre | keyless-gre }
```

**no**
Disables MIP encapsulation types supported for specific HA service

**allow**
Allows encapsulation type for MIP data.

```
**gre**
Default: Enabled.
Specifies the use of Generic Routing Encapsulation (GRE) for MIP data.
```

```
**keyless-gre**
Default: Disabled.
Specifies the use of GRE without exchanging keys for MIP data.
```

**Usage**
Use to disable or re-enable the use of GRE encapsulation or Key-less encapsulation for MIP sessions.
In case of chassis HA operating with other vendor equipment, which does not support the 3GPP2 to exchange key, this command with **keyless-gre** keyword will make the chassis HA to accept MIP data with legacy GRE.

**Example**
To disable GRE for MIP sessions, enter the following command:

```
no encapsulation allow gre
```

To re-enable GRE for MIP sessions, enter the following command:

```
encapsulation allow gre
```

To enable key-less GRE for MIP sessions, enter the following command:
encapsulation allow keyless-gre
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

`exit`

**Usage**

Use this command to return to the parent configuration mode.
fa-ha-spi

Configures the security parameter index (SPI) for specific HA service parameters.

**Product**
HA

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > HA Service Configuration

```
configure > context context_name > ha-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ha-service)#
```

**Syntax**

```
fa-ha-spi remote-address { fa_ip_address | fa_ip_address_mask } spi-number number {
encrypted secret enc_secret | secret secret } [ allow-fa-ha-auth-extension ] [ description string ] [ disallow-fa-ha-auth-extension ] [ hash-algorithm { hmac-md5 | md5 | rfc2002-md5 } ] [ replay-protection { nonce | timestamp [ timestamp-tolerance tolerance ] } ] [ timestamp-tolerance tolerance ]
```

```
no fa-ha-spi remote-address { fa_ip_address | fa_ip_address_mask } spi-number number
```

```
no
```

Disables the security parameter index (SPI) for specific HA service parameters.

```
remote-address { fa_ip_address | fa_ip_address_mask }
```

Specifies the IP address of the FA. `fa_ip_address` is entered using IPv4 dotted-decimal notation with CIDR for the subnet mask.

**Important:** The system supports unlimited peer FA addresses per HA but only maintains statistics for a maximum of 8,192 peer FAs. If more than 8,192 FAs are attached, older statistics are overwritten.

```
spi-number number
```

Specifies the SPI (number) which indicates a security context between the FA and the HA in accordance with RFC 2002.

`number` is an integer value from 256 through 4294967295.

```
encrypted secret enc_secret | secret secret
```

Configures the shared-secret between the HA service and the FA. The secret can be either encrypted or non-encrypted.

`encrypted secret enc_secret`: Specifies the encrypted shared key between the HA service and the FA. `enc_secret` must be an alphanumeric string of 1 through 236 characters that is case sensitive.
secret secret: Specifies the shared key between the HA service and the FA. secret must be an alphanumeric string of 1 through 236 characters that is case sensitive.

allow-fa-ha-auth-extension
Allows validation of FA HA Authentication extension.

description string
This is a description for the SPI. string must be an alphanumeric string of 0 through 31 characters.

hash-algorithm { hmac-md5 | md5 | rfc2002-md5 }
Default: hmac-md5
Specifies the hash-algorithm used between the HA service and the FA.
  hmac-md5: Configures the hash-algorithm to implement HMAC-MD5 per RFC 2002bis.
  md5: Configures the hash-algorithm to implement MD5 per RFC 1321.
  rfc2002-md5: Configures the hash-algorithm to implement keyed-MD5 per RFC 2002.

replay-protection { timestamp [ timestamp-tolerance tolerance ] | nonce }
Specifies the replay-protection scheme that should be implemented by the FA service for this SPI.
  nonce: Configures replay protection to be implemented using NONCE per RFC 2002.
  timestamp: Configures replay protection to be implemented using timestamps per RFC 2002.
  timestamp-tolerance: Specifies the allowable difference (tolerance) in timestamps that is acceptable. If the difference is exceeded, then the session will be rejected. tolerance is measured in seconds and can be configured to an integer from 1 and 65535. The default is 60.

Usage
An SPI is a security mechanism configured and shared by the HA service and the FA. Please refer to RFC 2002 for additional information.
Though it is possible for FAs and HAs to communicate without SPIs being configured, the use of them is recommended for security purposes. It is also recommended that a “default” SPI with a remote address of 0.0.0.0/0 be configured on both the HA and FA to prevent hackers from spoofing addresses.

Important: The SPI configuration on the HA must match the SPI configuration for the FA service on the system in order for the two devices to communicate properly.

A maximum of 2,048 SPIs can be configured per HA service.
Use the no version of this command to delete a previously configured SPI.

Example
The following command configures the FA service to use an SPI of 512 when communicating with an HA with the IP address 192.168.0.2. The key that would be shared between the HA and the FA service is q397F65. When communicating with this HA, the FA service will also be configured to use the rfc2002-md5 hash-algorithm.

    fa-ha-spi remote-address 192.168.0.2 spi-number 512 secret q397F65 hash-algorithm rfc2002-md5

The following command deletes the configured SPI of 400 for an HA with an IP address of 172.100.3.200:

    no fa-ha-spi remote-address 172.100.3.200 spi-number 400
**gre**

Configures Generic Routing Encapsulation (GRE) parameters.

**Product**

HA

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > HA Service Configuration

```
configure > context context_name > ha-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ha-service)#
```

**Syntax**

```
gre { checksum | checksum-verify | reorder-timeout timeout | sequence-mode { none | reorder } | sequence-numbers }
```

```default gre { checksum | checksum-verify | reorder-timeout | sequence-mode | sequence-numbers }
```

**no**

Disables the specified functionality.

**default**

Sets or restores default value assigned for specified parameter.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>checksum</strong></td>
<td>disabled</td>
<td>Enables the introduction of the checksum field in outgoing GRE packets.</td>
</tr>
<tr>
<td><strong>checksum-verify</strong></td>
<td>disabled</td>
<td>Enables verification of the GRE checksum (if present) in incoming GRE packets.</td>
</tr>
<tr>
<td><strong>reorder-timeout timeout</strong></td>
<td>100</td>
<td>Configures the maximum number of milliseconds to wait before processing reordered out-of-sequence GRE packets. timeout must be an integer from 0 through 5000.</td>
</tr>
<tr>
<td>**sequence-mode { none</td>
<td>reorder }**</td>
<td>none</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>none</strong>: Disables reordering of incoming out-of-sequence GRE packets.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>reorder</strong>: Enables reordering of incoming out-of-sequence GRE packets.</td>
</tr>
</tbody>
</table>
sequence-numbers

Default: Disabled
Enables the insertion of sequence numbers into the GRE packets.

Usage
Use this command to configure how the HA service handles GRE packets.

Example
To set the maximum number of milliseconds to wait before processing reordered out-of-sequence GRE packets to 500 milliseconds, enter the following command:

```
gre reorder-timeout 500
```

To enable the reordering of incoming out of sequence GRE packets, enter the following command:

```
gre sequence-mode reorder
```

To enable the insertion or removal of GRE sequence numbers in GRE packets, enter the following command:

```
gre sequence-numbers
```
idle-timeout-mode

Configures the sessions idle-timer reset behavior.

**Product**
HA

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > HA Service Configuration

```
configure > context context_name > ha-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ha-service)#
```

**Syntax**

```
idle-timeout-mode { aggressive | handoff | normal } [ upstream-only ]
```

**default idle-timeout-mode**

```
default
Resets the idle timeout mode to the default settings.
```

```
aggressive
Resets the session idle timer only when MIP user data is detected. This is the default behavior.
```

```
handoff
Resets the session idle timer when MIP user data is detected and an inter-Access Gateway/FA handoff occurs.
```

```
normal
Resets the session idle timer when MIP user data is detected and any MIP control signaling occurs.
```

```
upstream-only
Only upstream user data (data from the mobile node) resets the idle timer for the session. This is disabled by default.
```

**Usage**

Use this command to set how the current HA service resets the idle timer for a session.

**Example**

To reset the idle timer whenever user data is detected or whenever an inter-Access Gateway/FA occurs, use the following command:

```
idle-timeout-mode handoff
```
ikev1

Configures IPSec Internet Key Exchange (IKE) parameters.

**Product**
HA

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > HA Service Configuration

`configure > context context_name > ha-service service_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ha-service)#
```

**Syntax**

```
ikev1 { aaa-context aaa_context_string | peer-fa IPAddress crypto-map crypto_map_string [ encrypted ] [ secret secret_string ] | skew-lifetime seconds }no ikev1 { aaa-context | peer-fa IPAddress | skew-lifetime }
```

no

Disables IPSec IKE parameters.

**aaa-context aaa_context_string**
Configures AAA context from which to retrieve IKE keys. Must be followed by the context name.

`aaa_context_string` is an alphanumeric string of 1 through 63 characters.

**peer-fa IPAddress**
Sets the IKE crypto-map for a peer Foreign Agent (FA).

`IPAddress` is IP address entered using IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

**crypto-map crypto_map_string**
Configures IKE crypto-map. Must be followed by the crypto-map name.

`crypto_map_string` is an alphanumeric string of 1 through 63 characters.

**encrypted** designates use of encryption

**secret secret_string** uses a secret that is shared between FA and HA. `secret_string` is an alphanumeric string of 1 through 256 characters.

**skew-lifetime seconds**
Configures the “S” lifetime Skew (in seconds). `seconds` is an integer from 1 through 65534. Default is 10.

**Usage**
Use this command to configure IPSec IKE parameters.

**Example**

```
ikev1 peer-fa 11.22.33.44 crypto-map er encrypted secret ert
**ip context-name**

Specifies name of the destination context to be applied to the subscribers.

This configuration overrides the local subscriber configuration as well as the return attributes sent by RADIUS. All calls coming to this HA service are assigned this destination context; the IP address is allocated from the specified IP pool or group that is configured in the context specified in the service.

**Product**

HA

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > HA Service Configuration

```
classify > context context_name > ha-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ha-service)#
```

**Syntax**

```
ip context-name name

{ default | no } ip context-name

name

Specifies the name of the context to assign the subscriber to once authenticated. *name* must be an alphanumeric string from 1 through 79 characters.

no

Usage**

Removes the current assigned context from the subscriber’s data. Set the name of the destination context to be applied to the subscribers.

**Example**

```
ip context-name sampleName
no ip context-name
```
ip local-port

Configures the local User Datagram Protocol (UDP) port for the Pi interface’s IP socket on which to listen for Mobile IP Registration messages.

Product
HA

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > HA Service Configuration

Syntax

ip local-port number

default ip local-port

default

Sets or restores the default value assigned for the IP local port.

number

Specifies the UDP port number.

number is an integer from 1 through 65535. Default is 434.

Usage

Specify the UDP port that should be used for communications between the FA service and the HA.

Example

The following command specifies a UDP port of 3950 for the HA service to use to communicate with the HA on the Pi interface:

    ip local-port 3950
ip pool

Specifies name of the IP address pool or group to use for subscriber IP address allocation. This configuration overrides the local subscriber configuration, as well as the return attributes sent by RADIUS. All calls coming to this HA service are assigned this destination context and an IP address is allocated from the specified IP pool or group that is configured in the context specified in the service.

Product
HA

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > HA Service Configuration

Syntax

```
ip pool name
{ default | no } ip pool

name
Specifies the logical name of the IP address pool. name must be an alphanumeric string of 1 through 31 characters.

no
Removes the specified IP address pool specified from the current context or disables the option for an IP pool.

default
Clears the IP address pool or group setting.
```

Usage
Define a pool of IP addresses for the context to use in assigning IPs for this service.

Example
The specifies name of the IP address pool or group to use for subscriber IP address allocation:

```
   ip pool pool1
```

The following command removes the specified IP address pool:

```
   no ip pool pool1
```
min-reg-lifetime

Configures Mobile IP session minimum registration lifetime, in seconds.

**Product**

HA

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > HA Service Configuration

```
configure > context context_name > ha-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ha-service)#
```

**Syntax**

```
[ no | default ] min-reg-lifetime min_reg_lifetime_seconds
```

**no**

Disables the min registered lifetime.

**default**

Configures Mobile IP session minimum registration lifetime to default which is 0.

```
default
```

**min-reg-lifetime**

Configures Mobile IP session minimum registration lifetime.

```
min_reg_lifetime_seconds
```

Variable in the range between 1 and 65534.

**Usage**

Use this command to configure Mobile IP session minimum registration lifetime, in seconds, between 1 and 65534. Default is 0 seconds.

**Example**

Use the following command to configure mobile IP session to minimum registered life time to 100 seconds:

```
min-reg-lifetime 100
```
**mn-ha-spi**

Configures the security parameter index (SPI) between the HA service and the mobile node (MN).

**Product**
HA

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > HA Service Configuration

```bash
configure > context context_name > ha-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ha-service)#
```

**Syntax**

```
mn-ha-spi spi-number number [ description string ] [ encrypted secret enc_secret ] [ hash-algorithm { hmac-md5 | md5 | rfc2002-md5 } ] [ permit-any-hash-algorithm ] [ replay-protection { nonce | timestamp } ] [ secret secret ] [ timestamp-tolerance tolerance ]
```

```bash
no mn-ha-spi spi-number number
```

**spi-number number**

Specifies the SPI (number) which indicates a security context between the mobile node and the HA service in accordance with RFC 2002. `number` can be configured to an integer from 256 through 4294967295.

**description string**

This is a description for the SPI. `string` is an alphanumeric string of 1 through 31 characters.

**encrypted secret enc_secret | secret secret**

Configures the shared-secret between the HA service and the mobile node. The secret can be either encrypted or non-encrypted.

- **encrypted secret `enc_secret`**: Specifies the encrypted shared key between the HA service and the mobile node. `enc_secret` must be an alphanumeric string of 1 through 254 characters that is case sensitive.
- **secret `secret`**: Specifies the shared key between the HA service and the mobile node. `secret` must be an alphanumeric string of 1 through 127 characters that is case sensitive.

The `encrypted` keyword is intended only for use by the chassis while saving configuration scripts. The system displays the `encrypted` keyword in the configuration file as a flag that the variable following the `secret` keyword is the encrypted version of the plain text secret key. Only the encrypted secret key is saved as part of the configuration file.

**hash-algorithm { hmac-md5 | md5 | rfc2002-md5 }**

Default: hmac-md5

Specifies the hash-algorithm used between the HA service and the mobile node.

- **hmac-md5**: Configures the hash-algorithm to implement HMAC-MD5 per RFC 2002bis.
- **md5**: Configures the hash-algorithm to implement MD5 per RFC 1321.
- **rfc2002-md5**: Configures the hash-algorithm to implement keyed-MD5 per RFC 2002.
permit-any-hash-algorithm
Default: disabled
Allows verification of the MN-HA authenticator using all other hash-algorithms after failure with configured hash-algorithm. The successful algorithm is logged to aid in troubleshooting and used to create the MN-HA authenticator in the Registration Reply message.

replay-protection { nonce | timestamp }
Default: timestamp
Specifies the replay-protection scheme that should be implemented by the HA service for this SPI.
nonce: configures replay protection to be implemented using NONCE per RFC 2002.
timestamp: configures replay protection to be implemented using timestamps per RFC 2002.

timestamp-tolerance tolerance
Default: 60
Specifies the allowable difference (tolerance) in timestamps that is acceptable. If the difference is exceeded, then the session will be rejected. If this is set to 0, timestamp tolerance checking is disabled at the receiving end.
Tolerance is measured in seconds and can be configured to an integer from 0 through 65535.

Usage
An SPI is a security mechanism configured and shared by the HA service and the mobile node. Please refer to RFC 2002 for additional information.
Use the no version of this command to delete a previously configured SPI.

Example
The following command configures the HA service to use an SPI of 640 when communicating with a mobile node. The key that would be shared between the mobile node and the HA service is q397F65.

    mn-ha-spi spi-number 640 secret q397F65

The following command deletes the configured SPI of 400:

    no mn-ha-spi spi-number 400
nat-traversal

This command enables NAT traversal and also configures the forcing of UDP tunnels for NAT traversal.

Product
HA

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > HA Service Configuration

configure > context context_name > ha-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ha-service)#

Syntax

[ default | no ] nat-traversal [ force-accept ]

<table>
<thead>
<tr>
<th>no</th>
</tr>
</thead>
</table>
| Disables NAT traversal or disables forcing the acceptance of UDP tunnels for NAT traversal.

<table>
<thead>
<tr>
<th>default</th>
</tr>
</thead>
</table>
| Reset the defaults for this command.
Default: NAT traversal disabled, force-accept disabled.

<table>
<thead>
<tr>
<th>force-accept</th>
</tr>
</thead>
</table>
| This keyword configures the HA to accept requests when NAT is not detected but the Force (F) bit is set in the RRQ with the UDP Tunnel Request. By default this type of request is rejected if NAT is not detected.

Usage
Use this command to enable NAT traversal and enable the forcing of UDP tunnels for NAT traversal.

Example
The following command enables NAT traversal for the current HA service and forces the HA to accept UDP tunnels for NAT traversal:

```
nat-traversal force-accept
```
**optimize tunnel-reassembly**

Designates that tunnel reassembly optimization will be used for fragmented large packets passed between HA and FA. Default is disabled.

**Product**

HA

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > HA Service Configuration

```bash
configure > context context_name > ha-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ha-service)#
```

**Syntax**

```
[ default | no ] optimize tunnel-reassembly
```

**Usage**

Enabling this functionality fragments large packets prior to encapsulation for easier processing.

Tunnel reassembly optimization is disabled by default.

**Important:** You should not use this command without first consulting Cisco Systems Technical Support. This command applies to very specific scenarios where packet reassembly is not supported at the far end of the tunnel. There are cases where the destination network may either discard the data, or be unable to reassemble the packets.

**Important:** This functionality works best when the HA service is communicating with an FA service running in a system. However, an HA service running in the system communicating with an FA from a different manufacturer will operate correctly even if this parameter is enabled.

**Example**

Use the `no` version of this command to disable tunnel optimization if enabled.

The following command enables tunnel reassembly optimization:

```
optimize tunnel-reassembly
```
per-domain statistics-collection

Enables per-domain statistics collection.

**Product**  
HA

**Privilege**  
Security Administrator, Administrator

**Mode**  
Exec > Global Configuration > Context Configuration > HA Service Configuration  
```
configure > context context_name > ha-service service_name
```
Entering the above command sequence results in the following prompt:
```
[context_name]host_name(config-ha-service)#
```

**Syntax**
```
[ no ] per-domain statistics-collection
```

**Usage**

Use this command to enable per-domain statistics collection.

**Example**

The following command enables per-domain statistics collection.
```
per-domain statistics-collection
```
**policy bc-query-result**

Configure the binding cache (BC) query Response Result code.

**Product**
HA

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > HA Service Configuration

```
configure > context context_name > ha-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ha-service)#
```

**Syntax**

```
policy bc-query-result network-failure code
```

**default policy bc-query-result network-failure**

```
    network-failure code
```

**Usage**

Use this command to specify the type of response code to send in a P-MIP BC query result.

**Example**

The following command sets the P-MIP BC query result response code to 0xFFFE:

```
policy bc-query-result network-failure 0xFFFE
```
policy nw-reaching-fail

Specifies the action to take upon detection of an up-stream network-reachability failure.

Product
HA

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > HA Service Configuration

configure > context context_name > ha-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ha-service)#

Syntax

policy nw-reaching-fail { redirect ip_addr1 [ weight value ] [ ip_addr2 [ weight value ] ... ip_addr16 [ weight value ] ] reject [ use-reject-code { admin-prohibited | insufficient-resources } ] }

no policy nw-reaching-fail { redirect ip_addr1 ... ip_addr16 }

no

Deletes the network reachability policy completely or deletes the specified redirect addresses from the policy.

reject [ use-reject-code { admin-prohibited | insufficient-resources } ]

Upon network reachability failure reject all new calls for this context.

text-reject-code { admin-prohibited | insufficient-resources }: When rejecting calls send the specified reject code. If this keyword is not specified the admin-prohibited reject code is sent by default.

reject [ use-reject-code { admin-prohibited | insufficient-resources } ]

Upon network reachability failure reject all new calls for this context. If no reject code is specified, the HA sends a registration reply code of 81H (admin-prohibited).

text-reject-code { admin-prohibited | insufficient-resources }: Use the specified reject code when rejecting traffic.

admin-prohibited: When this keyword is specified and traffic is rejected, the error code 81H (admin-prohibited) is returned.

insufficient-resources: When this keyword is specified and traffic is rejected, the error code 82H (insufficient resources) is returned.

redirect ip_addr1 [ weight value ] [ ip_addr2 [ weight value ] ... ip_addr16 [ weight value ] ]

Upon network reachability failure redirect all calls to the specified IP address.

ip_addr1: This must entered using IPv4 dotted-decimal notation. Up to 16 IP addresses and optional weight values can be entered on one command line.
**weight value:** When multiple addresses are specified, they are selected in a weighted round-robin scheme. If a weight is not specified the entry is automatically assigned a weight of 1. `value` must be an integer from 1 through 10.

**Usage**

Use this command to set the action for the HA service to take upon a network reachability failure.

**Important:** Refer to the Context Configuration mode command `nw-reachability server` to configure network reachability servers.

**Important:** Refer to the Subscriber Configuration mode command `nw-reachability-server` to bind the network reachability to a specific subscriber.

**Important:** Refer to the `nw-reachability server server_name` keyword of the Context Configuration mode `ip pool` command to bind the network reachability server to an IP pool.

**Example**

To set the HA service to reject all new calls on a network reachability failure, enter the following command:

```
policy nw-reachability-fail reject
```

Use the following command to set the HA service to redirect all calls to the HA at IP address `192.168.100.10` and `192.168.200.10` on a network reachability failure:

```
policy nw-reachability-fail redirect 192.168.100.10 192.168.200.10
```
policy overload

Configures the overload policy within the HA service.

**Product**

HA

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > HA Service Configuration

```
configure > context context_name > ha-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ha-service)#
```

**Syntax**

```
policyoverload { redirect address [ weight weight_num ] [ address2 [ weight weight_num ] ... address16 [ weight weight_num ] ] | reject[ use-reject-code { admin-prohibited | insufficient-resources } ] }

no policyoverload [ redirect address [ address2...address16 ] ]
```

Deletes a previously set policy or removes a redirect IP address.

- **overload**: Without any options deletes the complete overload policy from the PDSN service.
- **overload redirect address [address2 ... address16]**: deletes up to 16 IP addresses from the overload redirect policy. The IP addresses must be expressed in IP v4 dotted-decimal notation.

```
redirect address [ weight weight_num ] [ address2 [ weight weight_num ] ... address16 [ weight weight_num ] ]
```

This option enables a redirect policy for overloading conditions. When a redirect policy is invoked, the HA service rejects new sessions with a Registration Reply Code of 136H (unknown home agent address) and provides the IP address of an alternate HA. This command can be issued multiple times.

- **address**: The IP address of an alternate HA expressed in IP v4 dotted-decimal notation. Up to 16 IP addresses can be specified either in one command or by issuing the redirect command multiple times. If you try to add more than 16 IP addresses to the redirect policy, the CLI issues an error message. If you specify an IP address and weight that already exists in the redirect policy the new values override the existing values.

- **weight weight_num**: When multiple addresses are specified, they are selected in a weighted round-robin scheme. Entries with higher weights are more likely to be chosen. If a weight is not specified the entry is automatically assigned a weight of 1. weight_num must be an integer from 1 through 10.

```
reject [ use-reject-code { admin-prohibited | insufficient-resources } ]
```

This option causes any overload traffic to be rejected. If no reject code is specified, the HA sends a registration reply code of 81H (admin-prohibited).

- **use-reject-code { admin-prohibited | insufficient-resources }**: Use the specified reject code when rejecting traffic.
admin-prohibited: When this keyword is specified and traffic is rejected, the error code 81H (admin-prohibited) is returned.

insufficient-resources: When this keyword is specified and traffic is rejected, the error code 82H (insufficient resources) is returned.

Usage
The system invokes the overload policy if the number of calls currently being processed exceeds the licensed limit for the maximum number of sessions supported by the system.
The system automatically invokes the overload policy when an on-line software upgrade is started.
Use the no version of this command to restore the default policy.
The setting for overload policy is reject.

Example
The following command enables an overload redirect policy for the HA service that will send overload calls to either of two destinations with weights of 1 and 10 respectively:

```
policy overload redirect 192.168.100.10 weight 1 192.168.100.20 weight 10
```
reg-lifetime

Configures Mobile IP session registration lifetime.

Product

HA

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > Context Configuration > HA Service Configuration configure > context context_name > ha-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ha-service)#

Syntax

reg-lifetime time

{ default | no } reg-lifetime

no

Sets the registration lifetime to infinite.

default

Sets the registration lifetime to default value, 600.

time

Specifies the registration lifetime in seconds. 
time is an integer from 1 through 65534.

Usage

Use this command o limit a mobile node’s lifetime. If the mobile node requests a shorter lifetime than what is specified, it is granted. However, Per RFC 2002, should a mobile node request a lifetime that is longer than the maximum allowed by this parameter, the HA service will respond with the value configured by this command as part of the Registration Reply. The default is 600 seconds.

Example

The following command configures the registration lifetime for the HA service to be 2400 seconds:

reg-lifetime 2400

The following command configures an infinite registration lifetime for MIP calls:

no reg-lifetime
reverse-tunnel

Enables use of reverse tunneling for Mobile IP session. Use no reverse-tunnel command to disable. If disabled, mobile node (MN) packets are not tunneled to the HA in the reverse direction.

Product
HA

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > HA Service Configuration

configure > context context_name > ha-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ha-service)#

Syntax
reverse-tunnel

{ default | no } reverse-tunnel

---

no

Indicates the reverse tunnel option is to be disabled. When omitted, the reverse tunnel option is enabled.

---

default

Indicates the reverse tunnel option is to be set to the default. When omitted, the reverse tunnel option is enabled.

Usage
Reverse tunneling involves tunneling datagrams originated by the mobile node to the HA service via the FA. When an MN arrives at a foreign network, it listens for agent advertisements and selects an FA that supports reverse tunnels. The MN requests this service when it registers through the selected FA. At this time, the MN may also specify a delivery technique such as Direct or the Encapsulating Delivery Style.

Among the advantages of using reverse-tunneling are that:
- All datagrams from the mobile node seem to originate from its home network
- The FA can keep track of the HA to which the mobile node is registered and tunnel all datagrams from the mobile node to its HA

Use the no version of this command to disable reverse tunneling. If reverse tunneling is disabled, and the mobile node does not request it, triangular routing will be performed.
Routing will be used.
The default setting is reverse tunnel enabled.

**Important:** If reverse tunneling is disabled on the system and a mobile node requests it, the call will be rejected with a reply code of 74H (reverse-tunneling unavailable).
Example

The following command disables reverse-tunneling support for the HA service:

```
no reverse-tunnel
```
**revocation**

Configures the Registration Revocation feature for a specific HA service.

**Product**
HA

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > HA Service Configuration

```bash
configure > context context_name > ha-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ha-service)#
```

**Syntax**

```
revocation { enable | max-retransmission number | negotiate-i-bit | retransmission-timeout secs | send-nai-ext | trigger { handoff | idle-timeout } }
no revocation { enable | negotiate-i-bit | send-nai-ext | trigger { handoff | idle-timeout } }
```

```
default revocation [ enable ] [ max-retransmission ] [ negotiate-i-bit ] [ retransmission-timeout ] [ send-nai-ext ] [ trigger { handoff | idle-timeout } ]
default
```

```
no
```

Completely disables registration revocation on the HA, disables trigger handoff, or disables revocation on idle timer expiration.

```
default
```

Sets or restores the default value assigned for specified parameter.

```
enable
```

Enables the MIP registration revocation feature on the HA. When enabled, if revocation is negotiated with an FA and a MIP binding is terminated, the HA can send a Revocation message to the FA. This feature is disabled by default.

```
max-retransmission number
```

Default: 3
The maximum number of retransmissions of a Revocation message before the revocation fails. `number` must be an integer from 0 through 10.

```
negotiate-i-bit
```

Default: disabled
Enables the HA to negotiate the i-bit via PRQ/RRP messages and processes the i-bit revocation messages.
**retransmission-timeout secs**
Default: 3
The number of seconds to wait for a Revocation Acknowledgement from the FA before retransmitting the Revocation message. *secs* must be an integer from 1 through 10.

**send-nai-ext**
Default: off
Enables sending the NAI extension in the revocation message.

**trigger { handoff | idle-timeout }**

**handoff**: Default: Enabled
Triggers the HA to send a Revocation message to the FA when an inter-Access Gateway/FA handoff of the MIP session occurs. If this is disabled, the HA is never triggered to send a Revocation message.

**idle-timeout**: Default: Enabled
Triggers the HA to send a Revocation message to the FA when a session idle timer expires.

---

**Usage**

Use this command to enable or disable the MIP revocation feature on the HA or to change settings for this feature. Both the HA and the FA must have Registration Revocation enabled and FA/HA authorization must be in use for Registration Revocation to be negotiated successfully.

**Example**

The following command enables Registration Revocation on the HA:

```
revocation enable
```

The following command sets the maximum number of retries for a Revocation message to 10:

```
revocation max-retransmission 10
```

The following command sets the timeout between retransmissions to 3:

```
revocation retransmission-timeout 3
```

The behavior of send MIP revocation to FA is as follows:

- 1st retry: Retransmit in 3 seconds after previous MIP revocation send.
- 2nd retry: Retransmit in 6 seconds after previous MIP revocation send (9 seconds after sending initial MIP revocation).
- 3rd retry: Retransmit in 12 seconds after previous MIP revocation send (21 seconds after sending initial MIP revocation).
- 4th retry: Retransmit in 24 seconds after previous MIP revocation send (45 seconds after sending initial MIP revocation).
- 5th retry: Retransmit in 48 seconds after previous MIP revocation send (93 seconds after sending initial MIP revocation).

---

**Important**: The value of retransmission-timeout doubles. HA disconnects the session forcibly in 120 seconds after sending initial MIP revocation.
**setup-timeout**

The maximum time allowed for session setup in seconds. Default is 60 seconds.

**Product**
HA

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > HA Service Configuration

`configure > context context_name > ha-service service_name`

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-ha-service)#`

**Syntax**

```
setup-timeout seconds

default setup-timeout

default

Sets or restores the default value.

seconds

Default: 60 seconds
The maximum amount of time (in seconds) to allow for setup of a session. `seconds` must be an integer from 1 through 1000000
```

**Usage**

Use this command to set the maximum amount of time allowed for setting up a session.

**Example**

To set the maximum time allowed for setting up a session to 5 minutes (300 seconds), enter the following command:

```
setup-timeout 300
```
**simul-bindings**

Specifies the maximum number of “care-of” addresses that can simultaneously be bound for the same user as identified by NAI and Home address.

**Product**
HA

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > HA Service Configuration

```
configure > context context_name > ha-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ha-service)#
```

**Syntax**

```
simul-bindings number
```

**default simul-bindings**

```
default

Sets or restores the default value.
```

```
number

Configures the maximum number of simultaneous “care-of” bindings that the HA service will maintain for any given subscriber.

is an integer from 1 through 3.
```

**Usage**

Per RFC 2002, the HA service creates a mobile binding record (MBR) for each subscriber session it is facilitating. Each MBR is associated with a care-of address. As the mobile node roams, it is possible that the session will be associated with a new care of address.

Typically, the HA service will delete an old binding and create a new one when the information in the Registration Request changes. However, the mobile could request that the HA maintain previously stored MBRs. This command allows you to configure the maximum number of MBRs that can be stored per subscriber if the requested. The default value is 3.

**Example**

The following command configures the HA service to support up to 4 MBRs per subscriber:

```
simul-bindings 4
```
### threshold dereg-reply-error

Sets an alarm or alert based on the number of de-registration reply errors per HA service.

**Product**
HA

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > HA Service Configuration

```sh
configure > context context_name > ha-service service_name
```

Entering the above command sequence results in the following prompt:
```
[context_name]host_name(config-ha-service)#
```

**Syntax**

```sh
threshold dereg-reply-error high_thresh [ clear low_thresh ]
```

```sh
no threshold dereg-reply-error
```

- **no**
  - Deletes the alert or alarm.

- **high_thresh**
  - Default: 0
  - Specifies the high threshold number of de-registration reply errors that must be met or exceeded within the polling interval to generate an alert or alarm. It can be configured to an integer from 0 through 100000.

- **clear low_thresh**
  - Default: 0
  - The low threshold number of de-registration reply errors that must be met or exceeded within the polling interval to clear an alert or alarm. It can be configured to an integer from 0 through 100000.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**

Use this command to set an alert or an alarm when the number of de-registration reply errors is equal to or greater than a specified number of calls per second. Alerts or alarms are triggered for the number of de-registration reply errors on the following rules:

- **Enter condition:** Actual number of de-registration reply errors > High Threshold
- **Clear condition:** Actual number of de-registration reply errors < Low Threshold

**Example**

```sh
threshold dereg-reply-error 50
clear low_thresh
```
The following command configures a de-registration reply error threshold of 1000 and a low threshold of 500 for a system using the Alarm thresholding model:

```
threshold reg-reply-error 1000 clear 500
```
threshold init-rrq-rcvd-rate

Sets an alarm or alert based on the average number of calls setup per second for the context.

**Product**
HA

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > HA Service Configuration

```
configure > context context_name > ha-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ha-service)#
```

**Syntax**

```
threshold init-rrq-rcvd-rate high_thresh [ clear low_thresh ]
```

```
no threshold init-rrq-rcvd-rate
```

```
no
```

Deletes the alert or alarm.

```
high_thresh
```

Default: 0

Specifies the high threshold average number of calls setup per second that must be met or exceeded within the polling interval to generate an alert or alarm. `high_thresh` is an integer from 0 through 100000.

```
clear low_thresh
```

Default: 0

The low threshold average number of calls setup per second that must be met or exceeded within the polling interval to clear an alert or alarm. `low_thresh` is an integer from 0 through 100000.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**

Use this command to set an alert or an alarm when the average number of calls setup per second is equal to or greater than a specified number of calls per second.

Alerts or alarms are triggered for the number of calls setup per second based on the following rules:

- **Enter condition:** Actual number of calls setup per second is greater than the high threshold.
- **Clear condition:** Actual number of calls setup per second is less that the low threshold.

**Example**
The following command configures a number of calls setup per second threshold of 1000 and a low threshold of 500 for a system using the Alarm thresholding model:

```plaintext
threshold init-rrq-rcvd-rate 1000 clear 500
```
threshold ipsec-call-req-rej

Configures a threshold for the total IPSec calls request rejected.

**Product**
HA

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > HA Service Configuration

```
configure > context context_name > ha-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ha-service)#
```

**Syntax**

```
threshold ipsec-call-req-rej high_thresh [ clear low_thresh ]

no threshold ipsec-call-req-rej
```

**no**

Deletes the alert or alarm.

```
high_thresh
Default: 0
Specifies the high threshold number of IPSec call requests rejected per second that must be met or exceeded within the polling interval to generate an alert or alarm.
high_thresh is an integer from 0 through 1000000.
```

```
clear low_thresh
Default: 0
Specifies the low threshold number of IPSec call requests rejected per second that must be met or exceeded within the polling interval to clear an alert or alarm.
low_thresh is an integer from 0 through 1000000.
```

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**

Use this command to set an alert or an alarm when the number of IPSec call requests rejected is equal to or greater than a specified number per second. Alerts or alarms are triggered for the number of IPSec IKE requests on the following rules:

- **Enter condition:** Actual number of IPSec IKE requests is greater than the high threshold.
- **Clear condition:** Actual number of IPSec IKE requests is less than the low threshold.
Example

The following command configures a number of IPSec call requests rejected threshold of 1000 and a low threshold of 800 for a system using the Alarm thresholding model:

```
threshold ipsec-call-req-rej 1000 clear 800
```
threshold ipsec-ike-failrate

Configures a threshold for the percentage of IPSec IKE failures.

Product
HA

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > HA Service Configuration

configure > context context_name > ha-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ha-service)#

Syntax

threshold ipsec-ike-failrate high_thresh [ clear low_thresh ]

no threshold ipsec-ike-failrate

---

no

Deletes the alert or alarm.

---

high_thresh

Default: 0

Specifies the high threshold percentage of IPSec IKE failures per second that must be met or exceeded within the polling interval to generate an alert or alarm.

high_thresh is an integer from 0 through 100.

---

clear low_thresh

Default: 0

Specifies the low threshold percentage of IPSec IKE failures per second that must be met or exceeded within the polling interval to clear an alert or alarm.

low_thresh is an integer from 0 through 100.

---

**Important**: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

---

Usage

Use this command to set an alert or an alarm when the percentage of IPSec IKE failures is equal to or greater than a specified number per second.

Alerts or alarms are triggered for the percentage of IPSec IKE failures on the following rules:

- **Enter condition**: Percentage of IPSec IKE failures is greater than the high threshold.
- **Clear condition**: Percentage of IPSec IKE failures is less than the low threshold.
Example

The following command configures a percentage of IPSec IKE failures threshold of 1000 and a low threshold of 800 for a system using the Alarm thresholding model:

```
threshold ipsec-ike-failrate 90 clear 80
```
threshold ipsec-ike-failures

Configures a threshold for the total IPSec IKE failures.

**Product**
HA

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > HA Service Configuration

```
configure > context context_name > ha-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ha-service)#
```

**Syntax**

```
threshold ipsec-ike-failures high_thresh [ clear low_thresh ]
```

```
no threshold ipsec-ike-failures
```

- **no**
  Deletes the alert or alarm.

- **high_thresh**
  Default: 0
  Specifies the high threshold number of IPSec IKE failures per second that must be met or exceeded within the polling interval to generate an alert or alarm.
  `high_thresh` is an integer from 0 through 1000000.

- **clear low_thresh**
  Default: 0
  Specifies the low threshold number of call IPSec IKE failures per second that must be met or exceeded within the polling interval to clear an alert or alarm.
  `low_thresh` is an integer from 0 through 1000000.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**

Use this command to set an alert or an alarm when the number of IPSec IKE failures is equal to or greater than a specified number per second.

Alerts or alarms are triggered for the number of IPSec IKE failures on the following rules:

- **Enter condition:** Actual number of IPSec IKE failures is greater than the high threshold.
- **Clear condition:** Actual number of IPSec IKE failures is less than the low threshold.
Example

The following command configures a number of IPSec IKE failures threshold of 1000 and a low threshold of 800 for a system using the Alarm thresholding model:

```
threshold ipsec-ike-failures 1000 clear 800
```
**threshold ipsec-ike-requests**

Configures a threshold for the total IPSec IKE requests.

**Product**
HA

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > HA Service Configuration

```
configure > context context_name > ha-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config- ha-service)#
```

**Syntax**

```
threshold ipsec-ike-requests high_thresh [ clear low_thresh ]
```

```
no threshold ipsec-ike-requests
```

- **no**
  Deletes the alert or alarm.

- **high_thresh**
  Default: 0
  Specifies the high threshold number of IPSec IKE requests per second that must be met or exceeded within the polling interval to generate an alert or alarm.
  *high_thresh* is an integer from 0 through 1000000.

- **clear low_thresh**
  Default: 0
  Specifies the low threshold number of call IPSec IKE requests per second that must be met or exceeded within the polling interval to clear an alert or alarm.
  *low_thresh* is an integer from 0 through 1000000.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**

Use this command to set an alert or an alarm when the number of IPSec IKE requests is equal to or greater than a specified number per second.

Alerts or alarms are triggered for the number of IPSec IKE requests on the following rules:

- **Enter condition:** Actual number of IPSec IKE failures is greater than the high threshold.
- **Clear condition:** Actual number of IPSec IKE failures is less than the low threshold.
Example

The following command configures a number of IPSec IKE requests threshold of 1000 and a low threshold of 800 for a system using the Alarm thresholding model:

```bash
threshold ipsec-ike-requests 1000 clear 800
```
threshold ipsec-tunnels-established

Configures a threshold for the total IPSec tunnels established.

Product
HA

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > HA Service Configuration

configure > context context_name > ha-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ha-service)#

Syntax

threshold ipsec-tunnels-established high_thresh [ clear low_thresh ]

no threshold ipsec-tunnels-established

no

Deletes the alert or alarm.

high_thresh

Default: 0

Specifies the high threshold number of IPSec tunnels established per second that must be met or exceeded within the polling interval to generate an alert or alarm.

high_thresh is an integer from 0 through 1000000.

clear low_thresh

Default: 0

Specifies the low threshold number of call IPSec tunnels established per second that must be met or exceeded within the polling interval to clear an alert or alarm.

low_thresh is an integer from 0 through 1000000.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Use this command to set an alert or an alarm when the number of IPSec tunnels established is equal to or greater than a specified number per second.

Alerts or alarms are triggered for the number of IPSec tunnels established on the following rules:

• Enter condition: Actual number of IPSec tunnels established is greater than the high threshold.
• Clear condition: Actual number of IPSec tunnels established is less than the low threshold.
Example

The following command configures a number of IPSec tunnels established threshold of 1000 and a low threshold of 800 for a system using the Alarm thresholding model:

```
threshold ipsec-tunnels-established 1000 clear 800
```
threshold ipsec-tunnels-setup

Configures a threshold for the total IPSec tunnels setup.

**Product**
HA

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > HA Service Configuration
configure > context context_name > ha-service service_name

Entering the above command sequence results in the following prompt:

```plaintext
[context_name]host_name(config-ha-service)#
```

**Syntax**

```plaintext
threshold ipsec-tunnels-setup high_thresh [ clear low_thresh ]

no threshold ipsec-tunnels-setup
```

**no**

Deletes the alert or alarm.

**high_thresh**

Default: 0
Specifies the high threshold number of IPSec tunnels setup per second that must be met or exceeded within the polling interval to generate an alert or alarm.

`high_thresh` is an integer from 0 through 1000000.

**clear low_thresh**

Default: 0
Specifies the low threshold number of call IPSec tunnels setup per second that must be met or exceeded within the polling interval to clear an alert or alarm.

`low_thresh` is an integer from 0 through 1000000.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**

Use this command to set an alert or an alarm when the number of IPSec tunnels setup is equal to or greater than a specified number per second.

Alerts or alarms are triggered for the number of IPSec tunnels setup on the following rules:

- **Enter condition:** Actual number of IPSec tunnels setup is greater than the high threshold.
- **Clear condition:** Actual number of IPSec tunnels setup is less than the low threshold.
Example

The following command configures a number of IPSec tunnels setup threshold of 1000 and a low threshold of 800 for a system using the Alarm thresholding model:

```
threshold ipsec-tunnels-setup 1000 clear 800
```
threshold reg-reply-error

Set an alarm or alert based on the number of registration reply errors per HA service.

Product
HA

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > HA Service Configuration

configure > context context_name > ha-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ha-service)#

Syntax

threshold reg-reply-error high_thresh [ clear low_thresh ]

no threshold reg-reply-error

---

no

Deletes the alert or alarm.

---

high_thresh

Default: 0
Specifies the high threshold number of registration reply errors that must be met or exceeded within the polling interval to generate an alert or alarm. high_thresh is an integer from 0 through 100000.

---

clear low_thresh

Default: 0
Specifies the low threshold number of registration reply errors that must be met or exceeded within the polling interval to clear an alert or alarm. low_thresh is an integer from 0 through 100000.

---

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

---

Usage

Use this command to set an alert or an alarm when the number of registration reply errors is equal to or greater than a specified number of calls per second.

Alerts or alarms are triggered for the number of registration reply errors on the following rules:

- **Enter condition:** Actual number of registration reply errors is greater than the high threshold.
- **Clear condition:** Actual number of registration reply errors is less than the low threshold.

---

Example
The following command configures a registration reply error threshold of \(1000\) and a low threshold of \(500\) for a system using the Alarm thresholding model:

```bash
threshold reg-reply-error 1000 clear 500
```
threshold rereg-reply-error

Set an alarm or alert based on the number of re-registration reply errors per HA service.

**Product**
HA

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > HA Service Configuration

```
configure > context context_name > ha-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ha-service)#
```

**Syntax**

```
threshold rereg-reply-error high_thresh [ clear low_thresh ]
```

```
no threshold rereg-reply-error
```

- **no**
  Deletes the alert or alarm.

- **high_thresh**
  Default: 0
  Specifies the high threshold number of re-registration reply errors that must be met or exceeded within the polling interval to generate an alert or alarm. `high_thresh` is an integer from 0 through 100000.

- **clear low_thresh**
  Default: 0
  Specifies the low threshold number of re-registration reply errors that must be met or exceeded within the polling interval to clear an alert or alarm. `low_thresh` is an integer from 0 through 100000.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

**Usage**

Use this command to set an alert or an alarm when the number of re-registration reply errors is equal to or greater than a specified number of calls per second.

Alerts or alarms are triggered for the number of re-registration reply errors on the following rules:

- **Enter condition:** Actual number of re-registration reply errors is greater than the high threshold.

- **Clear condition:** Actual number of re-registration reply errors is less than the low threshold.

**Example**
The following command configures a reregistration reply error threshold of 1000 and a low threshold of 500 for a system using the Alarm thresholding model:

```bash
threshold dereg-reply-error 1000 clear 500
```
wimax-3gpp2 interworking

Configures the interworking between WiMAX and 3GPP2 network at HA. This support provides handoff capabilities from 4G to 3G (PDSN) network access and vice-versa.

**Product**
HA

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > HA Service Configuration

configure > context context_name > ha-service service_name

Entering the above command sequence results in the following prompt:

[(context_name)host_name(config-ha-service)]#

**Syntax**

```
[ no | default ] wimax-3gpp2 interworking
```

- **no**
  Disables the pre-configured interworking between WiMAX and 3GPP2 networks at HA level.

- **default**
  Configures the **WiMAX-3GPP2 interworking** to default setting: disabled.

**Usage**

Use this command to enable/disable the interworking between WiMAX and 3GPP2 network for seamless session continuity.

This functionality provides HA support for both 4G and 3G technology HA (WiMAX HA and PDSN/HA) for handoff from 4G and 3G network access (ASN GW/FA and PDSN/FA) and vice-versa.

**Important:** Use this command in conjunction with the `authentication aaa-distributed-mip-keys required` command.

**Example**

The following command enables the interworking for a subscriber between WiMAX and 3GPP2 network.

```
wimax-3gpp2 interworking
```
Chapter 157
HD Storage Policy Configuration Mode Commands

The HD Storage Policy Configuration Mode is used to configure directory name and file parameters for Diameter record files being stored on the HD storage device.

Mode

Exec > Global Configuration > HD Storage Policy Configuration

configure > hd storage-policy policy_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-hd-storage-policy)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
directory

Configures the name of the directory on the HD storage drive where Diameter records are stored.

**Product**
- HSGW
- P-GW
- SAEGW
- S-GW

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > HD Storage Policy Configuration

```
configure > hd storage-policy policy_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-hd-storage-policy)#
```

**Syntax**

```
directory name dir_name

default directory name
```

- **default**
  Returns the command to its default setting of using the policy name as the directory name.

- **name dir_name**
  Specifies the name to be applied to the directory. *dir_name* must be an alphanumeric string of 1 through 63 characters.
  When configured, the actual directory path is:

  `/hd-raid/records/<record-type>/<dir_name>/`

  So if the directory name variable is entered as “sgwpgw”, the path is:

  `/hd-raid/records/acr/sgwpgw`

**Usage**

Use this command to name a directory on the HD storage drive where Diameter records are to be stored.

**Example**

The following command configures a directory named *cdr1*:

```
directory name cdr1
```
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Use this command to return to the parent configuration mode.
file

Configures file parameters for Diameter records being stored on the HD storage device.

Product
HSGW
P-GW
SAEGW
S-GW

Privilege
Administrator

Mode
Exec > Global Configuration > HD Storage Policy Configuration
configure > hd storage-policy policy_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-hd-storage-policy)#

Syntax

file { format acr { custom1...custom10 } | name { extension string | prefix string } | rotation { record-count num | time-interval sec | volume mb mbytes } }

default file { format acr | name prefix | rotation { record-count | time-interval | volume } }

no file { extension | rotation { record-count | time-interval } }

---

default

Returns the command to the default settings for the specified keywords.

---

no

Removes the configuration for the specified parameters.

---

format acr { custom1...custom10 }

Default: custom1
Specifies the file format used when storing records on the HD storage device. custom1 is a vendor-specific file format.

---

name { extension string | prefix string }

Specifies a string to be pre-pended or appended to the filenames. By default, the policy name is used for the prefix.

extension string: Specifies a file extension to append to the filename. string must be an alphanumeric string of 1 through 10 characters.

prefix string: Specifies a file prefix to append to the filename. string must be an alphanumeric string of 1 through 63 characters. This parameter replaces the policy name used by default.
rotation { record-count num | time-interval sec | volume mb mbytes }

Specifies the triggers that prompt file rotation on the HD storage drive. All options can be configured and upon reaching any of the thresholds, file rotation is initiated.

- **record-count num**: File rotation occurs when the number of records reaches the number configured in this keyword. *num* must be an integer from 1000 through 65000. Default = 10000
- **time-interval sec**: File rotation occurs at time intervals (in seconds) configured by this keyword. *sec* must be an integer from 30 through 86400. Default = 3600 (1 hour)
- **volume mb mbytes**: File rotation occurs when the record volume exceeds the value (in megabytes) configured by this keyword. *mbytes* must be an integer from 2 through 40. Default = 4

### Usage

Use this command to configure file parameters for Diameter records being stored on the HD storage device.

### Example

The following command sets the file rotation thresholds for files being stored on the HD storage device:

```plaintext
file rotation volume mb 4
file rotation record-count 15000
file rotation time-interval 7200
```

The following command replaces the policy name as the prefix of all files being stored through this policy with the prefix *sgw*:

```plaintext
file name prefix sgw
```
A new service “henbgw-access-service” is defined under Context Configuration Mode to initialize HeNB-GW functionality. This service configuration controls the S1-MME interface for communication between HeNB-GW to HeNB(s). HeNBs connect to the S1-MME bind address configured in this service.

**Mode**

Exec > Global Configuration > Context Configuration > HENBGW-ACCESS Service Configuration

```bash
configure > context context_name > henbgw-access-service service_name
```

Entering the above command sequence results in the following prompt:

```bash
[context_name]host_name(config-henbgw-access-service)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
associate henbgw-network-service

Associates a previously configured HeNB-GW Network service to the this HeNB-GW Access service. An HeNB-GW Network service must be configured in Context Configuration mode before using this configuration.

Product
HeNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > HENBGW-ACCESS Service Configuration

configure > context context_name > henbgw-access-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-henbgw-access-service)#

Syntax

associate henbgw-network-service svc_name [ context context_name ]

no associate henbgw-network-service

no

Removes the associated HeNB-GW Network service from this HeNB-GW Access service configuration.

svc_name

Identifies the name of the pre-configured HeNB-GW Network service to associate with this HeNB-GW Access service.

svc_name is an alphanumeric string of 1 through 63 characters.

context context_name

Identifies the name of the context to which the HeNBGW service belongs.

context_name is an alphanumeric string of 1 through 79 characters.

Usage

Use this command to bind/associate a pre-configured HeNB-GW Network service to the this HeNB-GW Access service. The HeNB-GW Network service can be configured in Context configuration mode. The associate configuration is used to establish associations with other helper services in general.

Example

Following command associates an HeNB-GW Network service named henb-network with specific HeNB-GW Access service.

associate henbgw-network-service henb-network
associate sctp-param-template

Associates a previously configured SCTP Parameter Template to the this HeNB-GW Access service. A SCTP Parameter Template must be configured globally before using this configuration.

Product
HeNB-GW

Privilege
Security Administrator, Administrator

Syntax

associate sctp-param-template template_name

no associate sctp-param-template

no

Removes the associated SCTP Parameter Template from this HeNB-GW Access service configuration.

template_name

Identifies the name of the pre-configured SCTP Parameter Template to associate with this HeNB-GW Access service.

模板_name is an alphanumeric string of 1 through 63 characters.

Usage

Use this command to bind/associate a pre-configured SCTP Parameter Template to the this HeNB-GW Access service. The SCTP Parameter Template can be configured global mode. The associate configuration is used to establish associations with other helper services in general.

Example

Following command associates an SCTP Parameter Template named sctp_tmpl with specific HeNB-GW Access service.

associate sctp-param-template sctp_tmpl
associate x2gw-service

This command Configures x2gw-service for this HENBGW ACCESS service.

Product
HeNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > HENBGW-ACCESS Service Configuration

configure > context context_name > hembgw-access-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-hembgw-access-service)#

Syntax

associate x2gw-service associate_x2gw-service_name context context_name

no associate x2gw-service

no
Removes the association of x2gw-service interface from this HeNB-GW Access service configuration.

associate_x2gw-service_name
Name of the service that will be used by this HENBGW ACCESS service to associate with. Name of the string is an alphanumeric, 1 through 63 characters.

context_name
Name of the context that will be used by this HENBGW ACCESS service to associate with. Name of the string is an alphanumeric, 1 through 79 characters.

Usage
Use this command to associate x2gw-service with HENBGW Access service.

Example

Following command associates an x2gw-service with specific HeNB-GW Access service with name gate123:

associate x2gw-service gate123
bind s1-mme

Binds the pre configured HeNB-GW Access Service to the IP address of the S1-MME interface.

**Product**
HeNB-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > HENBGW-ACCESS Service Configuration

```text
configure > context context_name > henbgw-access-service service_name
```

Entering the above command sequence results in the following prompt:

```text
[context_name]host_name(config-henbgw-access-service)#
```

**Syntax**

```text
bind s1-mme { ipv4-address | ipv6-address } ip_addr max-subscribers max_sub
no bind s1-mme
```

- **no**
  Removes the binding of S1-MME interface from this HeNB-GW Access service configuration.

- **ip_addr**
  Identifies the IP address of the S1-MME interface to associate with this HeNB-GW Access service. `addr_val` must be entered in the IPv4 (dotted decimal notation) or IPv6 (: / :: notation).

- **max-subscribers max_sub**
  Configures the maximum number of subscribers HENBGW ACCESS service can support. `max_sub` is an integer ranging from 0 through 4000000.

**Usage**

Use this command to bind the pre configured IPv4 address of the S1-MME interface to the HeNB-GW Access Service.

**Example**

Following command binds the S1-MME interface having 192.68.111.61 IP address with specific HeNB-GW Access service.

```text
bind s1-mme ipv4-address 192.68.111.61
```
csg-optimized-paging

Configures the support for Paging Optimization Function on this HeNB-GW Access service based on the CSG-ID in the Paging message.

Product
HeNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > HENBGW-ACCESS Service Configuration

cfg-configure > context context_name > hnbgw-access-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-hnbgw-access-service)#

Syntax

[ no ] csg-optimized-paging

no

Removes the paging optimization function from this HeNB-GW Access service configuration.

Usage

Use this command to enable the CSG-ID based paging optimization function to the HeNB-GW Access Service.

Example

Following command enables the CSG-ID based paging optimization on a specific HeNB-GW Access service.

csg-optimized-paging
**end**

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
exit

**Usage**
Use this command to return to the parent configuration mode.
**mme-id**

Configures the MME ID for this HeNB-GW Access service. For this configuration, MME Group ID and MME Code has to be configured.

**Product**
HeNB-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > HENBGW-ACCESS Service Configuration

configure > context context_name > henbgw-access-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-henbgw-access-service)#

**Syntax**

```
mme-id group-id mme_group_id mme-code mme_code

no mme-id
```

**no**
Removes the configured MME ID from this HeNB-GW Access service configuration.

```
mme_group_id
```

Identifies the MME Group ID which must be entered as an integer between 32768 and 65535.

```
mme_code
```

Identifies the MME code which is again an integer value between 0 and 255.

**Usage**

Use this command to configure the MME Identifier which includes the MME Group ID and MME Code for this HeNB-GW Access service. MME ID configuration is required, because it is the same ID which HeNB-GW sends in response messages to HeNBs.

⚠️ **Caution:** Changing the MME ID is a disruptive operation. HeNB-GW service is restarted on any change.

**Example**

Following command configures 32770 as the MME Group ID and 105 as MME code on a specific HeNB-GW Access service.

```
mme-id group-id 32770 mme-code 105
```
**plmn**

Configures the PLMN identifier for this HeNB-GW Access service. Other identifiers that are configured along with the PLMN include the MCC and MNC values too.

**Product**
HeNB-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > HENBGW-ACCESS Service Configuration

`configure > context context_name > hembgw-access-service service_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-hembgw-access-service)#
```

**Syntax**

```
[ no ]plmn id mcc mcc_val mnc mnc_val
```

- **no**
  Removes the existing PLMN configuration from this HeNB-GW Access service configuration.

- **mcc_val**
  Identifies the mobile country code for the IMSI which must be entered between 100 and 999 as a string of size 3.

- **mnc_val**
  Identifies the Mobile Network Code which is a value between 00 and 999, as a string of size 2 to 3.

**Usage**

Use this command to configure the PLMN related configuration for this HeNB-GW Access service.

**Example**

Following command configures 123 as the MCC value and 456 as the MNC value as part of the PLMN configuration for this HeNB-GW Access service.

```
plmn id mcc 123 mnc 456
```
s1-mme ip qos-dscp

This command configures the quality of service (QoS) differentiated service code point (DSCP) marking for IP packets sent out on the S1-MME interface, from the HeNB-GW to the HeNB(s).

Product
HeNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > HENBGW-ACCESS Service Configuration

configure > context context_name > henbgw-access-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-henbgw-access-service)#

Syntax

```plaintext
s1-mme ip qos-dscp { af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be | cs0 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef }

default s1-mme ip qos-dscp
```

```plaintext
qos-dscp { af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be | cs0 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef }

Default: af11

Specifies the DSCP for the specified QoS traffic pattern. qos-dscp can be configured to any one of the following:

af11: Assured Forwarding 11 per-hop-behavior (PHB)
af12: Assured Forwarding 12 PHB
af13: Assured Forwarding 13 PHB
af21: Assured Forwarding 21 PHB
af22: Assured Forwarding 22 PHB
af23: Assured Forwarding 23 PHB
af31: Assured Forwarding 31 PHB
af32: Assured Forwarding 32 PHB
af33: Assured Forwarding 33 PHB
af41: Assured Forwarding 41 PHB
af42: Assured Forwarding 42 PHB
af43: Assured Forwarding 43 PHB
be: Best effort forwarding PHB
```

```plaintext
cs0: Designates use of Class Selector 0 PHB. This is same as DSCP Value BE
cs1: Designates use of Class Selector 1 PHB
cs2: Designates use of Class Selector 2 PHB
cs3: Designates use of Class Selector 3 PHB
cs4: Designates use of Class Selector 4 PHB
cs5: Designates use of Class Selector 5 PHB
cs6: Designates use of Class Selector 6 PHB
cs7: Designates use of Class Selector 7 PHB
```
**Usage**

DSCP levels can be assigned to specific traffic patterns to ensure that data packets are delivered according to the precedence with which they are tagged. The diffserv markings are applied to the IP header of every subscriber data packet transmitted over the S1-MME interface(s).

**Example**

The following command sets the DSCP-level for data traffic sent over the S1-MME interface to `af12`:

```
s1-mme ip qos-dscp af12
```

**ef:** Expedited forwarding PHB
s1-mme sctp port

This command configures the local Stream Control Transmission Protocol (SCTP) port used for binding the SCTP socket to communicate with the HeNBs over S1-MME interface.

**Product**
HeNB-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > HENBGW-ACCESS Service Configuration

configure > context context_name > hembgw-access-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-hembgw-access-service)#

**Syntax**

```
s1-mme sctp port port_num

default s1-mme sctp port
```

**default**
Sets the SCTP port to the default value of 36412 to communicate with the HeNBs using S1-MME interface.

**port_num**
Specifies the SCTP port number to communicate with the HeNBs using S1-MME interface as an integer from 1 through 65535. Default: 36412

**Usage**

Use this command to assign the SCTP port with SCTP socket to communicate with the HeNB using S1AP. Only one SCTP port can be associated with one MME service.

**Example**

The following command sets the default SCTP port number 699 for to interact with Home eNodeB using S1AP on S1-MME interface:

```
default s1-mme sctp port
```
s1u-relay

This command configures the S1-U Relay service for the HeNB-GW Access service. The user enters in the S1-U Relay configuration mode using this command.

Product
HeNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > HENBGW-ACCESS Service Configuration
configure > context context_name > henbgw-access-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-henbgw-access-service)#

Syntax
[no] s1u-relay

no

Removes the S1-U Relay service function from this HeNB-GW Access service configuration.

Usage
Use this command to enable the S1-U Relay service function to the HeNB-GW Access Service. S1-U relay service is disabled by default.

Example
Following command enables the S-U Relay service on a specific HeNB-GW Access service.

s1u-relay
security-gateway

This command configuration defines the IPv4 address to be used as the connection point for establishing IKEv2 sessions and specify the crypto template to use for the security gateway (SeGW) for the HeNB-GW Access service.

**Product**
HeNB-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > HENBGW-ACCESS Service Configuration

```
configure > context context_name > hengw-access-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-hengw-access-service)#
```

**Syntax**

```
security gateway bind ipv4-address ip_addr crypto-template template_name [ context ctxt_name ]
```

```
no security gateway bind
```

<table>
<thead>
<tr>
<th><strong>no</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Removes the security gateway related configuration associated with this HeNB-GW Access service configuration.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>ip_addr</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Identifies the security gateway address used for this HeNB-GW Access service. It must be entered in dotted decimal notation.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>template_name</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Identifies the crypto template name for security gateway for this HeNB-GW Access service. It must be entered a string of size 0 to 127.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>ctxt_name</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Identifies the context name where crypto template is defined for this HeNB-GW Access service. It must be entered a string of size 1 to 79.</td>
</tr>
</tbody>
</table>

**Usage**

Use this command to configure the security gateway (SeGW) related configuration for this HeNB-GW Access service. SeGW configuration includes crypto template configuration as part of IPSec settings, therefore if the crypto-template is defined in a different context than the current HeNB-GW Access service, the context name has to be specified.

**Example**
Following command configures 192.68.111.15 as the SeGW address and crypto-temp as the crypto template name on a specific HeNB-GW Access service.

```
security gateway bind ipv4-address 192.68.111.15 crypto-template crypto-temp
```
timeout

Configures the the maximum duration of the session for this HeNB-GW Access service, in seconds, before system automatically reports/terminates the session.

Product
HeNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > HENBGW-ACCESS Service Configuration

command > context context_name> henbgw-access-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-henbgw-access-service)#

Syntax

timeout long-duration dur action { detection | disconnect }

no timeout long-duration

no

Removes the currently setup maximum duration of session.

dur

Specifies the number of seconds for the session’s timeout duration, before system automatically terminates the session or a defined action is to be taken.

dur is an integer from 1 through 2147483647. Default: 0

Usage

Use this command to configure the maximum duration of the session, in seconds, before system automatically reports/terminates the session of this HeNB-GW Access service.

Example

The following command sets the timeout duration of 60 seconds for a particular HeNB-GW Access service and disconnect the session:

    timeout long-duration 60 action disconnect
Chapter 159
HeNB-GW Network Service Configuration Mode Commands

A new service "henbgw-network-service" is defined under the Context configuration mode in order to support HeNB-GW functionality. This service configuration controls the S1-MME interface functionality between HeNB-GW and MME node.

Mode

Exec > Global Configuration > Context Configuration > HENBGW-NETWORK Service Configuration

configure > context context_name > henbgw-network-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-henbgw-network-service)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
**anr-info-retrieval**

This command enables the HeNB-GW to intercept and respond to the Automatic Neighbor Relation (ANR) related SON messages with the requested information.

**Product**
HeNB-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > HENBGW-NETWORK Service Configuration

```
configure > context context_name > henbgw-network-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name] host_name(config-henbgw-network-service)#
```

**Syntax**

```
[ no | default ] anr-info-retrieval
```

- **no**
  Removes the ANR information retrieval related function from this HeNB-GW Network service configuration.

- **default**
  Sets/Restores the default value assigned for the ANR information retrieval related function from the configured HeNB-GW Network service.

**Usage**

Use this command to enable the ANR information retrieval function to the HeNB-GW Network Service.

**Example**

Following command enables the ANR information retrieval function on a specific HeNB-GW Network service.

```
anr-info-retrieval
```
associate sctp-param-template

Associates a previously configured SCTP Parameter Template to the this HeNB-GW Network service. A SCTP Parameter Template must be configured globally before using this configuration.

Product
HeNB-GW

Privilege
Security Administrator, Administrator

Syntax

associate sctp-param-template template_name

no associate sctp-param-template

template_name

Identifies the name of the pre-configured SCTP Parameter Template to associate with this HeNB-GW Network service.

Usage
Use this command to bind/associate a pre-configured SCTP Parameter Template to the this HeNB-GW Network service. The SCTP Parameter Template can be configured global mode. The associate configuration is used to establish associations with other helper services in general.

Example
Following command associates an SCTP Parameter Template named sctp_tmpl with specific HeNB-GW Network service.

associate sctp-param-template sctp_tmpl
default-paging-drx

This command is used to configure the Default paging DRX value that is sent to the MME(s) in the S1 SETUP request message.

Product
HeNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > HENBGW-NETWORK Service Configuration

configure > context context_name > hengbw-network-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-henbgw-network-service) #

Syntax

default-paging-drx { v128 | v256 | v32 | v64 }

default default-paging-drx

default

Sets/Restores the default value assigned for Default-Paging-DRX for the configured HeNB-GW Network service.

Any one of the following DRX values can be configured:

- v128: Designates use of Paging DRX v128.
- v256: Designates use of Paging DRX v256.
- v32: Designates use of Paging DRX v32.
- v64: Designates use of Paging DRX v64.

Usage

Use this command to configure the Default Paging DRX value for this HeNB-GW Network service.

Example

Following command configures v256 as the Default Paging DRX value on a specific HeNB-GW Network service.

default-paging-drx v256
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > HENBGW-NETWORK Service Configuration

configure > context context_name > henbgw-network-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-henbgw-network-service)#

Syntax

dend

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > HENBGW-NETWORK Service Configuration

configure > context context_name > hnbgw-network-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-henbgw-network-service)#

Syntax

exit

Usage

Use this command to return to the parent configuration mode.
**logical-enb**

This command enables the configuration of one or more logical eNodeBs within the HeNB-GW.

**Product**
HeNB-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > HENBGW-NETWORK Service Configuration

```bash
configure > context context_name > henbgw-network-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-henbgw-network-service)#
```

**Syntax**

```bash
logical-enb global-enb-id plmn id mcc mcc_val mnc mnc_val { home-enb-id henb_id | macro-enb-id menb_id [ -noconfirm ] }

[ no ] logical-enb global-enb-id plmn id mcc mcc_val mnc mnc_val { home-enb-id henb_id | macro-enb-id menb_id }
```

---

**no**
Removes the configured logical eNodeB from this HeNB-GW Network service configuration.

**mcc mcc_val**
Identifies the mobile country code for the IMSI which must be entered between 100 and 999, as a string of size 3.

**mnc mnc_val**
Identifies the Mobile Network Code which is a value between 00 and 999, as a string of size 2 to 3.

**home-enb-id henb_id**
Identifies the Home eNodeB ID which is an integer from 1 to 268435455.

**macro-enb-id menb_id**
Identifies the Macro eNodeB ID which is again an integer value between 1 and 1048575.

**-noconfirm**
Creates a new HeNB-GW network service without prompting for confirmation.
Usage

Use this command for the configuration of one or more logical eNodeBs within the HeNB-GW. The Logical eNodeB configuration can be used to support load balancing within a pool of TAIs (i.e. Multiple logical eNodeBs can service calls connecting from a specific set of TAIs). It can also be used to create and support disjoint serving areas, that is each logical eNodeB will serve a different set of TAIs.

At least one logical eNodeB configuration is required to START an HeNB-GW Network service.

⚠️ Caution: Deleting or modifying any of the parameters for a fully configured logical eNodeB is a disruptive operation. It will result in the termination of SCTP connections to MMEs from that logical eNodeb.

Example

Following command configures a logical eNodeB having Home eNodeB ID as 1000 on a specific HeNB-GW Network service.

```bash
logical-enb global-enb-id plmn id mcc 123 mnc 456 home-enb-id 1000
```
paging-rate-control

This command is used to configure the Paging-Rate-Control which determines the maximum number of paging messages per second which an HeNB-GW can handle received from the MME(s).

Product
HeNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > HENBGW-NETWORK Service Configuration

configure > context context_name > henbgw-network-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-henbgw-network-service)#

Syntax

paging-rate-control number_of_msg

no paging-rate-control

no

Removes the configured rate of paging messages from this HeNB-GW Network service configuration.

number_of_msg

Identifies the number of paging messages to be handled by the HeNBGW service per second. This number must be entered as an integer between 1 and 65535 (min 1 and max 65535).

Usage

Use this command to configure the number of paging messages per second to be handled by this HeNB-GW Network service. MME ID configuration is required, because it is the same ID which HeNB-GW sends in response messages to HeNBs.

This parameter is not part of logical-enb configuration and therefore it would include paging messages received from all the MMEs to which this HeNB-GW is connected on the network side.

Important: Paging messages exceeding the configured rate are dropped. Total Paging and Dropped Statistics is updated in the logs.

Example

Following command configures 32770 as the number of paging messages per second to be handled on a specific HeNB-GW Network service.

    paging-rate-control 32770
**pws**

This command sets values for parameters related to public warning system feature.

**Product**
HeNB-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > HENBGW-NETWORK Service Configuration

```
configure > context context_name > henbgw-network-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-henbgw-network-service)#
```

**Syntax**

```
pws { kill-request-timeout kill_req_timeout_seconds | restart-indication-timeout restart_ind_timeout_seconds | warning-request-timeout warn_req_timeout_seconds }

default pws { kill-request-timeout | restart-indication-timeout | warning-request-timeout }
```

**Usage**

Use this command to set the values for parameters related to public warning system feature for this HeNB-GW Network service.

**Example**

Following command configures the Warning request timeout value to 100 seconds.

```
pws warning-request-timeout 100
```
s1ap-max-retransmissions

This command configures the number of times node level S1AP message is retransmitted towards MME.

**Product**

HeNB-GW

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > HENBGW-NETWORK Service Configuration

```plaintext
configure > context context_name > henbgw-network-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-henbgw-network-service)#
```

**Syntax**

```plaintext
s1ap-max-retransmissions number_of_retries

default s1ap-max-retransmissions
```

**default**

Configures the default number of S1AP retransmissions for this HeNB-GW Network service configuration. Default number of retransmissions is 4.

**number_of_retries**

Identifies the number of S1AP retransmissions to be configured. This number must be entered as an integer between 1 and 5.

**Usage**

Use this command to configure the maximum number of Node level S1AP retransmissions for this HeNB-GW Network service.

⚠️ **Caution:** Configuring s1ap-max-retransmissions to 0 will disable the S1AP retransmission support.

**Example**

Following command configures default (which is also 4) S1AP retransmission on a specific HeNB-GW Network service.

```plaintext
default s1ap-max-retransmissions
```
s1ap-retransmission-timeout

This command configures the timeout interval to support Node Level S1AP retransmissions if there is no response received from the peer (MME).

Product
HeNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > HENBGW-NETWORK Service Configuration

configure > context context_name > hbgw-network-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-hbgw-network-service)#

Syntax

s1ap-retransmission-timeout number_of_secs

default s1ap-retransmission-timeout

default

Configures the default S1AP retransmission timeout for this HeNB-GW Network service configuration.
Default retransmission timeout is 60 seconds.

number_of_secs

Identifies the number seconds as the S1AP retransmission timeout to be configured. This number must be entered as an integer between 1 and 600.

Usage
Use this command to configure the timeout interval to support Node Level S1AP retransmissions for this HeNB-GW Network service.

Example
Following command configures 100 as the S1AP retransmission timeout on a specific HeNB-GW Network service.

s1ap-retransmission-timeout 100
Chapter 160
HSGW Service Configuration Mode Commands

The HSGW Service Configuration Mode is used to create and manage a configuration allowing the HRPD Serving Gateway (HSGW) to communicate, send and receive call data, and session flows to/from a evolved Access Network/evolved Packet Control Function (eAN/ePCF) in an eHRPD network.

**Mode**

Exec > Global Configuration > Context Configuration > HSGW Service Configuration

`configure > context context_name > hsgw-service service_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-hsgw-service)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
a11-signalling-packets

Enables the DSCP marking feature for IP headers carrying outgoing A11-signalling A11 packets (such as RRP, RU, SU).

**Product**
HSGW

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > HSGW Service Configuration

```
configure > context context_name > hsgw-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-hsgw-service)#
```

**Syntax**

```
a11-signalling-packets ip-header-dscp value

[ default | no ] all-signalling-packets ip-header-dscp
```

**Usage**

Use this command to enable or disable the DSCP marking feature for IP headers carrying outgoing A11-signalling A11 packets. DSCP marking is disabled by default.

**Example**

The following command configures the HSGW service to support DSCP marking for IP headers on A11 packets in outgoing A11-signalling traffic:

```
a11-signalling-packets ip-header-dscp 0x21
```
associate

Associates accounting policies and QCI-QoS mapping parameters with this HSGW service.

Product
HSGW

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > HSGW Service Configuration

configure > context context_name > hsgw-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-hsgw-service)#

Syntax

associate { accounting-policy name | qci-qos-mapping name }

no associate { accounting-policy [ name ] | qci-qos-mapping }

no

Removes the specified associated policy or mapping from the service.

accounting-policy name

Specifies an existing accounting policy to associate with the HSGW service as an alphanumeric string of 1 through 63 characters.

qci-qos-mapping name

Specifies an existing QCI-QoS mapping configuration as an alphanumeric string of 1 through 63 characters. QCI-QoS mapping is configured through the qci-qos-mapping command in the Global Configuration Mode.

Usage

Use this command to associate an accounting policy with the HSGW service.

Example

The following command associates an accounting policy named acct2 to the HSGW service:

associate accounting-policy acct2
bind address

Binds the service to a logical IP interface serving as the A10 interface and specifies the maximum number of subscribers that can access this service over the configured interface.

Product
HSGW

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > HSGW Service Configuration

configure > context context_name > hsgw-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-hsgw-service)#

Syntax

bind address ip_address [ max-subscribers num ]

no bind address

no

Removes the interface binding from this service.

address ip_address

Specifies the IP address of the A10/A11 interface in IPv4 dotted-decimal notation.

max-subscribers num

Specifies the maximum number of subscribers that can access this service on this interface as an integer from 0 through 2500000. Default: 2500000

Important: The maximum number of subscribers supported is dependant on the license key installed and the number of active PSCs in the system. A fully loaded system with 13 active PSCs can support 3,000,000 total subscribers. Refer to the license key command and the Usage section (below) for additional information.

Usage

Associate the HSGW service to a specific logical IP address. The logical IP address or interface takes on the characteristics of an A10/A11 interface that provides the session connectivity to/from an eAN/PCF. Only one interface can be bound to a service. The interface should be configured prior to issuing this command.

This command also sets a limit as to the number of simultaneous subscribers sessions that can be facilitated by the service/interface at any given time.

When configuring the max-subscribers option, be sure to consider the following:

- The total number of A10/A11 interfaces you will configure
- The total number of subscriber sessions that all of the configured interfaces may handle during peak busy hours
• An average bandwidth per session multiplied by the total number of sessions
• The type of physical port (10/100Base-T or 1000Base-Tx) that these interfaces will be bound to

Taking these factors into account and distributing your subscriber session across all available interfaces will allow you to configure your interfaces to optimally handle sessions without degraded performance.

**Example**

The following command would bind the logical IP interface with the address of 112.334.556.778 to the HSGW service and specifies that a maximum of 200,000 simultaneous subscriber sessions can be facilitated by the interface/service at any given time:

```
bind address 112.334.556.778 max-subscribers 200000
```
**context-retention-timer**

Configures the maximum number of consecutive seconds that a UE session context (which includes the LCP, authentication and A10 session context for a given UE) is maintained by the HSGW before it is torn down.

**Product**
HSGW

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > HSGW Service Configuration

`configure > context context_name > hsgw-service service_name`

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-hsgw-service)#`

**Syntax**

```
context-retention-timer timeout [ sec ]
[ default | no ] context-retention-timer timeout
```

- **default**
  Disables the timer.

- **no**
  Disables the timer.

- **timeout [ sec ]**
  Specifies the amount of time (in seconds) that the session context is maintained before it is disassembled as an integer from 1 through 3600. Default: 60.
  In Release 15.0 and later, the maximum value has been increased to 86400 seconds (24 hours).

**Usage**
Use this command to configure a timer to retain session contexts for a specified amount of time before disassembling it.

**Example**
The following command allows the HSGW to maintain session contexts for 120 seconds before tearing them down:

```
context-retention-timer timeout 120
```
data-available-indicator

Enables sending the Data Available Indicator extension in A10/A11 Registration Reply messages.

**Product**
HSGW

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > HSGW Service Configuration

`configure > context context_name > hsgw-service service_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-hsgw-service)#
```

**Syntax**

```
data-available-indicator
```

**Usage**

Use this command to enable the sending of the Data Available Indicator extension in A10/A11 Registration Reply messages.
data-over-signaling

Enables the data-over-signaling marking feature for A10 packets.

**Product**
HSGW

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > HSGW Service Configuration

```
configure > context context_name > hsgw-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-hsgw-service)#
```

**Syntax**

```
[ default | no ] data-over-signaling
```

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Enables the data-over signaling feature for A10 packets.</td>
</tr>
<tr>
<td>no</td>
<td>Disables the data-over signaling feature for A10 packets.</td>
</tr>
</tbody>
</table>

**Usage**

Use this command to enable or disable the data-over signaling feature for A10 packets.
**dns-pgw**

Identifies the location of the DNS client to the HSGW service and enables/disables P-GW load balancing using DNS SRV lookup.

**Product**

HSGW

**Privilege**

Administrator

**Mode**

Exec > Global Configuration > Context Configuration > HSGW Service Configuration

`configure > context context_name > hsgw-service service_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-hsgw-service)#
```

**Syntax**

```
| dns-pgw { context name | selection { topology [ weight ] | weight } } |
|----------------------|---------------------------------------------|
| [ default | no ] dns-pgw { context | selection { topology [ weight ] | weight } } |
```

---

**default**

Returns the command to its default setting of the current context.

By default, topology will be enabled and weight will be disabled.

---

**no**

Removes the configured DNS client context name or P-GW DNS selection criteria from this service.

---

**context name**

Specifies an existing context in which the DNS client is configured as an alphanumeric string of 1 through 79 characters.

---

**selection { topology [ weight ] | weight }**

Specifies P-GW DNS selection criteria.

**topology**: Enables topology selection, which selects a P-GW topologically closer to the HSGW.

**topology weight**: Enables topology selection with weight.

**weight**: Enables selection with weight only when both preference values are the same; disables topology selection.

---

**Usage**

Use this command to identify to the HSGW service the context where the DNS client is configured. The DNS client is used to identify an FQDN for the peer P-GW. This command defaults to the same context as the HSGW service.

In addition, this command enables and disables P-GW load balancing using DNS SRV lookup by defining P-GW DNS selection criteria.
Example

The following command identifies the context where the DNS client is configured as `isp3`:

```
dns-pgw context isp3
```

The following command enables P-GW DNS topology selection with weight:

```
dns-pgw selection topology weight
```
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Use this command to return to the parent configuration mode.
**fqdn**

Configures the Fully Qualified Domain Name (FQDN) for this HSGW service.

**Product**
HSGW

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > HSGW Service Configuration

```
configure > context context_name > hsgw-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-hsgw-service)#
```

**Syntax**

```
fqdn  domain_name
```

- **default**
  
  Returns the command to the default setting of “null”.

- **no**
  
  Removes the configured FQDN name from this service.

- **domain_name**
  
  Specifies an FQDN for the HSGW service as an alphanumeric string of 1 through 256 characters.

⚠️ **Important:** In order to properly interact with other nodes in the network, the FQDN should be 96 alpha and/or numeric characters or less.

**Usage**

Use this command to configure an FQDN for this HSGW service. The FQDN is used when matching a P-GW with an HSGW.

**Topology Matching**

You may specify which P-GW you wish an HSGW interface to connect with by enabling topology matching within the FQDNs for both the HSGW service and P-GW service. Topology matching selects geographically closer nodes and reduces backhaul traffic for a specified interface.

The following optional keywords enable or disable topology matching when added to the beginning of an FQDN:

- `topon.<interface_name>`.
Beginning an FQDN with `topon` initiates topology matching with available P-GWs in the network. Once this feature is enabled, the rest of the FQDN is processed from right to left until a matching regional designator is found on a corresponding P-GW FQDN.

*topoff.<interface_name>.*

By default, topology matching is disabled. If you enable topology matching for any interfaces within a node, however, all interfaces not using this feature should be designated with `topoff`.

**Example**

The following command configures this HSGW service with an FQDN of `abc123.com`:

```
fqdn abc123.com
```

The following command configures this HSGW service with an FQDN that enables topology matching:

```
fqdn topon.<interface_name>.hsgw01.bos.ma.node.epc.mnc<value>.
mcc<value>.3gppnetwork.org
```

**Important:** The associated P-GW service must have a corresponding FQDN similar to the following:

```
topon.<interface_name>.pgw01.bos.ma.node.epc.mnc<value>.mcc<value>.3gppnetwork.org
```
fragment

Enables or disables Point-to-Point Protocol (PPP) payload fragmentation.

**Product**
HSGW

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > HSGW Service Configuration

```bash
configure > context context_name > hsgw-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-hsgw-service)#
```

**Syntax**

```
[ default | no ] fragment ppp-data
```

---

**default**

Returns the command to its default setting of enabled.

---

**no**

Disables PPP payload fragmentation.

**Usage**

Use this command to enable or disable PPP payload fragmentation.
**gre**

Configures Generic Routing Encapsulation (GRE) parameters for the A10 protocol within the HSGW service.

**Product**

HSGW

**Privilege**

Administrator

**Mode**

Exec > Global Configuration > Context Configuration > HSGW Service Configuration

```
configure > context context_name > hsgw-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-hsgw-service)#
```

**Syntax**

```
gre { checksum | checksum-verify | flow control [ action { disconnect-session | resume-session } ] [ timeout msecs ] + | ip-header-dscp value { all-control-packets | setup-packets-only } | reorder-timeout msecs | segmentation | sequence-mode { none | reorder } | sequence-numbers | threegpp2-ext-headers qos-marking }

default gre { checksum | checksum-verify | flow-control | ip-header-dscp | reorder-timeout | sequence-mode | sequence-numbers | threegpp2-ext-headers qos-marking }

no gre { checksum | checksum-verify | flow-control | ip-header-dscp | segmentation | sequence-numbers | threegpp2-ext-headers qos-marking }
```

**default**

Restores the specified parameter to its default setting.

**no**

Disables the specified functionality.

**checksum**

Enables the introduction of the checksum field in outgoing GRE packets. Default: disabled

**checksum-verify**

Enables verification of the GRE checksum (if present) in incoming GRE packets. Default: disabled

**flow-control [ action { disconnect-session | resume-session } ] [ timeout msecs ] +**

Default: no GRE flow-control

Enables 3GPP2 GRE flow control which causes the HSGW to send flow control enabled Normal Vendor Specific Extensions (NVSE) in A11 RRPs.

```
action { disconnect-session | resume-session }
```

Default: disconnect-session
Specifies the action to be taken when timeout is reached:

- **disconnect-session**: Ends the session and releases the call.
- **resume-session**: Switches flow control to XON and resumes delivery of packets to the RAN.

### `timeout msecs`

Specifies the amount of time (in milliseconds) to wait for an XON indicator from the RAN (after receiving an XOFF). Also sets the action to be taken if the timeout limit is reached.

- **msecs**: an integer from 1 through 1000000. Default: 1000

### `ip-header-dscp value { all-control-packets | setup-packets-only }`

Default: Disabled

Configures QoS Differentiated Services Code Point (DSCP) marking for GRE packets.

- **value**: Represents the DSCP setting as the first six most-significant bits of the ToS field. It can be configured to any hexadecimal value from 0x0 through 0x3F.

- **all-control-packets**: Dictates that the DSCP marking is to be provided in all GRE control packets.
- **setup-packets-only**: Dictates that the DSCP marking is to be provided only in GRE setup packets.

### `reorder-timeout msecs`

Configures the maximum number of milliseconds to wait before processing reordered out-of-sequence GRE packets as an integer from 0 through 5000. Default: 100

### `segmentation`

Enables GRE Segmentation for the HSGW service. Default: disabled

### `sequence-mode { none | reorder }

Default: none

Configures handling of incoming out-of-sequence GRE packets.

- **none**: Specifies that sequence numbers in packets are ignored and all arriving packets are processed in the order they arrive.
- **reorder**: Specifies that out of sequence packets are stored in a sequencing queue until one of the conditions is met:
  
  - The reorder timeout occurs: All queued packets are sent for processing and the accepted sequence number is updated to the highest number in the queue.
  - The queue is full (five packets): All packets in the queue are sent for processing, the reorder timer is stopped and the accepted sequence number is updated to the highest number in the queue.
  - An arriving packet has a sequence number such that the difference between this and the packet at the head of the queue is greater than five. All the packets in the queue are sent for processing, the reorder timer is stopped and the accepted sequence number is updated to the highest number that arrived.
  - A packet arrives that fills a gap in the sequenced numbers stored in the queue and creates a subset of packets whose sequence numbers are continuous with the current accepted sequence number. This subset of packets in the queue is sent for processing. The reorder timer continues to run and the accepted sequence number is updated to the highest number in the subset delivered.

### `sequence-numbers`

Enables insertion of GRE sequence numbers in data that is about to be transmitted over the A10 interface. Data coming into the system containing sequence numbers but that is out of sequence is not re-sequenced.
threegpp2-ext-headers qos-marking

When threegpp2-ext-headers qos-marking is enabled and the PCF negotiates capability in the A11 RRQ, the HSGW will include the QoS optional data attribute in the GRE 3gpp2 extension header.

The no keyword, enables qos-marking in the GRE header based on the tos value in the header.

Usage

Use this command to set GRE parameters for the A10 protocol within the HSGW service.

Example

The following command configures the HSGW service to support the inclusion of GRE sequence numbers in outgoing traffic:

```
   gre sequence-numbers
```
Enables the use of Robust Header Compression (RoHC) and enters the HSGW Service ROHC Configuration Mode where RoHC parameters are configured for the service.

Configures the local User Datagram Protocol (UDP) port for the A10/A11 interface IP socket.

Sets the parameters for IP source validation. Source validation is useful if packet spoofing is suspected or for verifying packet routing and labeling within the network. Source validation requires the source address of received packets to match the IP address assigned to the subscriber (either statically or dynamically) during the session.

Product
HSGW

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > HSGW Service Configuration
configure > context context_name > hsgw-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-hsgw-service)#

Syntax

```
ip { header-compression rohc | local-port number | source-violation { clear-on-valid-packet | drop-limit num | period secs | reneg-limit num } }
default ip { header-compression rohc | local-port | source-violation { drop-limit | period | reneg-limit } }
no ip { header-compression rohc | source-violation clear-on-valid-packet }
```

**default**

Resets the keyword to its default value.

**no**

**header-compression rohc**: Removes the RoHC configuration from this service.

**ip source-violation clear-on-valid-packet**: Disables the ability of the service to reset the reneg-limit and drop-limit counters after receipt of a properly addressed packet.

**header-compression rohc**

Specifies that Robust Header Compression will be applied to sessions using this service and enters the HSGW Service RoHC Configuration Mode where RoHC parameters are configured.

**local-port number**

Specifies the UDP port number as an integer from 1 through 65535. Default: 699
source-violation { clear-on-valid-packet | drop-limit num | period secs | reneg-limit num }

clear-on-valid-packet
Configures the service to reset the reneg-limit and drop-limit counters after receipt of a properly addressed packet. Default: disabled
drop-limit num
Specifies the number of allowed source violations within a detection period before forcing a call disconnect as an integer from 1 through 1000000. If num is not specified, the value is set to the default. Default: 10
period secs
Specifies the length of time (in seconds) for a source violation detection period to last; drop-limit and reneg-limit counters are decremented each time this value is reached.
The counters are decremented in this manner: reneg-limit counter is reduced by one (1) each time the period value is reached until the counter is zero (0); drop-limit counter is halved each time the period value is reached until the counter is zero (0). If secs is not specified, the value is set to the default.
secs is an integer from 1 through 1000000. Default: 120
reneg-limit num
Sets the number of allowed source violations within a detection period before forcing a PPP renegotiation. If num is not specified, the value is set to the default.
num is an integer from 1 through 1000000. Default: 5

Usage

Header Compression RoHC: Use this command to specify that sessions using this service will have Robust Header Compression applied and configure parameters supporting RoHC.
Entering this command results in the following prompt:

    [context_name]hostname(config-ip-header-compression-rohc)#

HSGW Service RoHC Configuration Mode commands are defined in the HSGW Service RoHC Configuration Mode Commands chapter.
Local Port: Specify the UDP port that should be used for communications between the Packet Control Function (PCF) and the HSGW.

Important: The UDP port setting on the PCF must match the local-port setting for the HSGW service on the system in order for the two devices to communicate.

Source Violation: This function is intended to allow the operator to configure a network to prevent problems such as when a user gets handed back and forth between two HSGWs a number of times during a handoff scenario.
This function operates in the following manner:
When a subscriber packet is received with a source address violation, the system increments both the IP source-violation reneg-limit and drop-limit counters and starts the timer for the IP-source violation period.
Every subsequent packet received with a bad source address during the IP-source violation period causes the reneg-limit and drop-limit counters to increment.
For example, if reneg-limit is set to 5, then the system allows 5 packets with a bad source address (source violations), but on the 5th packet, it re-negotiates PPP.
If the drop-limit is set to 10, the above process of receiving 5 source violations and renegotiating PPP occurs only once. After the second 5 source violations, the call is dropped. The period timer continues to count throughout this process.
If the configured source-violation period is exceeded at any time before the call is dropped, the reneg-limit counter is checked. If the reneg-limit counter is greater than zero (0), the reneg-limit is decremented by 1. If the reneg-limit counter equals zero, the drop-limit is decremented by half.

**Example**

The following command specifies a UDP port of 3950 for the HSGW service to use to communicate with the PCF on the A10/A11 interface:

```
ip local-port 3950
```

The following command sets the drop limit to 15 and leaves the other values at their defaults:

```
ip source-violation drop-limit 15
```
**lifetime**

Specifies how long an A10 connection can exist before its registration is considered expired.

**Product**
HSGW

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > HSGW Service Configuration

    configure > context context_name > hsgw-service service_name

Entering the above command sequence results in the following prompt:

    [context_name]host_name(config-hsgw-service)#

**Syntax**

    lifetime time

    [ default | no ] lifetime

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Resets the lifetime value to the default setting of 1800 seconds.</td>
</tr>
<tr>
<td>no</td>
<td>Specifies that an A10 connection can exist for an infinite amount of time.</td>
</tr>
<tr>
<td>time</td>
<td>Specifies the time (in seconds) that an A10 connection can exist before its registration is considered expired as an integer from 1 through 65534. Default: 1800</td>
</tr>
</tbody>
</table>

**Usage**

Use this command to set a limit to the amount of time that a subscriber session can remain up whether or not the session is active or dormant. If the lifetime timer expires before the subscriber terminates the session, the connection is terminated automatically.

**Example**

The following command specifies a time of **3600** seconds (1 hour) for subscriber sessions on this HSGW service:

    lifetime 3600
max-retransmissions

Configures the maximum number of times the HSGW service will attempt to communicate with an eAN/PCF before it marks it as unreachable.

Product
HSGW

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > HSGW Service Configuration

configure > context context_name > hsgw-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-hsgw-service)#

Syntax

max-retransmissions count

default max-retransmissions

---

default

Resets the maximum number of allowed retransmissions to the default value of 5.

---

count

Specifies the maximum number of times the HSGW service will attempt to communicate with an eAN/PCF before it marks it as unreachable.

count is an integer from 1 through 1000000. Default: 5

---

Usage

Use this command to limit the number of retransmissions to an eAN/PCF before marking it as unreachable. If the value configured is reached, the call is dropped.

Example

The following command configures the maximum number of retransmissions for the HSGW service to 3:

max-retransmissions 3
**mobile-access-gateway**

Identifies the mobile access gateway (MAG) context through which MIPv6 calls are to be routed.

**Product**
HSGW

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > HSGW Service Configuration

```bash
configure > context context_name > hsgw-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-hsgw-service)#
```

**Syntax**

```
mobile-access-gateway context context_name [ mag-service service_name ]
```

```
no mobile-access-gateway context
```

- **no**
  - Removes the configured MAG context route from this service.

```
context context_name [ mag-service service_name ]
```

- **context**
  - Specifies the name of the context and, optionally, the service through which MIPv6 sessions are to be routed.
  - `context_name` is an existing context expressed as an alphanumeric string of 1 through 79 characters.
  - `service_name` is an existing MAG service expressed as an alphanumeric string of 1 through 63 characters.

**Usage**

Use this command to specify where MIPv6 sessions are routed through this service.

**Example**

The following command identifies the MAG context `MAG1` as the context through which MIPv6 sessions are to be routed and further narrows the route by specifying the service name (`mag_serv3`):

```
mobile-access-gateway context MAG1 mag-service mag_serv3
```
network-initiated-qos

Enables the use of network initiated QoS functionality.

Product
HSGW

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > HSGW Service Configuration

configure > context context_name > hsgw-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-hsgw-service)#

Syntax

[ default | no ] network-initiated-qos

default

Returns the command to its default setting of enabled.

no

Disables the ability to use network initiated QoS functionality.

Usage

Use this command to enable or disable support for network initiated QoS functionality. Network initiated QoS is enabled by default.

When network initiated QoS functionality is enabled, if the vendor specific network control protocol (VSNCP) protocol configuration options (PCO) arrive from the UE with the BCM set, the HSGW CCR-I includes the Network-Request-Support AVP. If the PCRF behavior returns a BCM of MS+NW when this AVP is received, then flows originating from the network (RSVP Resv) would be triggered upon a PCC-Rule install.
plmn id

Configures Public Land Mobile Network identifiers used to determine if a mobile station is visiting, roaming or belongs to this network.

Product
HSGW

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > HSGW Service Configuration

configure > context context_name > hsgw-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-hsgw-service)#

Syntax

plmn id mcc number mnc number

mcc number mnc number

mcc number: Specifies the mobile country code (MCC) portion of the PLMN identifier as an integer from 100 through 999.

mnc number: Specifies the mobile network code (MNC) portion of the PLMN identifier as a 2- or 3-digit integer from 00 through 999.

Usage
The PLMN identifier is used to aid the HSGW service in the determination of whether or not a mobile station is visiting, roaming, or home. Multiple P-GW services can be configured with the same PLMN identifier. Up to five PLMN IDs can be configured for each P-GW Service. The configured IDs are used in Diameter-EAP-Request messages (as a Visited-Network-Identifier AVP).

Example
The following command configures the PLMN identifier with an MCC of 462 and MNC of 2:

plmn id mcc 462 mnc 02
policy overload

Specifies how an HSGW service should handle overload conditions.

Product
HSGW

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > HSGW Service Configuration
configure > context context_name > hsgw-service service_name

Entering the above command sequence results in the following prompt:
[context_name]host_name(config-hsgw-service)#

Syntax

policy overload { redirect address [ weight weight_num ] [ address2 [ weight weight_num ] ... address16 [ weight weight_num ] ] | reject [ use reject-code { admin-prohibite | insufficient-resources } ] } } 

default policy overload

no policy overload [ redirect address [ address2 ] ... [ address16 ] ]

default
Returns the command to its default setting of “reject” with the “admin-prohibited” code.

no
Removes a specified “redirect address” from this service.

redirect address [ weight weight_num ] [ address2 [ weight weight_num ] ... address16 [ weight weight_num ] ]

This option enables a redirect policy for overloaded conditions. When a redirect policy is invoked, the HSGW service rejects new sessions with an A11 Registration Reply Code of 88H (unknown HSGW address) and provides the IP address of an alternate HSGW. This command can be issued multiple times.

address: The IP address of an alternate HSGW expressed in IPv4 dotted decimal notation. Up to 16 IP addresses can be specified either in one command or by issuing the redirect command multiple times. If you try to add more than 16 IP addresses to the redirect policy the CLI issues an error message. If you specify an IP address and weight that already exists in the redirect policy the new values override the existing values.

weight weight_num: When multiple addresses are specified, they are selected in a weighted round-robin scheme. Entries with higher weights are more likely to be chosen. If a weight is not specified, the entry is automatically assigned a weight of 1 (default). weight_num must be an integer value from 1 through 10.

reject [ use reject-code { admin-prohibite | insufficient-resources } ]

This option will cause any overload traffic to be rejected. The HSGW sends an A11 Registration Reply Code of 82H (insufficient resources).
use-reject-code admin-prohibited: When this keyword is specified and traffic is rejected, the error code admin prohibited is returned instead of the error code “insufficient resources”. This is the default behavior.

use-reject-code insufficient-resources: When this keyword is specified and traffic is rejected, the error code “insufficient resources” is returned instead of the error code admin prohibited.

Usage

Policies can be implemented to dictate HSGW service behavior for overload conditions. The system invokes the overload policy if the number of calls currently being processed exceeds the licensed limit for the maximum number of sessions supported by the system. The system automatically invokes the overload policy when an on-line software upgrade is started. Use the no policy overload command to delete a previously configured policy. If after deleting the policy setting you desire to return the policy parameter to its default setting, use the default policy command.

The chassis is shipped from the factory with the policy options overload disabled.

Example

The following command configures the HSGW service to redirect overload traffic to two IPv4 addresses, one priority weighted 1 and the other priority weighted 5:

```
policy overload redirect 10.2.3.4 weight 1 10.2.3.5 weight 5
```
profile-id-qci-mapping

Associates a configured mapping table for RP QoS Profile ID to LTE QoS Class Index (QCI) mapping with this service.

**Product**
HSGW

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > HSGW Service Configuration

```text
configure > context context_name > hsgw-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-hsgw-service) #
```

**Syntax**

```
profile-id-qci-mapping name

no profile-id-qci-mapping [ name ]
```

- **no**
  Removes all profile maps or a specific profile map from this service.

- **name**
  Specifies the name of an existing Profile ID - QCI Mapping table to be associated with this service as an alphanumeric string of 1 through 63 characters.

**Usage**

Use this command to associate the HSGW service with a configured Profile ID - QCI Mapping table. The table is configured in the Global Configuration Mode using the `profile-id-qci-mapping-table` command.

**Example**

The following command associates a Profile ID - QCI Mapping table named `table3` with this service:

```
profile-id-qci-mapping table3
```
registration-deny

Configures parameters related to registration rejection.

Product
HSGW

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > HSGW Service Configuration

configure > context context_name > hsgw-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-hsgw-service)#

Syntax

registration-deny { handoff connection-setup-record-absent | newcall connection-setup-record-absent } [ use-deny-code { poorly-formed-request | reason-unspecified } ]

[ default | no ] registration-deny { handoff connection-setup-record-absent | newcall connection-setup-record-absent }

default | no
Returns the command to its default settings.

handoff connection-setup-record-absent
When enabled, the HSGW denies or discards handoff R-P sessions that do not have an Airlink Connection Setup record in the A11 Registration Request. Default is disabled. Default HSGW behavior is to accept such requests.

newcall connection-setup-record-absent
When enabled, the HSGW denies or discards new R-P sessions that do not have the Airlink Connection Setup record in the A11 Registration Request. Default is disabled. Default HSGW behavior is to accept such requests.

use-deny-code { poorly-formed-request | reason-unspecified }
Sets the specified Registration Deny Code when denying a new call or handoff because of a missing connection setup record.

Usage
Use this command to configure parameters relating to the rejection of registration requests.

Example

The following command denies registration for registration requests missing the connection setup record and replies with a use deny code of “poorly formed request”: 
registration-deny handoff connection-setup-record-absent use-deny-code poorly-formed-request
retransmission-timeout

Configures the maximum allowable time for the HSGW service to wait for a response from the eAN/PCF before it attempts to communicate with the eAN/PCF again (if the system is configured to retry the PCF), or marks the eAN/PCF as unreachable.

Product
HSGW

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > HSGW Service Configuration

configure > context context_name > hsgw-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-hsgw-service)#

Syntax

retransmission-timeout time

[ default | no ] retransmission-timeout

default
Resets the timeout setting to the default value of 3.

no
Deletes a previously configured timeout value.

time
Specifies the maximum allowable time (in seconds) for the HSGW service to wait for a response from the eAN/PCF before it: a) attempts to communicate with the eAN/PCF again (if the system is configured to retry the PCF), or b) marks the eAN/PCF as unreachable.

time is an integer from 1 through 1000000. Default: 3

Usage
Use the retransmission timeout command in conjunction with the max-retransmissions command in order to configure the HSGW service’s behavior when it does not receive a response from a particular PCF.

Example
The following command configures a retransmission timeout value of 5 seconds:

retransmission-timeout 5
rsvp

Configures resource reservation protocol (RSVP) parameters for this HSGW service in support of the network initiated QoS feature.

Product
HSGW

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > HSGW Service Configuration
configure > context context_name > hsgw-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-hsgw-service)#

Syntax

rsvp { max-retransmissions count | retransmission-timeout seconds }

[ default | no ] rsvp { max-retransmissions | retransmission-timeout }

---

default
Reset the maximum number of allowed retransmissions to the default value of 5 or the timeout setting to the default value of 3.

no
Disables the feature.

max-retransmissions count
Specifies the maximum retransmission count of RP control packets as an integer from 1 through 1000000. Default: 5

retransmission-timeout seconds
Specifies the maximum amount of time (in seconds) to allow for retransmission of RP control packets as an integer from 1 through 1000000. Default: 3

Usage
Use this command to set RSVP parameters for this HSGW service in support of the network initiated QoS feature.

Example
The following command configures the maximum number of retransmissions to 3:

```
rsvp max-retransmissions 3
```
setup-timeout

Specifies the maximum amount of time allowed for session setup.

Product
HSGW

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > HSGW Service Configuration
configure > context context_name > hsgw-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-hsgw-service)#

Syntax

setup-timeout seconds

[ default| no ] setup-timeout

default
 Resets the command to the default value of enabled with a timeout of 60 seconds.

no
 Disables the feature.

seconds
 Specifies the maximum amount of time (in seconds) to allow for setup of a session in this service as an integer from 1 though 1000000. Default: 60

Usage
Use this command to set the maximum amount of time allowed for setting up a session.

Example
The following command sets the maximum time allowed for setting up a session to 5 minutes (300 seconds):

setup-timeout 300
spi remote-address

Configures the security parameter index (SPI) between the HSGW service and the evolved Access Network/evolved Packet Control Function (eAN/ePCF). This command also configures the redirection of calls based on the PCF zone.

**Product**
HSGW

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > HSGW Service Configuration
configure > context context_name > hsgw-service service_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-hsgw-service)#
```

**Syntax**

```
spi remote-address { pcf_ip_address | ip_addr_mask_combo } spi-number number { encrypted secret enc_secret | secret secret } [ description string ] [ hash-algorithm { md5 | rfc2002-md5 } ] [ replay-protection { nonce | timestamp } ] [ timestamp-tolerance tolerance ] [ zone zone_id ]

no spi remote-address pcf_ip_address spi-number number
```

- **pcf_ip_address** | **ip_addr_mask_combo**
  - **pcf_ip_address**: Specifies the IP address of the ePCF. **pcf_ip_address** is an IP address expressed in IPv4 dotted decimal notation or IPv6 colon separated notation.
  - **ip_addr_mask_combo**: Specifies the IP address and mask bits of the PCF. **ip_addr_mask_combo** must be specified using the form “IP Address/Mask Bits” where the IP address must in IPv4 dotted-decimal or IPv6 colon-separated notation, and the mask bits are a numeric value corresponding to the number of bits in the subnet mask.

- **spi-number number**
  - Specifies the SPI which indicates a security context between the PCF and the HSGW as an integer from 256 through 4294967295.

- **encrypted secret** | **secret**
  - **encrypted secret** **enc_secret**: Specifies the encrypted shared key (**enc_secret**) between the PCF and the HSGW service. **enc_secret** must be between 1 and 236 alpha and/or numeric characters and is case sensitive.
  - **secret** **secret**: Specifies the shared key (**secret**) between the PCF and the HSGW service. **secret** must be between 1 and 127 alpha and/or numeric characters and is case sensitive.

The **encrypted** keyword is intended only for use by the chassis while saving configuration scripts. The system displays the **encrypted** keyword in the configuration file as a flag that the variable following the
**secret** keyword is the encrypted version of the plain text secret key. Only the encrypted secret key is saved as part of the configuration file.

```plaintext
description string
This is a description for the SPI expressed as an alphanumeric string of 1 through 31 characters.
```

```plaintext
hash-algorithm { md5 | rfc2002-md5 }
Specifies the hash-algorithm used between the HSGW service and the PCF. Default: md5
md5: Configures the hash-algorithm to implement MD5.
rfc2002-md5: Configures the hash-algorithm to implement keyed-MD5.
```

```plaintext
replay-protection { nonce | timestamp }
Specifies the replay-protection scheme that should be implemented by the HSGW service. Default: timestamp
nonce: Configures replay protection to be implemented using NONCE (Number ONCE).
timestamp: Configures replay protection to be implemented using timestamps.
```

```plaintext
timestamp-tolerance tolerance
Specifies the allowable difference (in seconds) between timestamps as an integer from 0 through 65535. If the difference is exceeded, the session will be rejected. If set to 0, timestamp tolerance checking is disabled at the receiving end. Default: 60
```

```plaintext
zone zone_id
Specifies the different PCF zones to configure in HSGW service. Mapping of a zone-number to a set of HSGWs can be done per HSGW service basis.
zone_id is an integer value from 1 through 32. A maximum of 32 PCF zones can be configured for a HSGW service.
```

**Usage**

An SPI is a security mechanism configured and shared by the PCF and the HSGW service. Please refer to IETF RFC 2002: IP Mobility Support for additional information.

Multiple SPIs can be configured if the HSGW service is communicating with multiple eAN/ePCFs.

**Important:** The SPI configuration on the PCF must match the SPI configuration for the HSGW service on the system in order for the two devices to communicate properly.

**Example**

This command used with the `zone` keyword redirects all calls on the basis of PCF zone to the specific HSGW on the basis of parameters configured using the `policy pcf-zone-match` command.

The following command configures the HSGW service to use an SPI of 256 when communicating with a PCF with the IP address 192.168.0.2. The key that would be shared between the PCF and the HSGW service is q397F65.

```
spi remote-address 192.168.0.2 spi-number 256 secret q397F65
```

The following command creates the configured SPI of 400 for an PCF with an IP address of 172.100.3.200 and zone id as 11:

```
spi remote-address 172.100.3.200 spi-number 400 zone 11
```
ue-initiated-qos

Configures the HSGW behavior for UE initiated QoS requests.

Product
HSGW

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > HSGW Service Configuration
configure > context context_name > hsgw-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-hsgw-service)#

Syntax

[ default | no ] ue-initiated-qos

----------

default

Returns the HSGW to the default behavior, where UE initiated QoS requests are accepted and forwarded to the PCRF via Gxa interface.

----------

no

Enables rejection of UE initiated QoS request for dedicated bearer in HSGW service. HSGW does not forward the request to the PCRF over Gxa and instead rejects the UE initiated QoS immediately.

Usage

Use this command to enable or disable support for UE initiated QoS functionality.
By default, UE initiated QoS requests are accepted and forwarded to the PCRF via Gxa interface. If PCRF rejects the UE initiated QoS, UE request is rejected.
This command allows rejection of UE initiated QoS request for dedicated bearer in HSGW service. HSGW does not forward the request to the PCRF over Gxa and instead rejects the UE initiated QoS immediately.

Example

The following command rejects UE-initiated QoS request for dedicated bearer in HSGW service:

no ue-initiated-qos
**unauthorized-flows**

Configures the service to wait a specified number of seconds before triggering a QoS update to downgrade an unauthorized flow.

**Product**
HSGW

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > HSGW Service Configuration

```
configure > context context_name > hsgw-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-hsgw-service)#
```

**Syntax**

```
unauthorized-flows qos-update wait-timeout seconds
```

```
[ default | no ] unauthorized-flows qos-update wait-timeout
```

- **default**
  Returns the command to its default setting.

- **no**
  Removes the configure wait-timeout setting for this service.

```
qos-update wait-timeout seconds
```

Specifies the number of seconds to wait before triggering the QoS update to downgrade the unauthorized flow as an integer from 1 through 65534.

**Usage**

Use this command to specific a wait timeout trigger for flows that are unauthorized by policy rules received via the Gxa interface from the PCRF. When the wit timer expires, the HSGW triggers a QoS update to downgrade the unauthorized flow.

**Example**

The following command configures the HSGW service to apply the wait time of 30 seconds after receiving an flow unauthorized by the PCRF:

```
unauthorized-flow qos-update wait-timeout 30
```
Chapter 161
HSGW Service RoHC Configuration Mode Commands

The HSGW Service RoHC Configuration Mode is used to configure Robust Header Compression (RoHC) parameters for the service.

Mode

Exec > Global Configuration > Context Configuration > HSGW Service Configuration > HSGW Service RoHC Configuration

`configure > context context_name > hsgw-service service_name > ip header-compression rohc`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ip-header-compression-rohc)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
cid-mode

This mode allows you to configure options that apply during RoHC compression for the service.

Product
HSGW

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > HSGW Service Configuration > HSGW Service RoHC Configuration

```
configure > context context_name > hsgw-service service_name > ip header-compression rohc
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ip-header-compression-rohc)#
```

Syntax

```
cid-mode { large | small } max-cid integer
default cid-mode
```

**default cid-mode**

- **default**
  
  Reset all options in the RoHC Profile Compression Configuration mode to their default values.

- **large**
  
  Use large packets with optional information for RoHC

- **small**
  
  This is the default packet size.
  Use small RoHC packets.

- **max-cid integer**
  
  Specifies the highest context ID number to be used by the compressor as an integer from 0 through 15 when small packet size is selected, and 0 through 31 when large packet size is selected. Default: 15

Usage

Use this command to set the RoHC packet size and define the maximum

Example

The following command sets large RoHC packet size and sets the maximum CID to 100:

```
cid-mode large max-cid 100
```

The following command sets the cid-mode to the default settings of small packets and max-cid 0:

```
default cid-mode
```
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
end

**Usage**
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
exit

**Usage**
Use this command to return to the parent configuration mode.
**mrru**

Specifies the size of the largest reconstructed reception unit that the decompressor is expected to reassemble from segments. The size includes the CRC. If maximum received reconstructed unit (MRRU) is negotiated to be 0, no segment headers are allowed on the channel.

**Product**
HSGW

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > HSGW Service Configuration > HSGW Service RoHC Configuration

configure > context context_name > hsgw-service service_name > ip header-compression rohc

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ip-header-compression-rohc)#
```

**Syntax**

```
mrru num_octets

default mrru
```

**default mrru**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>mrru num_octets</th>
<th>default mrru</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>default</strong></td>
<td>Resets the value of this command to its default setting of 0.</td>
<td></td>
</tr>
<tr>
<td><strong>num_octets</strong></td>
<td>Specifies the number of allowed octets for the MRRU as an integer from 0 through 65535. Default: 0</td>
<td></td>
</tr>
</tbody>
</table>

**Usage**

Use this command to set the size, in octets, of the largest reconstructed reception unit that the decompressor is expected to reassemble from segments.

**Example**

The following command sets the largest reconstructed reception unit to 1024 octets:

```
mrru 1024
```

The following command resets the MRRU size to its default of 0 octets:

```
default mrru
```
profile

Specifies the header compression profiles to use. A header compression profile is a specification of how to compress the headers of a specific kind of packet stream over a specific kind of link. At least one profile must be specified.

Product
HSGW

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > HSGW Service Configuration > HSGW Service RoHC Configuration

configure > context context_name > hsgw-service service_name > ip header-compression rohc

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ip-header-compression-rohc)#

Syntax

profile { [ esp-ip ] [ rtp-udp ] [ udp-ip ] [ uncompressed-ip ] }

default profile

default
Default: esp-ip rtp-udp udp-ip uncompressed-ip
Returns the RoHC profile configuration to its default setting.

esp-ip
Enables RoHC Profile 0x0003 which is for ESP/IP compression, compression of the header chain up to and including the first ESP header, but not subsequent subheaders.

rtp-udp
Enables RoHC Profile 0x0001 which is for RTP/UDP/IP compression

udp-ip
Enables RoHC Profile 0x0002 which is for UDP/IP compression; compression of the first 12 octets of the UDP payload is not attempted.

uncompressed-ip
Enables RoHC Profile 0x0000 which is for sending uncompressed IP packets.

Usage

Use this command to specify the RoHC header compression profiles.

Example

The following command sets the profiles to use as esp-ip and rtp-udp:
profile esp-ip rtp-udp
Chapter 162
HLR Configuration Mode Commands

The HLR Configuration Mode provides the commands and parameters to configure the home location register (HLR) node that is the database containing the subscriber profile and connection information for a specific GPRS/UMTS core network.

The HLR Configuration Mode is a sub-mode derived from the MAP Configuration Mode which controls the MAP service configuration. It is the MAP service that provides the application-layer protocol support used to connect the HLR to other nodes in the network such as the SGSN.

Exec > Global Configuration > Context Configuration > MAP Service Configuration > HLR Configuration
configure > context context_name > map-service service_name > hlr

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-map-service-service_name-hlr)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
The `acn-version-retention` command configures the ACN version retention method.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > MAP Service Configuration > HLR Configuration
configure > context context_name > map-service service_name > hlr

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-map-service-service_name-hlr)#
```

**Syntax**

```
acn-version-retention { per-imsi-prefix | per-subscriber }

default acn-version-retention
```

---

**default**

Returns the configuration to the default value: retains the version information per IMSI prefix.

---

**per-imsi-prefix**

Retain ACN version information, for communication with the HLR, on a per IMSI prefix basis.

---

**per-subscriber**

Retain ACN version information, for communication with the HLR, on a per subscriber basis.

---

**Usage**

By default, the SGSN sends ACN version 3 SAI (service area identity) to the HLR. If the SGSN receives an error message indicating that the HLR does not support that version, then the SGSN tries again with an ACN version 2 SAI. Next time the SGSN communicates with that HLR, it retains that version information and version persists based on the IMSI prefix.

Use this command to enable the SGSN to retain version according to subscriber.

---

**Example**

Configure the SGSN to retain version information according to the IMSI prefix:

```
default acn-version-retention
```
end

Exits the current configuration mode and returns to the Exec mode.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Return to the Exec mode.
exit

Exits the current configuration mode and returns to the MAP Service configuration mode.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**
exit

**Usage**
Return to the MAP Service configuration mode.
imsi

This command sets up IMSI (International Mobile Subscriber Identity) based configuration. The IMSI prefix includes the mobile country code (MCC) and the mobile network code (MNC).

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > MAP Service Configuration > HLR Configuration

configure > context context_name > map-service service_name > hlr

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-map-service-service_name-hlr)#
```

**Syntax**

```
[ no ] imsi { any | starts-with prefix_number } { imsi [ sgsn-source-address-format point-code-ssn [ source-ssn ssn ] | isdn isdn_number | mobile-global-title mgt_number [ max-gt-address-len max_gt_address ] | point-code pt-code ] }
```

- **no**
  Removes the imsi-prefix definition from the configuration.

- **any**
  Configures acceptance of any IMSI prefix.

- **starts-with prefix_number**
  Selects IMSI prefix-based routing.
  prefix_number is a string of up to 15 integers.

- **imsi**
  Enables configurable default behavior for routing.
  Entering imsi with the any keyword preserves the default behavior and the E.212 address is used as a destination address and the MAP request will be sent towards the HLR.
  If this keyword is not used with the any keyword, then the MAP request will be rejected.

- **isdn isdn_number**
  Defines the E.164 number of the HLR.
  isdn_number is a string of integers, up to 15.

- **mobile-global-title mgt_number [ max-gt-address-len max_gt_address_length ]**
  Defines the mobile global title address that the MCC/MNC portion of the IMSI will be converted to. If the maximum GT address length is specified (optional) and if the length of the MGT string is greater than defined, then the least significant digits will be omitted.
**Usage**

Routing will be done according to IMSI parameters configured with this command or according to the mobile global title address (replacing the MCC/MNC portion of the IMSI) is so specified.

**Example**

```plaintext
imsi starts-with 3 isdn 123456789 sgsn-source-address-format at point-code-ssn
```
policy routing

This command configures the policy for the routing of MAP messages. If this command is not configured or disabled (with the default keyword), then routing is done according to the configuration of the IMSI parameters.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > MAP Service Configuration > HLR Configuration
configure > context context_name > map-service service_name > hlr

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-map-service-service_name-hlr)#

Syntax

policy routing { hlr-isdn | ms-isdn }

default policy routing

no policy routing

---

default

Resets the policy routing to the system default, disabled.

---

no

Removes the policy routing configuration from the system.

---

hlr-isdn

Selects HLR-ISDN based routing.

---

ms-isdn

Selects mobile station (MS)-ISDN based routing.

---

Usage

Use this command to set the policy for routing MAP messages.

Example

policy routing hlr-isdn
release-compliance

Enables/disables the sending of EPS information in the Update GPRS Location Request message to the HLR.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > MAP Service Configuration > HLR Configuration

```
configure > context context_name > map-service service_name > hlr
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-map-service-service_name-hlr)#
```

**Syntax**

```
release-compliance release-8

no release-compliance
```

---

**release-compliance release-8**

Enables the sending of EPS information in the UGL Request message to the HLR. This setting sets the 3GPP release compliance to *Release 8 and above*.

**no release-compliance**

Disables the sending of EPS information in the UGL Request message to the HLR. This command sets the 3GPP release compliance setting to *Pre-release 8*. This is the default setting.

---

**Usage**

Use this command to enable or disable the sending of EPS information in the UGL Request message to the HLR.

Operators can use the `show map-service all` command to view the current 3GPP release compliance setting.

**Example**

This command enables the sending of EPS information in the UGL Request message to the HLR.

```
release-compliance release-8
```
Chapter 163
HNB-CS Network Configuration Mode Commands

The HNB-CS Network configuration mode provides the commands to create, provide, and manage the circuit switched (CS) network instance allowing the Home Evolved NodeB Gateway (HNB-GW) access with the CS core network in a 3G UMTS network.

**Mode**

Exec > Global Configuration > HNB-CS Network Configuration

`configure > cs-network cs_instance`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-cs-network-instance_id)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
associate alcap-service

Associates a previously defined Access Link Control Application Part (ALCAP) service with the CS network instance for multiplexing of different users onto one AAL2 transmission path using channel IDs (CIDs). This configuration is provided to support IuCS-over-ATM functionality.

Product
HNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > HNB-CS Network Configuration
configure > cs-network cs_instance

Entering the above command sequence results in the following prompt:

[local]host_name(config-cs-network-instance_id)#

Syntax

associate alcap-service svc_name context ctx_name

no associate alcap-service

Syntax

no

Removes the associated ALCAP service from this HNB-CS network instance configuration.

svc_name

Identifies the name of the ALCAP service preconfigured in Context configuration mode to associate with an HNB-CS network instance for multiplexing of different users onto one AAL2 transmission path using channel IDs (CIDs).

svc_name must be a preconfigured ALCAP service.

Only one instance of this command can be configured.

⚠️ Caution: If this CLI is not configured any RAB-ASST-REQ requesting AAL2 connection setup shall be rejected with an appropriate cause.

context ctx_name

Specifies the name of the context in which ALCAP service is configured.

cxt_name must be an existing context name in which this ALCAP service is configured.

Usage

Use this command to configure IuCS-over-ATM support. This association of ALCAP protocol service configuration in HNB-CS network instance provides multiplexing of different users onto one AAL2 transmission path using channel IDs (CIDs).
**Caution:** If this CLI is not configured any RAB-ASST-REQ message requesting AAL2 connection setup shall be rejected with an appropriate cause.

**Important:** This command must not be used more than once to configure Iu-CS-over-ATM support.

**Example**

Following command associates ALCAP service `alcap_svc1` configured in context named `Ctx_alcap1` with specific HNB-CS network instance:

```
associate alcap-service alcap_svc1context ctx_alcap1
```
associate rtp pool

Associates a previously defined RTP pool (IP pool) with the CS network instance to be used for assignment of IP address/port as RTP streams end point address over IuCS interface. This configuration support is provided for RTP stream management feature in an HNB-GW service.

Product
HNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > HNB-CS Network Configuration

*configure > cs-network cs_instance*

Entering the above command sequence results in the following prompt:

[local]host_name(config-cs-network-instance_id)#

Syntax

associate rtp pool pool_name context ctx_name

no associate rtp pool

no

Removes the associated RTP pool (IP pool) from this HNB-CS network instance configuration.

*pool_name*

Identifies the name of the RTP IP pool preconfigured in Context configuration mode to associate with an HNB-CS network instance to be used for assignment of IP address/port over the IuCS interface RTP streams. *pool_name* must be an existing IP pool name configured in Context configuration mode.

**Important:** For IP pool (RTP pool) configuration, refer *Context Configuration Commands Mode* chapter.

*context ctx_name*

Specifies the name of the context in which RTP pool (IP pool) is configured. *ctx_name* must be an existing context name in which this IP pool is configured.

Usage

Use this command to associate RTP pool (IP Pool) with an HNB-CS network instance for allotment of IP address/port over IuCS interface for RTP streams across all sessions. A fixed range of RTP ports from 5000 through 65000 shall be used to allocate to RTP stream.

**Important:** This command must be used to provide IP address/port for RTP streams end point address over IuCS interface.
**Important:** This configuration support is provided for RTP stream management feature on an HNB-GW service.

Example

Following command associates RTP pool named `rtp_1` with specific HNB-CS network instance:

```
associate rtp pool rtp_1
```
associate sccp-network

Associates a predefined Signaling Connection Control Part (SCCP) network ID with the CS network instance in order to route the messages towards MSC/VLR over IuCS interface.

**Product**
HNB-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > HNB-CS Network Configuration

```
configure > cs-network cs_instance
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-cs-network-instance_id)#
```

**Syntax**

```
associate-sccp-network sccp_net_id

no associate-sccp-network
```

**no**
Removes the associated SCCP network ID from this HNB-CS network instance configuration.

```
sccp_network_id
```

Identifies the predefined SCCP network ID to associate with an HNB-CS network instance over IuCS/IuFlex interface to enable connection with MSC/VLR(s).

*sccp_network_id* must be a predefined SCCP network ID in Global configuration mode.

**Usage**

Use this command to associate a preconfigured SCCP network ID over IuCS interface in HNB-GW service to connect with CS network elements; i.e. MSC.

**Important:** The SCCP network ID must be defined in Global Configuration mode before using it with this command.

**Important:** A single SCCP network configuration instance can not be shared with multiple HNB-CS network instances.

**Example**

Following command associates SCCP network 2 with specific HNB-CS network instance:

```
associate-sccp-network 2
```
**end**

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Use this command to return to the parent configuration mode.
global-rnc-id

Configures the Radio Network Concentrator (RNC) identifier in a Radio Network PLMN associated with HNB-CS network configuration instance. The RNC identifier is provided to the HNB during HNB-REGISTRATION.

Product
HNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > HNB-CS Network Configuration

configure > cs-network cs_instance

Entering the above command sequence results in the following prompt:

[local]host_name(config-cs-network-instance_id)#

Syntax

[ no ] global-rnc-id mcc mcc_num mnc mnc_num id id rnc_id

no

Deletes the RNC, MMC, and MNC information from the HNB-CS Network configuration instance.

mcc mcc_num

Specifies the mobile country code (MCC) part of radio network PLMN identifier as an integer value from 100 through 999.

mnc mnc_num

Specifies the mobile network code (MNC) part of radio network PLMN identifier as a 2- or 3-digit integer from 00 through 999.

Usage

Use this command to configure RNC id to associate Radio Network PLMN which will be sent to HNBs from HNB-GW during HNB-REGISTRATION procedure. Depending upon the requirement the RNC Identifier can be provided at the desired granularity.

Example

The following command configures the HNB-GW service to return an RNC identifier as 102 when an HNB-REGISTRATION request is received with LAC 1, and RAC 2:

   global rnc-id mcc 102 mnc 02 id 2
map core-network-id

Maps/associates the CS core network id to a default Mobile Switching Center (MSC) in network using MSC point code in HNB-CS network to allow HNBs to access UMTS network.

Product
HNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > HNB-CS Network Configuration

configure > cs-network cs_instance

Entering the above command sequence results in the following prompt:

[local]host_name(config-cs-network-instance_id)#

Syntax

map core-network-id cn_id point-code msc_point_code

no map core-network-id cn_id

no

Removes the mapping of a CS core network id with particular MSC point code.

cn_id

Specifies the core network identifier configured to represent a UMTS CS core network as an integer from 0 through 4095.

Multiple instance of this command can be mapped with different MSC point code.

point-code msc_point_code

Specifies the SS7 address of the default MSC in the CS network in point code value to a configured HNB-CS network instance.

point_code is an SS7 point code in dotted-decimal ###.###.### or 8-digit decimal ############ format.

Only one instance of this MSC point code can be mapped with one CS core network id.

Usage

Use this command to map a UMTS CS core network identifier with a particular MSC point code.

This command can be entered multiple times with same MSC point code to map with one or more CS core network Id, but a particular core network identifier can be mapped to one MSC only.

This command is instrumental in Iu-Flex functionality, whenever HNB-GW receives RESET/RESET-RES messages from MSC with Global CN-ID information element, the response from HNB-GW is sent to the node configured for that particular Global CN-ID.

If the RESET/RESET-RES messages do not have Global CN-ID IE, then the response of those messages is directed to the default MSC which is configured using msc point-code command in this mode.

Example

The following command configures the CS core network identifier 101 with an MSC point code 1.2.3:
map core-network-id 101 point-code 1.2.3

The following command configures the CS core network identifier 102 with the same MSC point code 1.2.3:

map core-network-id 102 point-code 1.2.3
map idnns

Configures the mapping of Intra-Domain NAS Node Selector (IDNNS) IE received from UE in RUA connect message towards HNB-GW to MSC point code. This is an important configuration for CS network resource sharing over Iu-Flex interface.

Product
HNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > HNB-CS Network Configuration
configure > cs-network cs_instance

Entering the above command sequence results in the following prompt:

[local]host_name(config-cs-network-instance_id)#

Syntax

map idnns range idnns_start to idnns_end point-code msc_point_code [ backup point-code bkup_msc_point_code ]

no map idnns range idnns_start to idnns_end

no

Removes the entries of mapping of range of IDNNS received from UE with particular MSC point code.

range idnns_start to idnns_end

Specifies the range of IDNNS received from the UE to map with a particular MSC point code during initial CS core network node selection.

idnns_start is an integer from 0 through 1023 that should be less than idnns_end.
idnns_end must be an integer from 0 through 1023 that should be more than idnns_start.
The command can be entered more than once to map multiple IDNNS ranges to the same MSC, but overlapping and mapping of the same range to different MSC point codes is not allowed.

point-code msc_point_code

Specifies the SS7 address of the MSC in the CS network to map with a range of IDNNS values.

msc_point_code is an SS7 point code in dotted-decimal ###.###.### or 8-digit decimal ####### format.

backup point-code bkup_msc_point_code

Specifies the SS7 address of the MSC to be used as a backup in the CS network to map with a range of IDNNS values.
bkup_msc_point_code is an SS7 point code in dotted-decimal ###.###.### or 8-digit decimal ####### format.
Usage

Use this command to map a NRI received from UE during initial CS network node selection to MSC point code through NRI range mapping over Iu-Flex interface.

The IDNNS refers to the information element in RUA connect message from UE towards RAN (HNB-GW). In IDNNS IE, if the choice of routing mentioned is other than local P-TMSI, then the value it provides is used against this configuration to map the MSC point code.

If backup MSC point-code is specified, then specified MSC works as backup for the IDNS range configured. This Backup MSC is selected if the mapped MSC for a given IDNNS range is going for offloading using `offload-msc point-code` command.

The command can be entered more than once to map multiple IDNNS ranges to same MSC point code, but overlapping and mapping of same range to different MSC point code is not allowed.

Example

The following command maps the IDNNS range from 101 to 201 with MSC point code 1.2.3 and point code 7.8.9 as backup MSC point code:

```
map nri range 101 to 201 point-code 1.2.3 backup point-code 7.8.9
```

The following command removes all IDNNS range matching entries between 301 to 399 from the configuration:

```
no map idnns range 301 to 399
```
map lac

Configures the mapping of the Location Area Code (LAC) received from UE to an MSC point code. This is an important configuration for CS network resource sharing without Iu-Flex interface configuration.

Product
HNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > HNB-CS Network Configuration
configure > cs-network cs_instance

Entering the above command sequence results in the following prompt:

[local]host_name(config-cs-network-instance_id)#

Syntax

map lac range lac_start to lac_end point-code msc_point_code

no map lac range lac_start to lac_end

no

Removes the entries of mapping of range of LACs received from UE with particular MSC point code.

range lac_start to lac_end

Specifies the range of LACs received from UE to map with particular MSC point code during initial CS core network node selection.

lac_start is an integer from 0 through 65535 that should be less than lac_end.
lac_end is an integer from 0 through 65535 that should be more than lac_start.
The command can be entered more than once to map multiple LAC ranges to same MSC, but overlapping is not allowed.

point-code msc_point_code

Specifies the SS7 address of the MSC in the CS network to map with a range of LAC values.
point_code is an SS7 point code in dotted-decimal ###.###.### or 8-digit decimal ####### format.

Usage

Use this command to map a LAC, received from UE during HNB registration, for MSC selection over IuCS interface through LAC range mapping with MSC point code.
This configuration is used during initial CS core network node selection when the LAC from the UE is available. This configuration is used when the core network is not using Iu-Flex interface for MSC selection.
The command can be entered more than once to map multiple LAC ranges to same MSC point code.
**Important:** This command can be used together with Iu-Flex configuration, but MSC selection based on LAC takes place only if Iu-Flex is not configured. If both Iu-Flex and LAC are configured then selection of MSC is based on Iu-Flex configuration only.

**Example**

The following command maps the LAC range from 20 to 50 with MSC point code 1.2.3:

```
map lac range 20 to 50 point-code 1.2.3
```

The following command removes all LAC range matching entries between 20 to 50 from the configuration:

```
no map lac range 20 to 50
```
map nri

Configures the mapping of Network Resource Identifier (NRI) sent from UE to the MSC point code. This is an important configuration for CS network resource sharing over Iu-Flex interface.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > HNB-CS Network Configuration

configure > cs-network cs_instance

Entering the above command sequence results in the following prompt:

[local]host_name(config-cs-network-instance_id)#

Syntax

map nri range nri_start to nri_end point-code msc_point_code

no map nri range nri_start to nri_end

<table>
<thead>
<tr>
<th>range nri_start to nri_end</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the range of NRIs received from UE to map with particular MSC point code during initial CS core network node selection.</td>
</tr>
<tr>
<td><em>nri_start</em> is an integer from 0 through 1023 that should be less than <em>nri_end</em>.</td>
</tr>
<tr>
<td><em>nri_end</em> is an integer from 0 through 1023 that should be more than <em>nri_start</em>.</td>
</tr>
<tr>
<td>The command can be entered more than once to map multiple NRI ranges to same MSC, but overlapping is not allowed.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>point-code msc_point_code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the SS7 address of the MSC in the CS network to map with a range of NRI values.</td>
</tr>
<tr>
<td><em>point_code</em> is an SS7 point code in dotted-decimal ###.###.### or 8-digit decimal ####### format.</td>
</tr>
</tbody>
</table>

Usage

Use this command to map a NRI received from UE during initial CS network node selection to MSC point code through NRI range mapping over Iu-Flex interface.

This configuration is used during initial CS core network node selection when the network resource identifier (NRI) from the UE is available. The NRI range is mapped to MSC point code. This configuration is used when the core network uses Iu-Flex interface.

The command can be entered more than once to map multiple NRI ranges to same MSC point code. It is possible to configure multiple ranges to more than one MSC however this configuration is required only when the CS core network is configured as Multi-Operator Core Network (MOCN).
When the CS core network is not MOCN and one range is mapped to more than one MSC then MSC is selected randomly in a non-predictable manner.

**Example**

The following command maps the NRI range from 101 to 201 with MSC point code 1.2.3:

```
map nri range 101 to 201 point-code 1.2.3
```

The following command maps the NRI range from 301 to 399 with MSC point code 1.2.3:

```
map nri range 301 to 399 point-code 1.2.3
```

The following command removes all NRI range matching entries between 301 to 399 from the configuration:

```
no map nri range 301 to 399
```
**msc deadtime**

Configures a timer on the HNB-GW to manage MSC availability in a CS core network on receiving of a PC-STATE-DOWN or SSN-STATE-DOWN (RANAP) indication from an SCCP instance.

**Product**
HNB-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > HNB-CS Network Configuration

`configure > cs-network cs_instance`

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-cs-network-instance_id)#
```

**Syntax**

```
msc deadtime { immediate | dur } [ no | default ] msc deadtime
```

- **no**
  Marks the peer node (MSC) as always available; it can never be marked down for a specific HNB-CS network instance.

- **default**
  Sets the default action for HNB-GW and provisions it as such that the peer node (MSC) is marked down as soon as HNB-GW receives PC-STATE-DOWN or SSN-STATE-DOWN (RANAP) indication from SCCP in a specific HNB-CS network instance. Default: Enabled

- **immediate**
  Sets the HNB-GW to mark the peer node (MSC) down immediately and clears all Iu-CS connections towards the MSC. Default: Disabled

- **dur**
  Sets the duration (in seconds) for a timer that starts when the HNB-GW receives a PC-STATE-DOWN or SSN-STATE-DOWN (RANAP) indication from SCCP for a peer MSC. On expiry of this timer the peer MSC is marked as dead and all Iu-CS connections towards that MSC are released.
  
  *dur* is an integer from 1 through 30.
  Only one instance of this command can be configured.

**Usage**

This command is used to configure a timer on HNB-GW to manage MSC availability in a CS core network on receiving of PC-STATE-DOWN or SSN-STATE-DOWN (RANAP) indication from SCCP. This configuration plays important role during RANAP reset procedure as well.
Timer value sets the duration in seconds for a timer which started once HNB-GW receives PC-STATE-DOWN or SSN-STATE-DOWN (RANAP) indication from SCCP for a peer MSC. On expiry of this timer the peer MSC is marked as dead and all Iu-CS connections towards that MSC shall be released.

**Important:** This command can be entered only once. Reentering this command overwrites the previous parameters.

**Example**

The following command configures the deadtime timer value for 10 seconds on HNB-GW. Once HNB-GW receives PC-STATE-DOWN or SSN-STATE-DOWN (RANAP) indication from SCCP for a peer MSC the HNB-GW waits for configured period and on expiry of timer it marks the specific MSC as dead:

```
msc deadtime 10
```
**msc point-code**

Configures the default MSC point-code within an HNB-CS network instance. This command is used when HNB-GW is to be connected to only one MSC with in a CS network or as default MSC for all HNBs connected through specific HNB-CS network instance.

**Product**

HNB-GW

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > HNB-CS Network Configuration  
`configure > cs-network cs_instance`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-cs-network-instance_id)#
```

**Syntax**

```
[ no ] msc point-code point_code
```

- **no**
  
  Removes the configured default MSC point code from a specific HNB-CS network instance.

**Caution:** Removing the MSC point code is a disruptive operation and affects all HNB sessions which are connected to particular MSC through an HNB-CS network instance.

**msc point-code**

Specifies the SS7 address of the default MSC in the CS network to this configured HNB-CS network instance.

*point_code* is an SS7 point code in dotted-decimal ###.###.### or 8-digit decimal ############ format. Only one instance of this command can be configured.

**Usage**

Use this command to configure a default MSC to which HNB connects for CS network access through HNB-GW service.

Point-code is an SS7 address for an element in the SS7 network. Point-codes must be defined in dotted-decimal format in a string of 1 to 11 digits. Format options include:

- 0.0.1 to 7.255.7 for point-code in the ITU range.
- 0.0.1 to 255.255.255 for point-code in the ANSI range.
- 0.0.1 to 15.31.255 for point-code in the TTC Range.
- a string of 1 to 11 digits in dotted-decimal to represent a point-code in a different range.
**Important:** This command can be entered only once. If entered again the previous value shall be overwritten.

**Example**

The following command configures a default MSC with point code 101.201.101 for HNBs to access CS network through HNB-GW service in this HNB-CS network instance:

```
msc point-code 101.201.101
```
**nri length**

Configures the network resource identifier (NRI) length in bits to identify a specific MSC serving in a pooled area. At least one NRI value has to be assigned to an MSC serving in a pool. The NRI is coded inside the temporary mobile subscriber identity (TMSI), located within bits 14 to 23 with a variable length between 0 and 10 bits. Operator needs to set this NRI length to indicate the number of bits that shall be used for the NRI field to set the parameters for Iu-Flex (MSC pooling) functionality.

**Product**
HNB-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > HNB-CS Network Configuration
configure > cs-network cs_instance

Entering the above command sequence results in the following prompt:

[local] host_name(config-cs-network-instance_id)#

**Syntax**

```
nri length nri_value

default nri length
```

**default**

Sets the NRI length to the default value of 0 and disables the Iu-Flex (MSC pooling) functionality.

```
nri length nri_value
```

Default: 0

Specifies the number of bits to be used in the P-TMSI (bits 23 to 18) to define the network resource identifier (NRI). The NRI length configuration also sets the maximum size of the pool. If not configured, the NRI length is of zero length. 

`length` is an integer from 1 to 10 that identifies the number of bits. When a non-zero value is configured the CS network is considered to be a pool.

**Usage**

Use this command to enable the Iu-Flex functionality on HNB-GW. This command identifies a unique MSC serving a pooled area for Iu-Flex functionality and at least one NRI value has to be assigned to an MSC serving in a pool. It performs MSC pooling/offloading scenario over Iu-Flex interface. The NRI is stored in the bits 14 to 23 of TMSI. The HNB-GW uses a portion of this NRI to set the parameters for Iu-Flex (MSC pooling) functionality.

If more than one NRI is configured, the HNB-GW service does round-robin between the available NRIs when new subscriber(s) (re)connect.

This command must be used in conjunction with `null nri` command to configure MSC pooling/offloading over Iu-Flex interface.

**Example**
The following command sets the HNB-GW to a bit length of 6 to derive the values from the NRI field (stored in bits 14 to 23 of TMSI) to set the parameters for Iu-Flex (MSC pooling) functionality:

```plaintext
nri length 6
```
null-nri

Configures the null NRI for load redistribution in support of Iu-Flex functionality. The NRI value defined with this command must be unique across the pool areas. This null-NRI is used by HNB-GW for load redistribution during MSC offloading.

Product
HNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > HNB-CS Network Configuration

configure > cs-network cs_instance

Entering the above command sequence results in the following prompt:

[local]host_name(config-cs-network-instance_id)#

Syntax

null-nri null_nri_value

no null-nri null_nri_value

no

Disables/removes the configured null-NRI value used for MSC offloading procedure.

null_nri_value

Specifies the null-NRI value to be used by HNB-GW for load redistribution during MSC offloading as an integer from 0 through 1023.
Without MOCN configuration this value can be entered only once.
For MOCN a unique null-NRI must be assigned to each MOCN operator identified by its PLMN-ID (MCC+MNC).
A 0 (zero) value configured as a null-NRI indicates the keyword is not to be used. There is no default value for this parameter.

Usage

Use this command to identify the MSC to be used by HNB-GW for load redistribution during MSC offloading over an Iu-Flex interface.
There is one unique null-NRI in a PLMN supporting pool functionality.
Without MOCN configuration this command can be entered only once. For MOCN a unique null-NRI must be assigned to each MOCN operator identified by its PLMN-ID (MCC+MNC).

Example

The following command sets the null-NRI as 1001 to be used by HNB-GW for load redistribution during MSC offloading:

null-nri 1001
offload-msc

Provisions the HNB-GW to enable or disable the exclusion of a particular primary MSC node during an NAS Node Selection Function (NNSF) procedure when it needs to be offloaded while using Iu-Flex functionality on the HNB-GW.

**Product**
HNB-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > HNB-CS Network Configuration

configure > cs-network cs_instance

Entering the above command sequence results in the following prompt:

[local]host_name(config cs-network-instance_id)#

**Syntax**

```
[ no ] offload-msc point-code msc_point_code
```

- **no**
  Removes the specified primary MSC point code from the exclusion list for NNSF function on HNB-GW and re-enables the inclusion of the primary MSC to be considered by HNB-GW.

- **point-code msc_point_code**
  Specifies the SS7 address of the primary MSC in the CS network to be excluded for NNSF function on HNB-GW when it needs to be offloaded via Iu-Flex functionality.

  *point_code* is an SS7 point code in dotted-decimal ###.###.### or 8-digit decimal ############ format.

  Only one instance of this primary MSC point code can be mapped with one CS core network id.

**Usage**

Use this command to provision the HNB-GW to enable or disable the exclusion of the primary MSC node when it needs to be offloaded.

When this command is enabled for exclusion of primary MSC node during NNSF function in HNB-GW, the HNB-GW excludes the particular node from being considered.

User can re-enable the inclusion of the primary MSC node to be considered for NNSF functionality by **no offload-msc point-code** command.

**Important:** Offload check is only for the primary point code and NOT for the backup point code.

**Example**

This command can be used for planned maintenance as well.

The following command configures the HNB-GW to exclude the primary MSC point code 1.2.3 from being considered in NSSF function for Iu-Flex support:

```
offload-msc point-code 1.2.3
```
The following command re-enables the inclusion of MSC point code 1.2.3 from being considered in NSSF function for Iu-Flex support:

```plaintext
no offload-msc point-code 1.2.3
```
ranap reset

Configures various Radio Access Network (RAN) Application Part reset procedure parameters for CS network association in an HNB access network.

**Product**
HNB-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > HNB-CS Network Configuration

configure > cs-network cs_instance

Entering the above command sequence results in the following prompt:

[local]host_name(config-cs-network-instance_id)#

**Syntax**

```
ranap reset { ack-timeout timer_value | guard-timeout g_timer | hnbgw-initiated | max-retransmissions retries }
```

```
default ranap reset { ack-timeout | guard-timeout | hnbgw-initiated | max-retransmissions }
```

```
no ranap { hnbgw-initiated }
```

---

**default**
Resets the RANAP RESET parameters in HNB-CS Network configuration instance.

---

**no**
Disables the RANAP RESET procedure related parameters in an HNB-CS Network configuration instance.

---

**ack-timeout timer_value**
Sets the timer value (in seconds) to wait for Reset Acknowledge from MSC. This is used during HNB-GW initiated RANAP RESET procedure in HNB-CS Network configuration instance.

*timer_value* is an integer value from 5 through 10. Default: 10

---

**guard-timeout g_timer_value**
Sets the timer value (in seconds) to send Reset Acknowledge to MSC. After this duration the HNB-GW sends RESET-ACK to MSC. This is used during MSC initiated RANAP RESET procedure in HNB-CS Network configuration instance.

*g_timer_value* is an integer value from 5 through 10. Default: 10

---

**hnbgw-initiated**
Enables the HNB-GW Initiated RANAP RESET procedures. Default: Disabled
max-retransmission retries

Sets the maximum number of retries allowed for transmission of RESET-ACK message to MSC. This is used during RANAP RESET procedure in HNB-CS Network configuration instance.

retries is an integer value from 0 through 2. When 0 is used retransmission is disabled. Default: 1

use-actual-plmn

Actual PLMN will be sent in RANAP Reset/Reset Resource. By default, Common PLMN will be sent.

Usage

Use this command to configure the RANAP RESET procedure related parameters in HNB-CS Network configuration for multiple HNB-GW service support.

Example

The following command configures the HNB-GW initiated RANAP RESET Procedure for an HNB-CS Network configuration instance:

```
ranap reset hnbgw-initiated
```
The 3G UMTS Home-NodeB Gateway Global Configuration Mode provides the global configurations for multiple HNB-GW services on a chassis to manage the access to the UMTS core network in a 3G UMTS network through a Femto node. This configuration mode is supported from StarOS 14.0 onward.

Mode

Exec > Global Configuration > HNB-GW Global Configuration

configure > hnbgw-global

Entering the above command sequence results in the following prompt:

[local]host_name(config-hnggw-global)#

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
access-control-db

Configures the access control database parameters in HNB-GW Global configuration mode to control HNB and UE access to the HNB-GW node.

Product

HNB-GW

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > HNB-GW Global Configuration

configure > hnbgw-global

Entering the above command sequence results in the following prompt:

[local]host_name(config-hnggw-global)#

Syntax

access-control-db imsi-purge-timeout { immediate | dur }

default access-control-db imsi-purge-timeout

default

Sets the default value to HNB-UE access control database on a chassis for HNB-GW Global configuration instance.

The default timeout duration for purging of the IMSI White List from the HNB-GW Access Control database is 24 hours. The HNB-GW service waits for 24 hours after all referenced HNBs have de-registered before purging the records.

immediate

Sets the HNB-GW Global configuration instance to purge the HNB-UE access control database immediately after all referenced HNBs have de-registered.

imsi-purge-timeout dur

Sets the timeout duration (in minutes) for the access control database to wait before purging the IMSI values received as a White List from HMS/BAC.

After all HNBs have de-registered, the Access Control database on HNB-GW maintains the IMSI White List received from HMS/BAC during HNB registration procedure for the configured durations before purging the list.

dur is an integer from 1 through 1440.

Usage

Use this command to configure the HNB-UE access control database parameters on a chassis for HNB-GW Global configuration instance.

This command sets the timeout duration to maintain the IMSI White List received from HMS/BAC during HNB registration procedure in HNB-GW Global configuration instance for the configured dur in minutes after de-registration of all referenced HNBs from HNB-GW node and then purge the database.
Example

Following command sets the HNB-GW Global configuration instance to purge all IMSI records from HNB-UE access control database immediately after all referenced HNBs de-registered from HNB-GW service instance.

```
access-control-db imsi-purge-timeout immediate
```
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
end

**Usage**
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

exit

Usage
Use this command to return to the parent configuration mode.
paging hybrid-hnb

Configures paging optimization parameters for hybrid HNBs connected through Hybrid Access mode in the HNB-GW Global parameter.

Product
HNB-GW
Privilege
Security Administrator, Administrator
Mode
Exec > Global Configuration > HNB-GW Global Configuration
configure > hnbgw-global
Entering the above command sequence results in the following prompt:

[local]host_name(config-hnbgw-global)#

Syntax

paging hybrid-hnb always

paging hybrid-hnb hnb-where-ue-registered [hnbs-having-imsi-in-whitelist] fallback {always | never |only-if-with-paging-area}

paging hybrid-hnb hnbs-having-imsi-in-whitelist fallback {always | never |only-if-with-paging-area}

paging hybrid-hnb never

paging hybrid-hnb only-if-with-paging-area

default paging hybrid-hnb

default
Sets the default behavior of paging optimization configuration for a hybrid HNB while using Hybrid Access mode support.
By default the HNB-GW pages hybrid HNBs only if paging-area IE is received in the paging message.

{always | never | only-if-with-paging-area}
Sets the HNB-GW Global parameter to page hybrid HNB for a paging message.
always: Sets the system to ALWAYS page the hybrid HNBs irrespective of paging-area IE is received in paging messages.
never: Sets the system to NEVER page any hybrid HNB.
only-if-with-paging-area: Sets the system to page the hybrid HNBs only when paging-area IE is received in paging messages.

hnb-where-ue-registered fallback {always | never | only-if-with-paging-area}
Sets the HNB-GW Global parameter to page hybrid HNB from where the UE is registered.
always: Sets the system to ALWAYS page the hybrid HNBs from where the UE is registered. If the UE is not registered then it pages the hybrid HNBs irrespective of paging-area IE is received in paging messages.
never: Sets the system to page the hybrid HNBs from where the UE is registered. If the UE is not registered then it NEVER pages any hybrid HNB.
only-if-with.paging-area: Sets the system to ALWAYS page the hybrid HNBs from where the UE is registered. If the UE is not registered then it pages the hybrid HNBs only when paging-area IE is received in paging messages.

hnbs-having-imsi-in-whitelist fallback {always | never | only-if-with-paging-area}

Sets the HNB-GW Global parameter to page hybrid HNB where HNB have IMSI in white-list.
always: Sets the system to ALWAYS page Hybrid HNB which have requested IMSI in whitelist. If no such Hybrid HNB is found, then system will page Hybrid HNBs irrespective of presence or absence of paging-area IE in paging messages.
ever: Sets the system to ALWAYS page Hybrid HNB which have requested IMSI in whitelist. If no such Hybrid HNB is found, then system will NEVER page Hybrid HNBs irrespective of presence or absence of paging-area IE in paging messages.
only-if-with-paging-area: Sets the system to ALWAYS page Hybrid HNB which have requested IMSI in whitelist. If no such Hybrid HNB is found, then system will page hybrid HNB only when paging-area IE is found in paging messages.

Usage
Use this command to configure the paging optimization parameters for hybrid HNBs connected through Hybrid Access mode in HNB-GW Global parameter.

Example
The following command configures the HNB-GW Global parameter to page an hybrid HNB from where the UE is registered and paging-area IE is received in paging message:

```bash
ing hybrdid-hnb hnb-where-ue-registered fallback only-if-with-paging-area
```
paging open-hnb

Configures paging optimization parameters for open HNBs connected through Hybrid Access mode in the HNB-GW Global parameter.

⚠️ Important: This command is deprecated from release 16.0.

**Product**
HNB-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > HNB-GW Global Configuration
configure > hnbgw-global
Entering the above command sequence results in the following prompt:

```
[local]host_name(config-hnggw-global)#
```

**Syntax**

```
paging open-hnb [hnb-where-ue-registered fallback] {always | never | only-if-with-paging-area}
default paging open-hnb
```

**default**
Sets the default behavior of paging optimization configuration for an open HNB while using Open Access mode support.
By default the HNB-GW pages open HNBs only if paging-area IE is received in the paging message.

```
default {always | never | only-if-with-paging-area}
```

Sets the HNB-GW Global configuration instance to page open HNB for a paging message.

- **always**: Sets the system to ALWAYS page the open HNBs irrespective of paging-area IE is received in paging messages.
- **never**: Sets the system to NEVER page any open HNB.
- **only-if-with-paging-area**: Sets the system to page the open HNBs only when paging-area IE is received in paging messages.

```
hnb-where-ue-registered fallback {always | never | only-if-with-paging-area}
```

Sets the HNB-GW Global configuration instance to page open HNB from where the UE is registered.

- **always**: Sets the system to ALWAYS page the open HNBs from where the UE is registered. If the UE is not registered then it pages the open HNBs irrespective of paging-area IE is received in paging messages.
- **never**: Sets the system to page the open HNBs from where the UE is registered. If the UE is not registered then it NEVER pages any open HNB.
- **only-if-with-paging-area**: Sets the system to ALWAYS page the open HNBs from where the UE is registered. If the UE is not registered then it pages the open HNBs only when paging-area IE is received in paging messages.
Usage

Use this command to configure the paging optimization parameters for open HNBs connected through Open Access mode in HNB-GW Global configuration instance.

Example

The following command configures the HNB-GW Global configuration instance to page an open HNB from where the UE is registered and `paging-area` IE is received in paging message:

```plaintext
paging open-hnb hnb-where-ue-registered fallback only-if-with-paging-area
```
sctp

Configures the SCTP-related parameters like timeout duration for various timers and cookie life over an IuH interface on a chassis for HNB-GW Global configuration instance.

Product
HNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > HNB-GW Global Configuration
configure > hnbgw-global

Entering the above command sequence results in the following prompt:

[local]host_name(config-hnbgw-global)#

Syntax

sctp { alpha-rto alpha_rto_dur | beta-rto beta_rto_dur | max-in-strms in_strms | max-out-strms out_strms | max-retx { assoc | init | path } max_retry }

default sctp { alpha-rto | beta-rto | max-in-strms | max-out-strms | max-retx { assoc | init | path } }

default
Restores the SCTP parameters to default value in HNB-GW Global configuration instance. Default values for all parameters are as follows:

• alpha-rto: 5 seconds
• beta-rto: 10 seconds
• max-in-strms: 4
• max-out-strms: 4
• max-retx assoc: 10 retries
• max-retx init: 5 retries
• max-retx path: 5 retries

alpha-rto alpha_rto_dur
Sets the alpha retransmission timeout duration (in seconds) for SCTP association between HNB and HNB-GW as an integer from 0 through 65535. A “zero” value disables the timer in this configuration. Default: 5

beta-rto beta_rto_dur
Sets the beta retransmission timeout duration (in seconds) for SCTP association between HNB and HNB-GW an integer from 0 through 65535. A “zero” value disables the timer in this configuration. Default: 10
max-retx { assoc | init | path } max_retry

Sets the maximum number of retries allowed in SCTP states for SCTP association between HNB and HNB-GW.

**assoc**: Sets the maximum number of consecutive retransmissions to its peer is allowed. If the value of this counter exceeds the limit configured with this keyword the HNB-GW considers the peer HNB unreachable and stop transmitting any more data to it. The SCTP association is automatically closed when the peer endpoint becomes unreachable. Default number of attempts max_retry for this state is 10.

**init**: Sets the maximum attempts allowed after T1-init timer expires. If the T1-init timer expires then the HNB-GW retransmits INIT chunk and re-start the T1-init timer without changing state. This is repeated up to the configured times with this configuration. After that, the HNB-GW aborts the initialization process. Default number of attempts max_retry for this state is 5.

**path**: Sets the maximum attempts allowed after T3-rtx timer expires. Each time the T3-rtx timer expires on any address, or when a HEARTBEAT sent to an idle address is not acknowledged within a RTO, the error counter of that destination address incremented. When the value in the error counter exceeds this protocol parameter of that HNB address, the HNB-GW marks the destination transport address as inactive. Default number of attempts max_retry for this state is 5.

**max_retry** is an integer from 0 through 255.

max-in-strms in_strms

Sets the maximum number of inward SCTP streams allowed on HNB-GW for an associated HNB in an SCTP association as an integer from 1 through 16. Default: 4

max-out-strms out_strms

Sets the maximum number of outgoing SCTP streams allowed from HNB-GW for an associated HNB in an SCTP association as an integer from 1 through 16. Default: 4

**Usage**

Use this command to configure the SCTP protocol messaging and session management parameters in SCTP association between HNB and HNB-GW.

**Example**

The following command sets the maximum number of inward SCTP streams allowed to 4 on HNB-GW for the SCTP association:

```
default max-in-strms
```
tnnsf-timer

Configures the NAS Node Selection Function (NNSF) timer (T-NNSF) which is used by the HNB-GW to store the IMSI and the relevant Global-CN-ID in the short term after Paging. This timer is used for Iu-Flex feature support.

Product
HNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > HNB-GW Global Configuration

configure > hnbgw-global

Entering the above command sequence results in the following prompt:

[local] host_name(config-hnggw-global)#

Syntax

```
        tnnsf-timer dur

[ no | default ] tnnsf-timer
```

no
Disables/removes the configured timer value of NNSF timer (T-NNSF) for HNB-GW Global configuration instance.

default
Sets the timer value of NNSF timer (T-NNSF) for HNB-GW Global configuration instance to default value of 30 seconds.

```
        tnnsf-timer dur
```

Configures the NNSF timer (in seconds) which is used by the HNB-GW to store the IMSI and the relevant Global-CN-ID as an integer from 10 through 60. Default: 30

Usage

Use this command to configure the NNSF timer value in seconds for Iu-Flex support. Whenever the MSC sends the paging request with IMSI, the HNB-GW stores the Global_CN_ID of the node which issued the paging request message for the given IMSI and HNB-GW starts the tnnsf-timer. HNBGW stores the mapping of IMSI to Global_CN_ID until the tnnsf-timer expires

Example

The following command sets the NNSF timer value to 30 seconds on a chassis for HNB-GW Global configuration instance:

```
default tnnsf-timer
```
Chapter 165  
HNB-GW Service Configuration Mode Commands

The 3G UMTS Home-NodeB Gateway Service Configuration Mode manages access to the UMTS core network in a 3G UMTS network through a Femto node.

**Mode**

Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

`configure > context context_name > hnbgw-service service_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-hnbgw-service)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
access-control-db

Configures the access control database parameters in an HNB-GW service instance to control HNB and UE access to the HNB-GW node.

Product
HNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

configure > context context_name > hnb-gw-service service_name

Entering the above command sequence results in the following prompt:

[local] host_name(config-hnb-gw-service) #

Syntax

access-control-db imsi-purge-timeout {immediate | dur }

default access-control-db imsi-purge-timeout

default

Sets the default value to HNB-UE access control database on HNB-GW service instance.
The default timeout duration for purging of the IMSI White List from the HNB-GW Access Control database is 24 hours. The HNB-GW service waits for 24 hours after all referenced HNBs have de-registered before purging the records.

immediate

Sets the HNB-GW service to purge the HNB-UE access control database immediately after all referenced HNBs have de-registered.

imsi-purge-timeout dur

Sets the timeout duration (in minutes) for the access control database to wait before purging the IMSI values received as a White List from HMS/BAC.
After all HNBs have de-registered, the Access Control database on HNB-GW maintains the IMSI White List received from HMS/BAC during HNB registration procedure for the configured durations before purging the list.
dur is an integer from 1 through 1440.

Usage

Use this command to configure the HNB-UE access control database parameters on HNB-GW service.
This command sets the timeout duration to maintain the IMSI White List received from HMS/BAC during HNB registration procedure in HNB-GW service for the configured dur in minutes after de-registration of all referenced HNBs from HNB-GW node and then purge the database.

Example
Following command sets the HNB-GW service instance to purge all IMSI records from HNB-UE access control database immediately after all referenced HNBs de-registered from HNB-GW service instance.

```
access-control-db imsi-purge-timeout immediate
```
**associate cbs-service**

Configures CBS service for this HNBGW service.

**Product**

HNB-GW

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

```
configure > context context_name > hnbgw-service service_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-hnbgw-service)#
```

**Syntax**

```
associate cbs-service svc_name

no associate cbs-service
```

**no**

Removes the configured CBS service from this HNB-GW service configuration.

**svc_name**

Identifies the name of the pre-configured CBS service to associate with an HNB-GW service. **svc_name** is an alphanumeric string of 1 through 63 characters.

**Usage**

Use this command to configure CBS service for HNB-GW service.

**Example**

Following command configures CBS service named *cbs-hnb1* with specific HNB-GW service.

```
associate cbs-service cbs-hnb1
```
associate gtpu-service

Associates a previously configured GTP-U service to bind the HNB-GW service with an HNB towards the HNB side. A GTP-U service must be configured in Context Configuration mode before using this configuration.

**Product**
HNB-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

```
configure > context context_name > hnbgw-service service_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-hnbgw-service)#
```

**Syntax**

```
associate gtpu-service svc_name

no associate gtpu-service
```

no

Removes the associated GTP-U service from this HNB-GW service configuration.

```
svc_name
```

Identifies the name of the pre-configured GTP-U service to associate with an HNB-GW service towards the Home-NodeB side.

svc_name is an alphanumeric string of 1 through 63 characters.

**Usage**

Use this command to configure GTP-U data plan between HNB-GW service and Home-NodeB. The service defined for GTP-U can be configured in Context configuration mode.

**Important:** Another GTP-U service can be used to bind the HNB-GW service towards the Core Network and can be configured in HNB-PS Configuration mode. For more information on GTP-U service configuration, refer *GTP-U Service Configuration Mode Commands*.

**Example**

Following command associates GTP-U service named *gtpu-hnbl* with specific HNB-GW service towards Home-NodeB side.

```
associate gtpu-service gtpu-hnbl
```
associate rtp pool

Associates a previously defined RTP pool (IP pool) with the HNB-GW service. This pool is used by HNB-GW to send an IP address to HNB where HNB uses it to map the RTP streams over Iuh interface. This command is used for RTP stream management on HNB-GW.

Product
HNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

configure > context context_name > hnb-gw-service service_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-hnb-gw-service)#

Syntax

associate rtp pool pool_name

no associate rtp pool

no

Removes the associated RTP pool (IP pool) from this HNB-GW service configuration.

pool_name

Specifies the name of the pre-configured RTP IP pool that the HNB-GW uses to assign IP addresses when mapping RTP streams over the Iuh interface.

pool_name is an alphanumeric string of 1 through 31 characters.

Important: For IP pool (RTP pool) configuration, refer ip pool command in Context Configuration Mode Commands chapter.

Usage

Use this command to associate an RTP pool (IP Pool) with an HNB-GW service for allotment of RTP IP address to HNB-GW node and send the same to HNB for RTP stream management support. The HNB maps the RTP streams with received IP address(es) while communicating with HNB-GW over Iuh interface where HNB-GW communicates with MSC/VLR through IuCS-over-IP tunnel.

This command is used for RTP stream management on HNB-GW.

Important: This command must be used to provide IP address for mapping of RTP streams on Iuh interface between HNB and HNB-GW.

Example
Following command associates RTP pool named `rtp_1` with HNB-GW service for RTP stream end point from Home-NodeB:

```
associate rtp pool rtp_1
```
**authorised-macro-lai macro-info-ie-absent-action**

This command configures the Action if Macro Coverage information IE is absent in HNB Location Information. The HNB will be accepted for Action Accept and rejected for Action Reject.

**Product**
HNB-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

```
configure > context context_name > hnbgw-service service_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-hnbgw-service)#
```

**Syntax**

```
authorised-macro-lai macro-info-ie-absent-action { accept | reject }
```

**Example**

The following command accepts HNB even if Macro Coverage information IE is absent in HNB Location Information:

```
authorised-macro-lai macro-info-ie-absent-action accept
```
**authorised-macro-lai mcc**

This command configures MCC of Pre-Configured macro lai range for HNB Authorisation.

**Product**
HNB-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

`configure > context context_name > hnbgw-service service_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-hnbgw-service)#
```

**Syntax**

```
[ no ]authorised-macro-lai mcc mcc mnc mnc lac range min to max
```

- `no`
  Removes the MCC of Pre-Configured macro lai range for HNB Authorisation.

- `mcc mcc`
  MCC of Pre-Configured macro lai range for HNB Authorisation.
  `mcc` is a number ranging from 100 through 999.

- `mnc mnc`
  MNC of Pre-Configured macro lai range for HNB Authorisation.
  `mnc` is a number ranging from 00 through 999.

- `lac range min to max`
  LAC of Pre-Configured macro lai range for HNB Authorisation.
  LAC is configured as range, if single lac make min is equal to max.
  Macro LAC from `min` to `max` integer values between 0 through 65535.

**Usage**

Use this command to configure the MCC of Pre-Configured macro lai range for HNB Authorisation.

**Example**

The following command configures the MCC of Pre-Configured macro lai range for HNB Authorisation with `mcc 888`, `mnc 44` and `lac range from 10 to 1000`:

```
authorised-macro-lai mcc 678 mnc 788 lac range 10 to 1000
```
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
```
end
```

**Usage**
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Use this command to return to the parent configuration mode.
handin

Allows or disallows the incoming hand-over of an MS in HNB-GW via the Serving Radio Network Subsystem (SRNS) Relocation procedure for the specified packet switched/circuit switched (PS/CS) core network (CN) domain.

**Product**
HNB-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

`configure > context context_name > hnbgw-service service_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-hnbgw-service)#
```

**Syntax**

```
[ no | default ] handin cn-domain [ cs | ps ]
```

---

**no**

Disallows the incoming MS hand-over for the particular CN domain via SRNS Relocation procedure in an HNB-GW service instance.

If hand-over is restricted the relocation request will be rejected with rejection cause “Relocation Not Supported In Target RNC Or Target System”.

---

**default**

Sets the HNB-GW service instance to allow the incoming MS hand-over for the particular CN domain via SRNS Relocation procedure in an HNB-GW service instance.

---

**cs**

Sets the HNB-GW service instance to allow the incoming MS hand-over for the CS core network domain via SRNS Relocation procedure in an HNB-GW service instance.

---

**ps**

Sets the HNB-GW service instance to allow the incoming MS hand-over for the PS core network domain via SRNS Relocation procedure in an HNB-GW service instance.

---

**Usage**

Use this command to set HNB-GW service instance for allowing/disallowing incoming hand-over of an MS in HNB-GW via SRNS Relocation procedure for PS or CS core network domain.

If hand-over is restricted the Relocation Request message will be rejected with rejection cause “Relocation Not Supported In Target RNC Or Target System”.

---

**Example**

The following command configures the HNB-GW service instance to allow hand-over of an MS in HNB-W via SRNS Relocation procedure for PS core network domain:
handin ps
**hnb override-vsa location-based-service**

This command enables / disables overriding of a particular vendor specific attribute of configured location based HNB Service.

**Product**
HNB-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

```configure > context context_name > hnbgw-service service_name```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-hnbgw-service)#
```

**Syntax**

```hnb override-vsa location-based-service```

```no hnb override-vsa location-based-service```

```default hnb override-vsa location-based-service```

**no**

Disables the overriding of vendor specific attribute for location based service.

**default**

When set to default, overriding of vendor specific attribute will be disabled.

**Usage**

Use this command to enable / disable overriding of a particular vendor specific attribute of configured location based HNB Service.

**Example**

The following command enables overriding of a particular vendor specific attribute of configured location based HNB Service :

```hnb override-vsa location-based-service```
**hnb-access-mode hybrid**

This command configures the Hybrid HNB access mode in HNB-GW service instance and related parameters.

**Product**
HNB-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

`configure > context context_name > hnbgw-service service_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-hnbgw-service)##
```

**Syntax**

```
hnb-access-mode hybrid [ max-non-access-controlled-ue num ]
```

- `no hnb-access-mode hybrid`
- `default hnb-access-mode hybrid`

**no**
Disables the Hybrid Access Mode of HNB service.

**default**
Sets the default configuration of Hybrid Access Mode support. The default value of Maximum Non-Access-Controlled UEs per Hybrid HNB is 64.

By default, HNB-GW allows registration of Non-Access-Controlled UEs per Hybrid HNB and a maximum of 16 UEs can register from a hybrid HNB in an HNB-GW service instance.

**max-non-access-controlled-ue num**
Maximum Non-Access-Controlled UEs per Hybrid HNB.

- `num` is an integer from 0 through 64.

**Usage**

Use this command to configure the Hybrid HNB access mode in HNB-GW service instance and related parameters.

**Example**

The following command configures the Hybrid HNB access mode in HNB-GW service instance and related parameters.:

```
hnb-access-mode hybrid
```
**hnb-access-mode mismatch-action**

This command configures the mismatch action of HNB access mode in HNB-GW service instance and related parameters.

**Product**
HNB-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

`configure > context context_name > hnbgw-service service_name`

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-hnbgw-service) #
```

**Syntax**

```
hnb-access-mode mismatch-action { accept-aaa-value | hnb-reg-rej }

default hnb-access-mode mismatch-action
```

**default**
Sets the default Hybrid Access Mode of HNB service. The default value of Maximum Non-Access-Controlled UEs per Hybrid HNB is 64.

**accept-aaa-value**
Supports the Accept AAA value.

**hnb-reg-rej**
Supports the HNB Registration Reject.

**Usage**
Use this command to configure the mismatch action of HNB access mode in HNB-GW service instance and related parameters.

**Example**
The following command configures the mismatch action of HNB access mode in HNB Service to Accept AAA value:

```
hnb-access-mode mismatch-action accept-aaa-value
```
hnb-access-mode open

Configures the Open HNB access mode in HNB-GW service instance and related parameters.

Product
HNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration
configure > context context_name > hnbgw-service service_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-hnbgw-service)#

Syntax

hnb-access-mode open [ max-registered-ue reg_ue_open]

no hnb-access-mode open

default hnb-access-mode open

no

Disables Open Access mode support.
If disabled and an Open HNB tries to register, the HNB-GW sends HNB-Registration-Reject message with “OAM Intervention” cause.

Important: UE-Reg/CS-Call/PS-Call requests (both existing and future) is allowed from already registered Open HNBs even after operator has disabled the Open Access support. No new Open HNB registration is allowed once operator disables the Open Access support.

default

Sets the default configuration of Open Access mode support.
By default, HNB-GW allows registration of Open HNBs and a maximum of 64 UEs can register from an open HNB in an HNB-GW service instance.

max-registered-ue reg_ue_open

Sets the HNB-GW service instance to allow the maximum number of UEs through an open HNB under Open Access mode support.

reg_ue_open defines the maximum number of UEs that can register from an Open HNB as an integer from 1 through 64.
If a UE tries to register from an Open HNB which has already reached to the configured limit configured, the HNB-GW sends HNB-Registration-Reject message with “ue not allowed in this hnb” cause in an HNB-GW service instance.
**Usage**

Use this command to configure the HNB-GW service instance for Open Access Mode support and related parameters.

This command enables Open Access mode support to allow the UEs that can register from an Open HNB. If a UE tries to register from an Open HNB with an HNB-GW service instance, which is already reached to the limit configured through `max-registered-ue reg_ue_open` the HNB-GW sends HNB-Registration-Reject message with "ue not allowed in this hnb" cause.

**Important:** If Operator has reduced the maximum number of UEs allowed per Open HNB during the session, this will not have any effect on already registered UEs/CS-Calls/PS-Calls even if previously configured `reg_ue_open` is beyond the newly configured `reg_ue_open` value. Limits are respected while handling new requests.

**Example**

The following command configures the HNB-GW service instance to allow 16 UEs to register through an open HNB:

```
  hnb-access-mode open max-registered-ue 16
```
hnb-identity

Configures and also allows modification to the HNB ID before it is sent to the AAA server for authentication in HNB-GW service instance.

Product
HNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

configure > context context_name > hnbw-service service_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-hnbw-service)#

Syntax

[ default | no ] hnb-identity oui discard-leading-char

no
Disables discarding of leading character of HNB-id if it contains Organizationally Unique Identifier

default
Enables the default behavior of discarding of leading character of HNB-id if it contains Organizationally Unique Identifier. By default this feature is deactivated.

oui discard-leading-char

This CLI allows to modify the HNB ID before it is sent to the AAA server for authentication. By using this CLI, first character of the HNB-id can be removed if the HNB-id follows the format: ‘1<OUI>-<SerialNumber>@<realm>’.

Example

The following command configures the discarding of leading character of HNB-id if it contains Organizationally Unique Identifier:

hnb-identity oui discard-leading-char
ip iu-qos-dscp

Enables or disables the DSCP marking parameter for data packets carried over an IuCS/IuPS interface towards MSC/SGSN. By default this command is **Disabled**.

**Product**
HNB-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

configure > context context_name > hnbgw-service service_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-hnbgw-service)#

**Syntax**

```
ip iu-qos-dscp protocol udp payload { gtpu | rtcp | rtp } dscp_code
[ default | no ] ip iu-qos-dscp protocol udp payload { gtpu | rtcp | rtp } dscp_code
```

- **no**
  
  Use this keyword to place the configuration in **pass-through** mode (no marking of DSCP). Use of this keyword is allowed even when there is no previous DSCP parameter set.

  **Important:** In this configuration the **no** keyword does not disable or remove a previous configuration.

- **default**
  
  Enables the DSCP marking on HNB-GW and set/restores the QoS parameters to their default setting.

  ```
  udp payload { gtpu | rtcp | rtp } dscp_code
  ```

  Specifies the QoS traffic pattern towards MSC/SGSN in SCTP protocol association over IuCS/IuPS interface. By this keyword the Traffic classes specified by a user based on UDP protocol and GTPU, RTCP, and RTP type of payload identified based on the transport level port numbers.

  Default DSCP code in UDP traffic are:

  - **GTP-U**: cs1
  - **RTCP**: ef
  - **RTP**: af41

  ```
  dscp_code
  ```

  Specifies the QoS DSCP codes supported for SCTP and UDP traffic and its payloads towards MSC/SGSN over IuCS/IuPS interface.

  **following type of DSCP codes** **dscp_code** **are supported over IuH interface:**
• af11: Marks traffic as Assured Forwarding 11 PHB (high throughput data)
• af12: Marks traffic as Assured Forwarding 12 PHB (high throughput data)
• af13: Marks traffic as Assured Forwarding 13 PHB (high throughput data)
• af21: Marks traffic as Assured Forwarding 21 PHB (low latency data)
• af22: Marks traffic as Assured Forwarding 22 PHB (low latency data)
• af23: Marks traffic as Assured Forwarding 23 PHB (low latency data)
• af31: Marks traffic as Assured Forwarding 31 PHB (multimedia streaming)
• af32: Marks traffic as Assured Forwarding 32 PHB (multimedia streaming)
• af33: Marks traffic as Assured Forwarding 33 PHB (multimedia streaming)
• af41: Marks traffic as Assured Forwarding 41 PHB (multimedia conferencing). This is the default DSCP code for RTP payloads in UDP protocol.
• af42: Marks traffic as Assured Forwarding 42 PHB (multimedia conferencing)
• af43: Marks traffic as Assured Forwarding 43 PHB (multimedia conferencing)
• cs1: Marks traffic with Class Selector 1 (low priority data). This is the default DSCP code for GTP-U payloads in UDP protocol.
• cs2: Marks traffic with Class Selector 2 (OAM)
• cs3: Marks traffic with Class Selector 3 (broadcast video)
• cs4: Marks traffic with Class Selector 4 (real-time interactive)
• cs5: Marks traffic with Class Selector 5 (signaling). This is the default DSCP code for all SCTP payloads.
• cs6: Marks traffic with Class Selector 6 (network control)
• df: Marks traffic as Default Forwarding (best effort: DSCP = 0)
• ef: Marks traffic as Expedited Forwarding PHB (telephony). This is the default DSCP code for RTCP payloads in UDP protocol.

Usage
Use this command to enable/disable the DSCP marking for data packets over IuCS/PS interface. This command assigns the DSCP levels to specific traffic patterns in order to ensure that the packets are delivered according to the precedence with which they are tagged. The Diffserv markings are applied to the IP header of every subscriber data packet transmitted over IuCS/IuPs interface(s) towards MSC/SGSN.

This command adds DSCP marking on egress traffic going towards CN (CS/PS). To make the configuration pass-through mode or not marking DSCP at all in the packets, no variant of command is used. Use of no is allowed even when there is no previous DSCP configuration done.

Important: By default this command is Disabled.

Important: When DSCP configuration is not specified, the system works in pass-through mode and DSCP values in the ingress (from CN) and egress (to HNB) data packets remain unchanged. Multiple traffic classes can share the same code point value.
Following type shown in following tables respectively:

Table 31. Supported DSCP Codes and Service Class

<table>
<thead>
<tr>
<th>Service Class</th>
<th>DSCP Code</th>
<th>Service Class</th>
<th>DSCP Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>high throughput data</td>
<td>af11</td>
<td>low priority data</td>
<td>cs1</td>
</tr>
<tr>
<td></td>
<td>af12</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>af13</td>
<td></td>
<td></td>
</tr>
<tr>
<td>low latency data</td>
<td>af21</td>
<td>OAM</td>
<td>cs2</td>
</tr>
<tr>
<td></td>
<td>af22</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>af23</td>
<td></td>
<td></td>
</tr>
<tr>
<td>multimedia streaming</td>
<td>af31</td>
<td>broadcast video</td>
<td>cs3</td>
</tr>
<tr>
<td></td>
<td>af32</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>af33</td>
<td></td>
<td></td>
</tr>
<tr>
<td>multimedia conferencing</td>
<td>af41</td>
<td>real-time interactive</td>
<td>cs4</td>
</tr>
<tr>
<td></td>
<td>af42</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>af43</td>
<td></td>
<td></td>
</tr>
<tr>
<td>best effort/ default forwarding, value zero</td>
<td>df</td>
<td>Signaling</td>
<td>cs5</td>
</tr>
<tr>
<td>telephony</td>
<td>ef</td>
<td>network control</td>
<td>cs6</td>
</tr>
</tbody>
</table>

Example

The DSCP level can be configured for multiple traffic patterns within a single instance of this command.

The following command configures the DSCP code for the SCTP IuCS/IuPS streaming traffic pattern for all payloads to be ef:

\[ \text{ip iu-qos-dscp protocol sctp payload all ef} \]
### ip iuh-qos-dscp

Enables or disables the DSCP marking parameter for control and data packets transmitted over an IuH interface towards HNB. By default this command is **Disabled**.

**Product**
HNB-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

```
configure > context context_name > hnbw-service service_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-hnbw-service)#
```

**Syntax**

```
ip iuh-qos-dscp protocol { sctp payload all | udp payload { gtpu | rtcp | rtp } } dscp_code
```

Use this keyword to set the configuration in **pass-through** mode. Use of this keyword is allowed even when there is no previous DSCP parameter set.

**Important:** In this configuration the `no` keyword does not disable/remove a previous configuration.

```
[ default | no ] ip iuh-qos-dscp protocol { sctp payload all | udp payload { gtpu | rtcp | rtp } } dscp_code
```

**default**

Enables the DSCP marking on HNB-GW and set/restores the QoS parameters to its default setting.

```
sctp payload all dscp_code
```

Specifies the QoS traffic pattern towards HNB in SCTP protocol association over IuH interface. By this keyword the Traffic classes specified by a user based on SCTP protocol and all type of payload identified based on the transport level port numbers. By default DSCP codes **cs5** is supported for all payloads in SCTP protocol.

```
udp payload { gtpu | rtcp | rtp } dscp_code
```

Specifies the QoS traffic pattern towards HNB in SCTP protocol association over IuH interface. By this keyword the Traffic classes specified by a user based on UDP protocol and GTPU, RTCP, and RTP type of payload identified based on the transport level port numbers. Default DSCP code in UDP traffic are:

- **GTP-U:** `cs1`
**rtcp**: ef
**rtp**: af41

dscp_code

Specifies the QoS DSCP codes supported for SCTP and UDP traffic and its payloads towards HNB over IuH interface. The following type of DSCP codes dscp_code are supported over IuH interface:

- **af11**: Marks traffic as Assured Forwarding 11 PHB (high throughput data)
- **af12**: Marks traffic as Assured Forwarding 12 PHB (high throughput data)
- **af13**: Marks traffic as Assured Forwarding 13 PHB (high throughput data)
- **af21**: Marks traffic as Assured Forwarding 21 PHB (low latency data)
- **af22**: Marks traffic as Assured Forwarding 22 PHB (low latency data)
- **af23**: Marks traffic as Assured Forwarding 23 PHB (low latency data)
- **af31**: Marks traffic as Assured Forwarding 31 PHB (multimedia streaming)
- **af32**: Marks traffic as Assured Forwarding 32 PHB (multimedia streaming)
- **af33**: Marks traffic as Assured Forwarding 33 PHB (multimedia streaming)
- **af41**: Marks traffic as Assured Forwarding 41 PHB (multimedia conferencing). This is the default DSCP code for RTP payloads in UDP protocol.
- **af42**: Marks traffic as Assured Forwarding 42 PHB (multimedia conferencing)
- **af43**: Marks traffic as Assured Forwarding 43 PHB (multimedia conferencing)
- **cs1**: Marks traffic with Class Selector 1 (low priority data). This is the default DSCP code for GTP-U payloads in UDP protocol.
- **cs2**: Marks traffic with Class Selector 2 (OAM)
- **cs3**: Marks traffic with Class Selector 3 (broadcast video)
- **cs4**: Marks traffic with Class Selector 4 (real-time interactive)
- **cs5**: Marks traffic with Class Selector 5 (signaling). This is the default DSCP code for all SCTP payloads.
- **cs6**: Marks traffic with Class Selector 6 (network control)
- **df**: Marks traffic as Default Forwarding (best effort: DSCP = 0)
- **ef**: Marks traffic as Expedited Forwarding PHB (telephony). This is the default DSCP code for RTCP payloads in UDP protocol.

**Usage**

Use this command to enable/disable the DSCP marking for control and data packets carried by the IP protocols and their payloads on IuH. This command assigns the DSCP levels to specific traffic patterns in order to ensure that the packets are delivered according to the precedence with which they are tagged. The DiffServ markings are applied to the IP header of every subscriber data packet transmitted over IuH interface(s) towards HNB.
This command adds DSCP marking on egress traffic going towards HNB. To make the configuration pass-through mode or not marking DSCP at all in the packets, no variant of command is used. Use of no is allowed even when there is no previous DSCP configuration done.

**Important:** By default this command is Disabled.

**Important:** When DSCP configuration is not specified, system works in pass-through mode and DSCP value in the ingress (from CN) and egress (to HNB) control and data packets remain unchanged. Multiple traffic classes can share the same code point value.

Following type shown in following tables respectively:

### Table 32. Supported DSCP Codes and Service Class

<table>
<thead>
<tr>
<th>Service Class</th>
<th>DSCP Code</th>
<th>Service Class</th>
<th>DSCP Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>high throughput data</td>
<td>af11</td>
<td>low priority data</td>
<td>cs1</td>
</tr>
<tr>
<td></td>
<td>af12</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>af13</td>
<td></td>
<td></td>
</tr>
<tr>
<td>low latency data</td>
<td>af21</td>
<td>OAM</td>
<td>cs2</td>
</tr>
<tr>
<td></td>
<td>af22</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>af23</td>
<td></td>
<td></td>
</tr>
<tr>
<td>multimedia streaming</td>
<td>af31</td>
<td>broadcast video</td>
<td>cs3</td>
</tr>
<tr>
<td></td>
<td>af32</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>af33</td>
<td></td>
<td></td>
</tr>
<tr>
<td>multimedia conferencing</td>
<td>af41</td>
<td>real-time interactive</td>
<td>cs4</td>
</tr>
<tr>
<td></td>
<td>af42</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>af43</td>
<td></td>
<td></td>
</tr>
<tr>
<td>best effort/ default forwarding, value zero</td>
<td>df</td>
<td>Signaling</td>
<td>cs5</td>
</tr>
<tr>
<td>telephony</td>
<td>ef</td>
<td>network control</td>
<td>cs6</td>
</tr>
</tbody>
</table>

The DSCP level can be configured for multiple traffic patterns within a single instance of this command.

**Example**

The following command configures the DSCP code for the SCTP IuH streaming traffic pattern for all payloads to be ef:

```
ip iuh-qos-dscp protocol sctp payload all ef
```
paging cs-domain

Configures paging optimization parameters for CS domain in the HNB-GW service instance.

Product
HNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

configure > context context_name > hnb-gw-service service_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-hnb-gw-service)#

Syntax

paging cs-domain { handle-unknown-imsi { use-cn.paging-area | use-whitelist } | phase1
page-last-known-hnb timeout timeout_val1 | phase2 paging-grid-fan-out timeout
timeout_val2 | phase3 paging-area-fan-out timeout timeout_val3 }

no paging cs-domain { handle-unknown-imsi { use-cn.paging-area | use-whitelist } | phase1
page-last-known-hnb | phase2 paging-grid-fan-out | phase3 paging-area-fan-out }

default paging cs-domain { handle-unknown-imsi { use-cn.paging-area | use-whitelist } | phase1
page-last-known-hnb timeout | phase2 paging-grid-fan-out timeout | phase3 paging-
area-fan-out timeout }

default
Sets the default behavior of paging optimization configuration for the a specific HNB-GW service.

no
Removes paging optimization configuration for an appended option in a specific HNB-GW service.

handle-unknown-imsi
Handles Unknown IMSIs Options.

use-cn.paging-area
Uses paging area provided by Core Network for forwarding the Page Req to all open/hybrid HNBs.

use-whitelist
Uses whitelist of HNBs for forwarding the Page req to all closed/hybrid HNBs.

phase1
Paging Phase1 Configuration - Forwards Page Req to last-known-hnb.
**page-last-known-hnb**
Page the last known HNB for the call.

**timeout timeout_val1**
Sets the timeout value in seconds for the last-known-hnb paging configuration. It is an integer value ranging from 1 to 30.

**phase2**
Paging Phase2 Configuration - Forwards Page Req to all HNBs in the Grid of last-known-hnb.

**paging-grid-fan-out**
Pages the last known paging grid.

**timeout_val2**
Sets the timeout value in seconds for the grid fan-out paging configuration. It is an integer value ranging from 1 to 30.

**phase3**
Paging Phase3 Configuration - Forwards Page Req to all HNBs in the LAI of last-known-hnb.

**paging-area-fan-out**
Pages the last known paging area.

**timeout_val3**
Sets the timeout value in seconds for the area fan-out paging configuration. It is an integer value ranging from 1 to 30.

**Usage**
Use this command to configure the CS domain paging optimization parameters for a specific HNB-GW service instance.

**Example**
The following command configures the CS domain paging optimization for grid fan-out timeout as 15 seconds for a specific HNB-GW service:

```
    paging cs-domain phase2 paging-grid-fan-out timeout 15
```
paging imsi-purge-timer

Configures paging optimization based on the timer for purging the unregistered IMSIs in the HNB-GW service instance.

**Product**
HNB-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

```bash
configure > context context_name > hnbgw-service service_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-hnbgw-service)#
```

**Syntax**

```bash
 paging imsi-purge-timer timeout timeout_val1
```

```bash
 default paging imsi-purge-timer timeout
```

**Usage**
Sets the default value for the IMSI purge timer as 3 hours.

```bash
 default
```

Sets the timeout value for the IMSI purge timer in hours. It is an integer ranging 1 to 12.

```bash
 timeout_val1
```

**Example**
Use this command to configure the timer value for purging the unknown IMSIs for paging optimization configuration in a specific HNB-GW service instance.

The following command configures the IMSI purge timer as 4 hours for a specific HNB-GW service instance:

```bash
 paging imsi-purge-timer timeout 4
```
paging ps-domain

Configures paging optimization parameters for PS domain in the HNB-GW service instance.

**Product**
HNB-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration
configure > context context_name > hnb-gw-service service_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-hnb-gw-service)#

**Syntax**

```
paging ps-domain { handle-unknown-imsi { use-cn-paging-area | use-whitelist } } | phase1 page-last-known-hnb timeout timeout_val1 | phase2 paging-grid-fan-out timeout timeout_val2 | phase3 paging-area-fan-out timeout timeout_val3 }

no paging ps-domain { handle-unknown-imsi [ use-cn-paging-area | use-whitelist ] } | phase1 page-last-known-hnb | phase2 paging-grid-fan-out | phase3 paging-area-fan-out }

default paging ps-domain { handle-unknown-imsi [ use-cn-paging-area | use-whitelist ] } | phase1 page-last-known-hnb timeout | phase2 paging-grid-fan-out timeout | phase3 paging-area-fan-out timeout }
```

**default**
Sets the default behavior of paging optimization configuration for the a specific HNB-GW service.

**no**
Removes paging optimization configuration for an appended option in a specific HNB-GW service.

**handle-unknown-imsi**
Handles Unknown IMSIs Options.

**use-cn-paging-area**
Uses paging area provided by Core Network for forwarding the Page Req to all open/hybrid HNBs.

**use-whitelist**
Uses whitelist of HNBs for forwarding the Page req to all closed/hybrid HNBs.

**phase1**
Paging Phase1 Configuration - Forwards Page Req to last-known-hnb.
**page-last-known-hnb**

Page the last known HNB for the call.

**timeout timeout_val1**

Sets the timeout value in seconds for the last-known-hnb paging configuration. It is an integer value ranging from 1 to 30.

**phase2**

Paging Phase2 Configuration - Forwards Page Req to all HNBs in the Grid of last-known-hnb.

**paging-grid-fan-out**

Pages the last known paging grid.

**timeout_val2**

Sets the timeout value in seconds for the grid fan-out paging configuration. It is an integer value ranging from 1 to 30.

**phase3**

Paging Phase3 Configuration - Forwards Page Req to all HNBs in the LAI of last-known-hnb.

**paging-area-fan-out**

Pages the last known paging area.

**timeout_val3**

Sets the timeout value in seconds for the area fan-out paging configuration. It is an integer value ranging from 1 to 30.

**Usage**

Use this command to configure the PS domain paging optimization parameters for a specific HNB-GW service instance.

**Example**

The following commandconfigures the PS domain paging optimization grid fan-out timeout as 20 seconds for a specific HNB-GW service:

```
paging ps-domain phase2 paging-grid-fan-out timeout 15
```
**paging open-hnb**

Configures paging optimization parameters for open HNBs connected through Open Access mode in the HNB-GW service instance. In this release it is used to configure paging optimization for Open Access mode support only. This command is deprecated release 15.0 onwards. Paging optimization can be configured using other `paging` commands available in this chapter.

**Important:** From Release 14.0 and onward this command is part of HNB-Global Configuration Mode.

**Important:** From Release 16 and later, this command has been deprecated.

**Product**

HNB-GW

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

`configure > context context_name > hnbgw-service service_name`

Entering the above command sequence results in the following prompt:

`[local]host_name(config-hnbgw-service)#`

**Syntax**

```
paging open-hnb [hnb-where-ue-registered fallback ] {always | never | only-if-with-paging-area}

default paging open-hnb
```

**default**

Sets the default behavior of paging optimization configuration for an open HNB while using Open Access mode support. By default the HNB-GW pages open HNBs only if paging-area IE is received in the paging message.

```
{always | never | only-if-with-paging-area}
```

Sets the HNB-GW service instance to page open HNB for a paging message.

**always:** Sets the system to ALWAYS page the open HNBs irrespective of paging-area IE is received in paging messages.

**never:** Sets the system to NEVER page any open HNB.

**only-if-with-paging-area:** Sets the system to page the open HNBs only when paging-area IE is received in paging messages.

```
hnb-where-ue-registered fallback {always | never | only-if-with-paging-area}
```

Sets the HNB-GW service instance to page open HNB from where the UE is registered.

**always:** Sets the system to ALWAYS page the open HNBs from where the UE is registered. If the UE is not registered then it pages the open HNBs irrespective of paging-area IE is received in paging messages.
HNB-GW Service Configuration Mode Commands

```
never: Sets the system to page the open HNBs from where the UE is registered. If the UE is not registered then it NEVER pages any open HNB.
only-if-with-paging-area: Sets the system to ALWAYS page the open HNBs from where the UE is registered. If the UE is not registered then it pages the open HNBs only when paging-area IE is received in paging messages.
```

Usage

Use this command to configure the paging optimization parameters for open HNBs connected through Open Access mode in HNB-GW service instance.

Example

The following command configures the HNB-GW service instance to page an open HNB from where the UE is connected and paging-area IE is received in paging message:

```
paging open-hnb hnb-where-ue-registered fallback only-if-with-paging-area
```
radio-network-plmn

Creates, remove and enters the HNB-RN-PLMN Configuration mode. In this mode you can configure various parameters for radio network public mobile land networks (PLMNs). A maximum of 16 radio PLMN-IDs can be configured in an HNB-GW service.

Product
HNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

configure > context context_name > hnbgw-service service_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-hnbgw-service)#

Syntax

radio-network-plmn mcc mcc_num mnc mnc_num [ -noconfirm ]

no radio-network-plmn mcc mcc_num mnc mnc_num

Removes the configured radio network PLMN identifier for an HNB-GW service.

⚠️ Caution: Removing the PLMN-ID is a disruptive operation; the HNB-GW service will be re-started.

mcc mcc_num
Specifies the mobile country code (MCC) part of radio network PLMN identifier as an integer value from 101 through 998.

mnc mnc_num
Specifies the mobile network code (MNC) part of radio network PLMN identifier as a 2- or 3-digit integer from 01 through 998.

-noconfirm
Executes the command without any additional prompt and confirmation from the user.

Usage
Use this command to configure the radio network PLMN identifier for an HNB-GW service. This command also creates a configuration mode to configure various parameters for defined radio network PLMN identifier in HNB-GW service.
Caution: Changing or removing the PLMN-ID is a disruptive operation; the HNB-GW service will be re-started.

Entering this command results in the following prompt:

```
[context_name] hostname(config-radio-network-plmn) #
```

A maximum of 16 radio network PLMN identifiers are supported for an HNB-GW service.

Example

The following command configures the radio network PLMN identifier with MCC value as 102 and MNC value as 20 for an HNB-GW service:

```
radio-network-plmn mmc 102 mnc 20
```
ranap reset

Configures various Radio Access Network (RAN) Application Part reset procedure parameters in an HNB access network.

Product
HNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration
configure > context context_name > hnbgw-service service_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-hnbgw-service)#

Syntax

ranap reset {ack-timeout timer_value | guard-timeout g_timer | hnbgw-initiated | max-retransmissions retries}

default ranap reset {ack-timeout | guard-timeout | hnbgw-initiated | max-retransmissions }

no ranap hnbgw-initiated

default
Resets the RANAP RESET parameters on HNB-GW service instance.

no
Disables the RANAP RESET procedure related parameters in an HNB-GW service instance.

ack-timeout timer_value
Sets the timer value (in seconds) to wait for Reset Acknowledge from SGSN/MSC. This is used during HNB-GW initiated RANAP RESET procedure in HNB-GW service instance.
timer_value is an integer value from 5 through 10. Default: 10

guard-timeout g_timer_value
Sets the timer value (in seconds) to send Reset Acknowledge to SGSN/MSC. After this duration the HNB-GW sends RESET-ACK to SGSN/MSC. This is used during SGSN/MSC initiated RANAP RESET procedure in HNB-GW service instance.
g_timer_value is an integer value from 5 through 10. Default: 10

hnbgw-initiated
Enables the HNB-GW Initiated RANAP RESET procedures. Default: Disabled
max-retransmission retries

Sets the maximum number of retries allowed for transmission of RESET-ACK message to SGSN/MSC. This is used during RANAP RESET procedure in HNB-GW service instance.

retries is an integer value from 0 through 2. When 0 is used retransmission is disabled. Default: 1

Usage

Use this command to configure the RANAP RESET procedure related parameters in HNB-GW service.

Example

The following command configures the HNB-GW initiated RANAP RESET Procedure for an HNB-GW service:

```bash
ranap reset hnbgw-initiated
```
**rtcp report**

Enables or disables the generation of RTP Control Protocol (RTCP) packet/report types on a per HNB-GW service instance basis. It also sets the time interval in seconds between two consecutive RTCP reports.

**Product**

HNB-GW

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

configure > context context_name > hnbw-service service_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-hnbw-service)#

**Syntax**

rtcp report interval *dur*

[ no | default ] rtcp report interval

---

**no**

Disables the RTCP report generation on HNB-GW service. When RTP configuration is not explicitly mentioned, this is the default behavior.

**default**

Restores the report interval value to its default value of 5 seconds.

**interval *dur***

Sets the time interval (in seconds) between two consecutive RTCP reports as an integer from 5 through 30. Default: 5

**Usage**

Use this command to configure the enabling or disabling of the generation of RTCP packet/report types on a per HNB-GW service instance basis and sets the specified time interval in seconds between two consecutive RTCP reports.

RTCP enables the receiver to detect if there is any packet loss and needs to compensate for any delay jitter. RTP and RTCP protocols work independently of the underlying Transport layer and Network layer protocols. Whenever this command is disabled, RTCP report generation stops from the next expiry of the previously configured interval and after enabling, reports are generated only for the calls that established as new calls in the future. For existing calls reports generated as per configuration in place.

RTCP reports are generated for each RAB for RTP received from and sent to IuH interface.

**Important:** The same interval is applicable for all kinds of RTCP packets/reports across all sessions on an HNB-GW service.
Example

The following command configures the RTCP report generation interval to 15 seconds on an HNB-GW service for RTP stream:

```bash
rtcp report interval 15
```
**rtp mux**

Configures the HNB-GW service to allow an Home-NodeB to multiplex multiple RTP streams in one IP packet. This support is provided for RTP stream management feature on HNB-GW.

**Product**

HNB-GW

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

```conf
configure > context context_name > hnbgw-service service_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-hnbgw-service)#
```

**Syntax**

```
[ no | default ] rtp mux
```

- **default**
  
  Sets the multiplexing option to default state of “disabled”.

- **no**
  
  Removes the configured option to multiplex multiple RTP stream in one packet by Home-NodeB in HNB-GW configuration.

**Usage**

Use this command to allow an Home-NodeB to multiplex multiple RTP streams in one IP packet. This configuration support is provided for RTP stream management feature on HNB-GW and it is disabled by default.

**Example**

The following command sets the HNB-GW to allow HNB to multiplex multiple RTP stream in one packet:

```
rtp mux
```
sctp bind

Configures the SCTP IP address and port that is used for binding the SCTP socket to communicate with the Home-NodeB over an Iuh interface within an HNB-GW service.

**Product**
HNB-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

```
configure > context context_name > hnbgw-service service_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-hnbgw-service)#
```

**Syntax**

```
sctp bind { address address | port port_num }

[ no ] sctp bind { address | port }
```

- **no**
  Removes the SCTP binding.

- **address address**
  Specifies the IP address of the HNB-GW Iuh interface in IPv4 dotted-decimal.

- **port port_num**
  Specifies the SCTP port number to communicate with the Home-NodeBs using Iuh interface as an integer form 1 through 65535.

**Usage**

Use this command to assign the SCTP IP address and port with SCTP socket on HNB-GW to communicate with the Home-NodeB using Iuh interface. This SCTP configuration provides the IP-address and listen port where HNB-GW service shall bind to listen for incoming SCTP associations from HNB.

**Example**

The following command sets the SCTP port number 999 on HNB-GW to listen from Home-NodeB over Iuh interface:

```
sctp bind port 999
```

The following command sets the SCTP address 10.2.3.4 of HNB-GW to use with Home-NodeB over Iuh interface:

```
sctp bind address 10.2.3.4
```
sctp checksum-type

Configures SCTP checksum-type.

Product
HNB-GW

Privilege
Security Administrator, Administrator

Syntax

sctp checksum-type { adler32 | crc32 }

default sctp checksum-type

Usage
Use this command to configure SCTP checksum-type.

Example

The following command sets the SCTP checksum-type to adler32 on HNB-GW:

    sctp checksum-type adler32
sctp connection-timeout

Configures the SCTP connection timeout duration to explicitly remove the SCTP association with a non-responsive HNB in an HNB-GW service.

**Product**
HNB-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration
`configure > context context_name > hnbgw-service service_name`

Entering the above command sequence results in the following prompt:

`[local]host_name(config-hnbgw-service)#`

**Syntax**

```
sctp connection-timeout dur
[ default | no ] sctp connection-timeout
```

- **no**
  Disables the connection time out configuration on HNB-GW service.

- **default**
  Restores the connection timeout duration value to its default value of 10 seconds.

- **dur**
  Sets the connection timeout duration (in seconds) after which the association is explicitly removed. In case of an HNB de-registration scenario, the HNB-GW waits for configured amount time before initiating the procedure to clear the SCTP association.
  `dur` is an integer from 5 through 30. Default: 10

**Usage**

Use this command to configure the minimum duration value before removing the SCTP association between a non-responding HNB and HNB-GW. If HNB registration not happened within the configured period after the SCTP association is established then the SCTP association is explicitly removed. In a scenario where an HNB de-registered due to any reason, the HNB-GW waits for the configured amount of time before initiating the procedure to clear the SCTP association.

**Example**

The following command sets the SCTP connection timeout duration to 15 seconds on HNB-GW after expiry of which the SCTP association is removed:

```
sctp connection-timeout 15
```
sctp cookie-life

Configures the SCTP valid cookie-life, Min 5000ms and Max 120000ms with granularity of 100ms.

Product
HNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

```
configure > context context_name > hnbgw-service service_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-hnbgw-service)#
```

Syntax

```
sctp cookie-life dur
```

```
default sctp cookie-life
```

```
default
```

Restores the SCTP cookie-life value.

```
dur
```

Sets the SCTP cookie-life (in seconds).

```
dur is an integer from 50 through 1200.
```

Usage

Use this command to configure the SCTP valid cookie-life.

Example

The following command sets the SCTP cookie-life value to 55 on HNB-GW:

```
sctp cookie-life 55
```
**sctp heart-beat-timeout**

Configures the SCTP heartbeat timer parameters for SCTP connection over an IuH interface in an HNB-GW service instance.

**Product**
HNB-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

`configure > context context_name > hnbgw-service service_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-hnbgw-service)#
```

**Syntax**

```
sctp heart-beat-timeout dur

[ default | no ] sctp heart-beat-timeout
```

- **no**
  Disables the heartbeat timer configuration for SCTP over IuH in HNB-GW service instance.

- **default**
  Restores the default time out value for heartbeat timer to 30 seconds.

- **dur**
  Sets the heartbeat timer timeout duration (in seconds) after which the next heartbeat command is sent to HNB from HNB-GW in SCTP over an IuH interface. In an HNB de-registration scenario, the HNB-GW waits for configured amount time before initiating the procedure to clear the SCTP association. `dur` is an integer from 1 through 300. Default: 30

**Usage**

Use this command to configure the minimum duration value before retransmitting the HEARTBEAT chunk to HNB from HNB-GW in SCTP transmission. By default HNB-GW monitors the reachability of the idle HNBs by sending a HEARTBEAT chunk periodically to the HNB address. Each time the HEARTBEAT timer expires on any address, or when a HEARTBEAT sent to an idle address is not acknowledged within a Retransmission Timeout duration, the error counter of that HNB incremented. When the value in the error counter exceeds the protocol parameter for maximum retransmission for that destination address, the HNB-GW mark the destination HNB as inactive and a notification is sent to the upper layer.

**Example**

The following command sets the SCTP HEARTBEAT timeout duration to 15 seconds on HNB-GW after expiry of which the HNB-GW retransmits the HEARTBAT chunk to HNB over SCTP association:
sctp heart-beat-timeout 15
sctp mtu-size

This command configures SCTP mtu-size, Min 508 bytes and Max is 65535 bytes with granularity of 1 byte.

Product
HNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

configure > context context_name > hnbgw-service service_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-hnbgw-service)#

Syntax

sctp mtu-size { max | min | start } size

default sctp mtu-size { max | min | start }

default

Sets the SCTP mtu-size to its default value.

size

size is an integer from 508 through 65535.

Usage

Use this command to configure the SCTP mtu-size.

Example

The following command configures the SCTP mtu-size max value to 555 on HNB-GW:

sctp mtu-size max 555
sctp rto

This command sets the SCTP Retransmission Timeout value.

Product
HNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration
configure > context context_name > hnbw-service service_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-hnbw-service)#

Syntax

sctp rto { initial initial_value | max max_value | min min_value }

default sctp rto { initial | max | min }

default
Sets the SCTP Retransmission Timeout value to default.

initial_value
initial_value is SCTP Retransmission Timeout initial value, which is an integer from 1 through 1200.

max_value
max_value is SCTP Retransmission Timeout max value (Min 500 ms and max 120000 ms with granularity of 100 ms), which is an integer from 5 through 1200.

min_value
min_value is SCTP Retransmission Timeout max value (Min 100 ms and max 5000 ms with granularity of 100 ms), which is an integer from 1 through 50.

Usage
Use this command to set the SCTP Retransmission Timeout value.

Example
The following command sets the SCTP max Retransmission Timeout value to 555 on HNB-GW:

sctp rto max 555
sctp sack-frequency

This command configures the SCTP Selective Ack Frequency.

Product
HNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration
configure > context context_name > hnbgw-service service_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-hnbgw-service)#

Syntax

sctp sack-frequency value

default sctp sack-frequency

- default
  Sets the SCTP sack-frequency value to default.

- value
  Min value is 1 and Max value is 5.
  value is an integer from 1 through 5.

Usage
Use this command to configure the SCTP Selective Ack Frequency.

Example
The following command configure the SCTP Selective Ack Frequency to 5 on HNB-GW:

```
sctp sack-frequency 55
```
sctp sack-period

This command is used to configure SCTP Selective Ack Period in Seconds.

Product
HNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

configure > context context_name > hnbgw-service service_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-hnbgw-service)#

Syntax

**sctp sack-period** value

default sctp sack-period

default

Sets the SCTP sack-period value to default.

value

Min 0 ms and Max is 500ms with granularity of 100ms.

Value is an integer from 0 through 5.

Usage

Use this command to configure the SCTP Selective Ack Period in Seconds.

Example

The following command configures the SCTP Selective Ack Period in Seconds to 5 on HNB-GW:

```
sctp sack-period 55
```
security-gateway bind

Binds the SeGW in an HNB-GW service to a logical IP interface serving as an Iuh interface and associates an IPsec IKEv2 crypto-map template.

Product
HNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

configure > context context_name > hnbgw-service service_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-hnbgw-service)#

Syntax

security-gateway bind address address crypto-template cryp_name [ context ctx_name]

no security-gateway bind

no

Removes a previously configured IPsec IP address use for binding the IKEv2 IPSec tunnel (local bind address) to communicate with the Home-NodeBs using Iuh interface.

bind address address

Specifies the IP address for the Iuh interface for the IPSec tunnel. This is the IP address where the HNB-GW service is bound and that is provided to the Home-NodeB during HNB-GW discovery. The IP address is expressed in IPv4 dotted-decimal.

crypto-template cryp_name

Specifies the Crypto-map template to be used for IPsec IKEv2 tunneling for the interface configured as an Iuh.

cryp_name specifies the name of the pre-configured Crypto-map template which is configured in Crypto-Map Template Configuration mode and associated with the HNB-GW service to create an IPSec tunnel with a Home-NodeB during HNB-GW discovery procedure over an Iuh interface.

context ctx_name

Specifies the name of the pre-configured context in which the Security Gateway service is configured. By default this command uses the HNB-GW service context for the security Gateway configuration.

Usage

Use this command to associate or tie the HNB-GW service to a specific logical IP address that is used for binding the Iuh socket to communicate with the Home-NodeB using IPSec tunnel. A maximum of one IP address can be configured with this command for one HNB-GW service.
The HNB-GW passes the IP address during setting up the HNB-GW discovery procedure with the Home-NodeB.

⚠️ **Caution:** This is a critical configuration. The HNB-GW service cannot be started without this configuration. Any change to this configuration would lead to restarting the HNB-GW service and removing or disabling this configuration stops the HNB-GW service.

**Example**

The following command binds the logical IP interface with the address of 10.2.3.4 to the HNB-GW service using existing IPsec Crypto-Map template `crypto1` to establish IPSec tunnel with Home-NodeB:

```
security-gateway bind address 10.2.3.4 crypto-template crypto1
```

The following command disables a binding that was previously configured:

```
security-gateway bind address
```
**sessmgr-to-cbsmgr-pacing-timer**

This command configures pacing timer value for SABP messages being sent from Sessmgr to CBSmgr. Default value is 100ms.

**Product**
HNB-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

`configure > context context_name > hnbgw-service service_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-hnbgw-service)#
```

**Syntax**

```
(sessmgr-to-cbsmgr-pacing-timer miliseconds)
```

**Usage**
Pacing timer value in miliseconds which is an integer from 10 through 500.

**Example**

Use this command to configure pacing timer value for SABP messages being sent from Sessmgr to CBSmgr.

The following command sets pacing timer value for SABP messages being sent from Sessmgr to CBSmgr to 50:

```
(sessmgr-to-cbsmgr-pacing-timer 50)
```
tnnsf-timer

Configures the NAS Node Selection Function (NNSF) timer (T-NNSF) which is used by the HNB-GW to store the IMSI and the relevant Global-CN-ID in the short term after Paging. This timer is used for Iu-Flex feature support.

**Product**
HNB-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration

```bash
configure > context context_name > hnbw-service service_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-hnbw-service)#
```

**Syntax**

```
tnnsf-timer dur
[no | default] tnnsf-timer
```

- **no**
  Disables/removes the configured timer value of NNSF timer (T-NNSF) from HNB-GW service instance.

- **default**
  Sets the timer value of NNSF timer (T-NNSF) for HNB-GW service instance to default value of 30 seconds.

```
 tnnsf-timer dur
```

Configures the NNSF timer (in seconds) which is used by the HNB-GW to store the IMSI and the relevant Global-CN-ID as an integer from 10 through 60. Default: 30

**Usage**

Use this command to configure the NNSF timer value in seconds for Iu-Flex support. Whenever the MSC sends the paging request with IMSI, the HNB-GW stores the Global_CN_ID of the node which issued the paging request message for the given IMSI and HNB-GW starts the tnnsf-timer. HNBGW stores the mapping of IMSI to Global_CN_ID until the tnnsf-timer expires

**Example**

The following command sets the NNSF timer value to 30 seconds in an HNB-GW service instance:

```
default tnnsf-timer
```
ue registration-timeout

Configures the UE registration timeout duration to de-register the connected UE from an HNB-GW service.

Product
- HNB-GW

Privilege
- Security Administrator, Administrator

Mode
- Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration
- configure > context context_name > hnbgw-service service_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-hnbgw-service)#

Syntax

```
ue registration-timeout dur
[ default | no ] ue registration-timeout
```

- **no**
  Disables the UE registration timeout duration and explicitly de-registers UE from the HNB-GW service.

- **default**
  Restores the UE registration timeout duration value to its default value of 120 seconds.

- **dur**
  Sets the UE registration timeout duration (in seconds) after which the UE is de-registered from HNB-GW. In a scenario when all Iu connections are released for a subscriber, the HNB-GW service de-registers the UE after the configured duration only.
  
  `dur` is an integer from 60 through 300. Default: 120

Usage

Use this command to configure the minimum duration value before de-registering the UE when subscriber fails to establish the Iu connection. If subscriber’s Iu session does not established before configured period then UE is de-registered. Also in a scenario where all Iu connections are released for a subscriber, the HNB-GW service waits for configured period before starting UE deregistration procedure.

Example

The following command sets the UE registration timeout duration to 150 second on HNB-GW after expiry of which the UE is de-registered:

```
ue registration-timeout 150
```
Chapter 166
HNB-PS Network Configuration Mode Commands

The HNB-PS Network Configuration Mode is used to manage the packet switched (PS) network instance on HNB-GW service to provide HNB access with the PS core network in a 3G UMTS network.

Mode

Exec > Global Configuration > HNB-PS Network Configuration

configure > ps-network ps_instance

Entering the above command sequence results in the following prompt:

[local]host_name(config-ps-network-instance_id)#

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
**associate gtpu-service**

Associates a previously configured GTP-U service to provide a GTP-U tunnel with an SGSN towards the core network side. A GTP-U service must be configured in Context Configuration mode before using this configuration.

**Product**
HNB-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > HNB-PS Network Configuration

configure > ps-network ps_instance

Entering the above command sequence results in the following prompt:

[local] host_name(config-ps-network-instance_id) #

**Syntax**

```
associate gtpu-service svc_name context ctx_name
```

```
no associate gtpu-service
```

**Usage**

Use this command to configure GTP-U data plan tunnel between HNB-GW service and GSNs in core network. The service defined for GTP-U tunnel must be configured in Context configuration mode.

**Important:** Another GTP-U service can be used to bind the HNB-GW service to GTP-U tunnel with HNB in HNB access network and can be configured in HNB-GW Service Configuration mode. For more information on GTP-U service configuration, refer to *GTP-U Service Configuration Mode Commands* chapter.

**Example**

The following command associates GTP-U service *gtpu_svc1* configured in context named *Ctx_gtpu1* with specific HNB-PS network instance for GTP-U tunnel towards GSN in core network:

```
associate gtpu-service gtpu_svc1 context Ctx_gtpu1
```
**associate-sccp-network**

Associates a previously defined Signaling Connection Control Part (SCCP) network identifier with the PS network instance in order to route the messages towards the SGSN via the IuPS interface.

**Product**
HNB-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > HNB-PS Network Configuration
configure > ps-network ps_instance

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ps-network-instance_id)#
```

**Syntax**

```
associate-sccp-network sccp_net_id

no associate-sccp-network
```

**no**
Removes the associated SCCP network configuration instance from this HNB-PS network instance configuration.

```
sccp_net_id
```
Specifies a predefined SCCP network identifier.

**Usage**

Use this command to associate a predefined SCCP network ID with the IuPS interface in HNB-GW service to connect with PS network elements; i.e. SGSN.

**Important:** The SCCP network ID must be defined in Global Configuration mode before using it with this command.

**Important:** A single SCCP network ID can not be shared with multiple HNB-PS network instances.

**Example**

The following command associates SCCP network ID 2 with specific HNB-PS network instance:

```
associate-sccp-network 2
```
**end**

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
ALL

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Use this command to return to the parent configuration mode.
global-rnc-id

Configures the Radio Network Concentrator (RNC) identifier in a Radio Network PLMN associated with HNB-PS network configuration instance. The RNC identifier is provided to the HNB during HNB-REGISTRATION.

**Product**
HNB-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > HNB-PS Network Configuration
c
configure > ps-network ps_instance

Entering the above command sequence results in the following prompt:

[local]host_name(config-ps-network-instance_id)#

**Syntax**

```
[ no ] global-rnc-id  mcc  mcc_num  mnc  mnc_num  id  rnc_id  [ common-plmn  mcc  mcc_num  mnc  mnc_num ]
```

- **no**
  Deletes the RNC, MMC, and MNC information from the HNB-PS Network configuration instance.

- **mcc  mcc_num**
  Specifies the mobile country code (MCC) part of radio network PLMN identifier as an integer value from 100 through 999.

- **mnc  mnc_num**
  Specifies the mobile network code (MNC) part of radio network PLMN identifier as a 2- or 3-digit integer from 00 through 999.

- **id  rnc_id**
  Specifies the RNC identifier as an integer from 0 through 4095.

- **common-plmn  mcc  mcc_num  mnc  mnc_num**
  Configures the Common PLMN for this PS Network.
  **mcc  mcc_num** configures the MCC of Common PLMN for this PS Network as an integer value from 100 through 999.
  **mnc  mnc_num** configures the MNC of Common PLMN for this PS Network as a 2- or 3-digit integer from 00 through 999.
Usage

Use this command to configure RNC id to associate Radio Network PLMN which will be sent to HNBs from HNB-GW during HNB-REGISTRATION procedure. Depending upon the requirement the RNC Identifier can be provided at the desired granularity.

Example

The following command configures the HNB-GW service to return an RNC identifier as 102 when an HNB-REGISTRATION request is received with LAC 1, and RAC 2:

```
global rnc-id mcc 102 mnc 02 id 2
```
map core-network-id

Maps/associates the PS core network identifier to a default SGSN in the network using an SGSN point code to allow HNBs to access the UMTS network.

**Product**
HNB-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > HNB-PS Network Configuration
configure > ps-network ps_instance

Entering the above command sequence results in the following prompt:

[local] host_name(config-ps-network-instance_id)#

**Syntax**

map core-network-id cn_id point-code sgsn_point_code

no map core-network-id cn_id

no
Removes the mapping of a PS core network id with particular SGSN point code.

**cn_id**
Specifies the core network identifier configured to represent a UMTS PS core network as an integer from 0 through 4095.
Multiple instance of this command can be mapped with different SGSN point codes.

**point-code sgsn_point_code**
Specifies the SS7 address of the default SGSN in the PS network.
point_code is an SS7 point code in dotted-decimal ###.###.### or 8-digit decimal ####### format.
Only one instance of this SGSN point code can be mapped with one PS core network identifier.

**Usage**
Use this command to map a UMTS PS core network identifier with a particular SGSN point code.
This command can be entered multiple times with same SGSN point code to map with one or more PS core network Id, but a particular core network identifier can be mapped to one SGSN only.
This command is instrumental in Iu-Flex functionality, whenever HNB-GW receives RESET/RESET-RES messages from SGSN with Global CN-ID information element, the response from HNB-GW is sent to the node configured for that particular Global CN-ID.
If the RESET/RESET-RES messages do not have Global CN-ID IE, then the response of those messages is directed to the default SGSN which is configured using sgsn point-code command in this mode.

**Example**
The following command configures the PS core network identifier 101 with an SGSN point code 1.2.3:
map core-network-id 101 point-code 1.2.3

The following command configures the PS core network identifier 102 with the same SGSN point code 1.2.3:

map core-network-id 102 point-code 1.2.3
map idnns range

Configures the mapping of an Intra-Domain NAS Node Selector (IDNNS) IE received from UE in an RUA connect message towards HNB-GW. This is an important configuration for PS network resource sharing over an Iu-Flex interface.

Product
HNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > HNB-PS Network Configuration

configure > ps-network ps_instance

Entering the above command sequence results in the following prompt:

[local] host_name(config-ps-network-instance_id) #

Syntax

map idnns range idnns_start to idnns_end point-code sgsn_point_code [backup point-code bkup_sgsn_point_code]

no map idnns range idnns_start to idnns_end

no

Removes the entries of mapping of range of IDNNS received from UE with particular SGSN point code.

range idnns_start to idnns_end

Specifies the range of IDNNSs received from UE to map with particular SGSN point codes during the initial PS core network node selection.

idnns_start is an integer from 0 through 1023 that should be less than idnns_end.

idnns_end is an integer from 0 through 1023 that should be more than idnns_start.

The command can be entered more than once to map multiple IDNNS ranges to the same SGSN. However, overlapping and mapping of the same range to different SGSN point codes is not allowed.

point-code sgsn_point_code

Specifies the SS7 address of the SGSN in the PS network.

sgsn_point_code is an SS7 point code in dotted-decimal ###.###.### or 8-digit decimal ######## format.

backup point-code bkup_sgsn_point_code

Specifies the SS7 address of the SGSN to be used as the backup in the PS network.

bkup_sgsn_point_code is an SS7 point code in dotted-decimal ###.###.### or 8-digit decimal ######## format.
Usage

Use this command to map a NRI received from UE during initial PS network node selection to SGSN point code through NRI range mapping over Iu-Flex interface.

The IDNNS refers to the information element in RUA connect message from UE towards RAN (HNB-GW). In IDNNS IE, if the choice of routing mentioned is other than local P-TMSI, then the value it provides is used against this configuration to map the SGSN point code.

If backup SGSN point-code is specified, then specified SGSN works as backup for the IDNS range configured. This Backup SGSN is selected if the mapped SGSN for a given IDNNS range is going for offloading using `offload-sgsn point-code` command.

The command can be entered more than once to map multiple IDNNS ranges to same SGSN point code, but overlapping and mapping of same range to different SGSN point code is not allowed.

Example

The following command maps the IDNNS range from 101 to 201 with SGSN point code 1.2.3 and point code 7.8.9 as backup SGSN point code:

```
map nri range 101 to 201 point-code 1.2.3 backup point-code 7.8.9
```

The following command removes all IDNNS range matching entries between 301 to 399 from the configuration:

```
no map idnns range 301 to 399
```
map nri range

Configures the mapping of the Network Resource Identifier (NRI) received from UE to an SGSN point code. This is an important configuration for PS network resource sharing over Iu-Flex interface.

Product
HNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > HNB-PS Network Configuration
   configure > ps-network ps_instance

Entering the above command sequence results in the following prompt:

[local]host_name(config-ps-network-instance_id)#

Syntax

map nri range nri_start to nri_end point-code sgsn_point_code

no map nri range nri_start to nri_end

no
Removes the entries of mapping of range of NRIs received from UE with a particular SGSN point code.

range nri_start to nri_end

Specifies the range of NRIs received from UE to map with a particular SGSN point code during initial PS core network node selection.

nri_start is an integer from 0 through 1023 that should be less than nri_end.
nri_end is an integer from 0 through 1023 that should be more than nri_start.
The command can be entered more than once to map multiple NRI ranges to the same SGSN, but overlapping is not allowed.

point-code sgsn_point_code

Specifies the SS7 address of the SGSN in the PS network to map with range of NRI values.
point_code is an SS7 point code in dotted-decimal ###.###.### or 8-digit decimal ####### format.

Usage

Use this command to map a NRI received from UE during initial PS network node selection to SGSN point code through NRI range mapping over Iu-Flex interface.
This configuration is used during initial PS core network node selection when the network resource identifier (NRI) from the UE is available. The NRI range is mapped to SGSN point code. This configuration is used when the core network uses Iu-Flex interface.
The command can be entered more than once to map multiple NRI ranges to same SGSN point code.
It is possible to configure multiple ranges to more than one SGSN however this configuration is required only when the PS core network is configured as Multi-Operator Core Network (MOCN).
When the PS core network is not MOCN and one range is mapped to more than one SGSN then SGSN is selected randomly in a non-predictable manner.

### Example

The following command maps the NRI range from 101 to 201 with SGSN point code 1.2.3:

```plaintext
map nri range 101 to 201 point-code 1.2.3
```

The following command maps the NRI range from 301 to 399 with SGSN point code 1.2.3:

```plaintext
map nri range 301 to 399 point-code 1.2.3
```

The following command removes all NRI range matching entries between 301 to 399 from the configuration:

```plaintext
no map nri range 301 to 399
```
nri length

Configures the network resource identifier (NRI) length in bits to identify a specific SGSN serving in a pooled area. At least one NRI value must be assigned to an SGSN serving in a pool. The NRI is coded inside of the temporary mobile subscriber identity (TMSI), located within bits 14 to 23 with a variable length between 0 and 10 bits. The operator must set this NRI length to indicate the number of bits that shall be used for the NRI field to set the parameters for Iu-Flex (SGSN pooling) functionality.

Product
HNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > HNB-PS Network Configuration
  configure > ps-network ps_instance
Entering the above command sequence results in the following prompt:

[local]host_name(config-ps-network-instance_id)#

Syntax

nri length nri_value

default nri length

    default
    Sets the NRI length to default value of 0 and disables the Iu-Flex (SGSN pooling) functionality.

    nri length nri_length

    Default: 0
    Specifies the number of bits to be used in the P-TMS (bits 23 to 18) to define the network resource identifier (NRI). The NRI length configuration also sets the maximum size of the pool. If not configured, the NRI length is set to zero length.
    length is an integer from 1 to 10. When a non-zero value is configured the PS network is considered to be a pool. Default: 0

Usage

Use this command to enable the Iu-Flex functionality on HNB-GW. This command identifies a unique SGSN serving a pooled area for Iu-Flex functionality and at least one NRI value has to assigned to an SGSN serving in a pool. It performs SGSN pooling/offloading scenario over Iu-Flex interface. The NRI is stored in the bits 14 to 23 of TMSI. The HNB-GW uses a portion of this NRI to set the parameters for Iu-Flex (SGSN pooling) functionality.

If more than one NRI is configured, the HNB-GW service does round-robin between the available NRIs when new subscriber(s) (re)connect.

This command must be used in conjunction with null nri command to configured SGSN pooling/offloading over Iu-Flex interface.

Example
The following command sets the HNB-GW to use bit length as 6 to derive the values from the NRI field (stored in the bits 14 to 23 of TMSI) to set the parameters for Iu-Flex (SGSN pooling) functionality:

```
nri length 6
```
null-nri

Configures the null network resource identifier (NRI) for load redistribution in support of Iu-Flex functionality. The NRI value defined with this command must be unique across the pool areas. This null-NRI is used by HNB-GW for load redistribution during SGSN offloading.

Product
HNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > HNB-PS Network Configuration

configure > ps-network ps_instance

Entering the above command sequence results in the following prompt:

[local]host_name(config-ps-network-instance_id)#

Syntax

null-nri null_nri_value

no null-nri null_nri_value

Usage

Use this command to identify the SGSN by HNB-GW to be used for load redistribution during SGSN offloading over Iu-Flex interface.

Without MOCN configuration this command can be entered only once. In case of MOCN a unique null-NRI must be assigned to each MOCN operator identify by its PLMN-id (MCC+MNC).

Example

The following command sets the null-NRI as 1001 to be used by HNB-GW for load redistribution during SGSN offloading:

null-nri 1001
offload-sgsn

Enables or disables the exclusion of a specified primary SGSN node during the NAS Node Selection Function (NNSF) procedure when it needs to be offloaded using Iu-Flex functionality.

Product
HNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > HNB-PS Network Configuration
configure > ps-network ps_instance

Entering the above command sequence results in the following prompt:

[local]host_name(config-ps-network-instance_id)#

Syntax

[ no ] offload-sgsn point-code sgsn_point_code

no

Removes the specified primary SGSN point code from the exclusion list for NNSF function on HNB-GW and re-enables the inclusion of the primary SGSN node to be considered by HNB-GW.

point-code sgsn_point_code

Specifies SS7 address of primary SGSN in PS network having specific point code value to be excluded for NNSF function on HNB-GW when it needs to be offloaded in Iu-Flex functionality.

point_code is an SS7 point code in dotted-decimal ###.###.### or 8-digit decimal ###### format. Only one instance of this primary SGSN point code can be mapped with one PS core network id.

Usage

Use this command to provision the HNB-GW to enable or disable the exclusion of the SGSN node when it needs to be offloaded.

When this command is enabled for exclusion of SGSN node during NNSF function in HNB-GW, the HNB-GW excludes the particular node from being considered.

User can re-enable the inclusion of the SGSN node to be considered for NNSF functionality by no

offload-sgsn point-code command.

Important: The offload check is only for the primary point code and NOT for the backup point code.

Example

This command can be used for planned maintenance as well.

The following command configures the HNB-GW to exclude the primary SGSN point code 1.2.3 from being considered in NSSF function for Iu-Flex support:

offload-sgsn point-code 1.2.3
The following command re-enables the inclusion of SGSN point code 1.2.3 from being considered in NSSF function for Iu-Flex support:

```
no offload-sgsn point-code 1.2.3
```
**ranap reset**

Configures various Radio Access Network (RAN) Application Part reset procedure parameters for PS network association in an HNB access network.

**Product**
HNB-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > HNB-PS Network Configuration
configure > ps-network ps_instance

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ps-network-instance_id)#
```

**Syntax**

```
ranap reset { ack-timeout timer_value | guard-timeout g_timer | hnbwg-initiated | max-retransmissions retries }

default ranap reset { ack-timeout | guard-timeout | hnbwg-initiated | max-retransmissions }

no ranap { hnbwg-initiated }
```

---

**default**

Resets the RANAP RESET parameters in HNB-PS Network configuration instance.

**no**

Disables the RANAP RESET procedure related parameters in an HNB-PS Network configuration instance.

**ack-timeout timer_value**

Sets the timer value (in seconds) to wait for Reset Acknowledge from SGSN. This is used during HNB-GW initiated RANAP RESET procedure in HNB-PS Network configuration instance.

*timer_value* is an integer value from 5 through 10. Default: 10

**guard-timeout g_timer_value**

Sets the timer value (in seconds) to send Reset Acknowledge to SGSN. After this duration the HNB-GW sends RESET-ACK to SGSN. This is used during SGSN initiated RANAP RESET procedure in HNB-PS Network configuration instance.

*g_timer_value* is an integer value from 5 through 10. Default: 10

**hnbgw-initiated**

Enables the HNB-GW Initiated RANAP RESET procedures. Default: Disabled
max-retransmission retries

Sets the maximum number of retries allowed for transmission of RESET-ACK message to SGSN. This is used during RANAP RESET procedure in HNB-PS Network configuration instance.

retries is an integer value from 0 through 2. When 0 is used retransmission is disabled. Default: 1

Usage

Use this command to configure the RANAP RESET procedure related parameters in HNB-PS Network configuration for multiple HNB-GW service support.

Example

The following command configures the HNB-GW initiated RANAP RESET Procedure for an HNB-PS Network configuration instance:

    ranap reset hnbgw-initiated
sgsn deadtime

Configures a timer on HNB-GW to manage SGSN availability in a PS core network on receiving of a PC-STATE-DOWN or SSN-STATE-DOWN (RANAP) indication from SCCP.

Product
HNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > HNB-PS Network Configuration

configure > ps-network ps_instance

Entering the above command sequence results in the following prompt:

[local]host_name(config-ps-network-instance_id)#

Syntax

sgsn deadtime { immediate | dur }

[ no | default ] sgsn deadtime

---

no

Makes the peer node (SGSN) always available for all HNB-PS network instances.

---

default

Sets the default action for HNB-GW such that the peer node (SGSN) is marked down as soon as HNB-GW receives a PC-STATE-DOWN or SSN-STATE-DOWN (RANAP) indication from SCCP in a specific HNB-PS network instance. Default: Enabled

---

immediate

Sets the HNB-GW to mark the peer node (SGSN) down immediately and clears all Iu-PS connections towards the SGSN. Default: Disabled

---

dur

Sets the duration (in seconds) for a timer which starts once HNB-GW receives a PC-STATE-DOWN or SSN-STATE-DOWN (RANAP) indication from SCCP for a peer SGSN. On expiry of this timer the peer SGSN is marked as dead and all Iu-PS connections towards that SGSN are released.

dur is an integer from 1 through 30.

Only one instance of this command can be configured.

Usage

This command is used to configure a timer on HNB-GW to manage SGSN availability in a PS core network on receiving of PC-STATE-DOWN or SSN-STATE-DOWN (RANAP) indication from SCCP.
Timer value sets the duration in seconds for a timer which started once HNB-GW receives PC-STATE-DOWN or SSN-STATE-DOWN (RANAP) indication from SCCP for a peer SGSN. On expiry of this timer the peer SGSN is marked as dead and all Iu-PS connections towards that SGSN shall be released.

**Important:** This command can be entered only once. Reentering this command overwrites the previous parameters.

**Example**

The following command configures the deadtime timer value for 10 seconds on HNB-GW. Once HNB-GW receives PC-STATE-DOWN or SSN-STATE-DOWN (RANAP) indication from SCCP for a peer SGSN the HNB-GW waits for configured period and on expiry of timer it marks the specific SGSN as dead:

```
sgsn deadtime 10
```
sgsn point-code

Configures the default SGSN point-code with the HNB-PS network instance. This command is used when HNB-GW is to be connected to only one SGSN with in a PS network or as the default SGSN for all HNBs connected through specific HNB-PS network instance.

Product
HNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > HNB-PS Network Configuration

configure > ps-network ps_instance

Entering the above command sequence results in the following prompt:

[local]host_name(config-ps-network-instance_id)#

Syntax

[ no ] sgsn point-code point_code

- **no**
  - Removes the configured default SGSN point code from specific HNB-PS network instance.

⚠️ **Caution:** Removing the SGSN point code is a disruptive operation and affects all HNB sessions which are connected to particular SGSN through an HNB-PS network instance.

- **point_code**
  - Specifies the SS7 address of the default SGSN in a PS network.
  - *point_code* is an SS7 point code in dotted-decimal ###.###.## or 8-digit decimal ####### format.
  - Only one instance of this command can be configured.

Usage

Use this command to configure a default SGSN to which HNB connects for PS network access through the HNB-GW service.

Point-code is an SS7 address for an element in the SS7 network. Point-codes must be defined in dotted-decimal format in a string of 1 to 11 digits. Format options include:

- 0.0.1 to 7.255.7 for point-code in the ITU range.
- 0.0.1 to 255.255.255 for point-code in the ANSI range.
- 0.0.1 to 15.31.255 for point-code in the TTC Range.
- A string of 1 to 11 digits in dotted-decimal to represent a point-code in a different range.

⚠️ **Important:** This command can be entered only once. If entered again the previous value shall be overwritten.

Example
The following command configures a default SGSN with point code 101.201.101 for HNBs to access PS network through HNB-GW service in this HNB-PS network instance:

```
sgsn point-code 101.201.101
```
Chapter 167
HNB-RN PLMN Configuration Mode Commands

This HNB Radio Network PLMN configuration mode defines the radio network PLMN parameters related to the HNB-GW connection with a UMTS Femto radio network.

Mode

Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration > HNB-RN PLMN Configuration

configure > context context_name > hnbgw-service service_name > radio-network-plmn mcc mcc_number mnc mnc_number

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-hnbgw-radio-plmn)#

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
associate cs-network

From StarOS Release 14.0 onward this command is deprecated.
associate ps-network

From StarOS Release 14.0 onward this command is deprecated.
**authorised-macro-lai**

Configures the macro LAI based authorization parameters for this HNB-GW service.

**Product**
HNB-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration > HNB-RN PLMN Configuration

```bash
configure > context context_name > hnbw-service service_name > radio-network-plmn mcc mcc_number mnc mnc_number
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-hnbw-radio-plmn)#
```

**Syntax**

```bash
authorised-macro-lai { macro-info-ie-absent-action { accept | reject } | mcc mcc_id mnc mnc_id lac range range_from to range_to }

default authorised-macro-lai macro-info-ie-absent-action

no authorised-macro-lai mcc mcc_id mnc mnc_id lac range range_from to range_to
```

**default**
Configures the default parameters for macro LAI based authorization for the system configuration. Default action is to reject HNB if IE is absent.

**no**
Deletes the macro LAI based authorization parameters from the system configuration.

**mcc-id**
Specifies the MCC of pre-configured macro lai range for HNB authorization as a number, ranging from 100..999

**mnc-id**
Specifies the MNC of pre-configured macro lai range for HNB authorization, ranging from 00..999

**lac range**
Specifies the LAC of pre-configured macro LAI range for HNB authorization.

**range_from**
Specifies the LAC range minimum value, which is an integer from 0..65535.
**range_to**

Specifies the LAC range maximum value, which is also an integer from 0..65535.

---

**Usage**

Use this command to configure the macro LAI based authorization parameters for an existing HNB-GW service.

**Example**

The following command configures the default action for macro LAI based authorization for an existing HNB-GW service.

```plaintext
default authorised-macro-lai macro-info-ie-absent-action
```
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

exit

**Usage**

Use this command to return to the parent configuration mode.
rnc-id

Configures the Radio Network Concentrator (RNC) identifier in a Radio Network PLMN associated with HNB-GW service. The RNC identifier is provided to the HNB during HNB-REGISTRATION.

**Product**

HNB-GW

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > HNB-GW Service Configuration > HNB-RN PLMN Configuration

```plaintext
configure > context context_name > hnb-gw-service service_name > radio-network-plmn mcc mcc_number mnc mnc_number
```

Entering the above command sequence results in the following prompt:

```plaintext
[context_name]host_name(config-hnb-gw-radio-plmn)#
```

**Syntax**

```
[ no ] rnc-id rnc_id
```

- **no**
  
  Deletes the RNC id from the system configuration.

- **rnc-id**
  
  Specifies the RNC identifier as an integer from 0 through 4095.

**Usage**

Use this command to configure RNC id for Radio Network PLMN which will be sent to HNBs from HNB-GW during HNB-REGISTRATION procedure. Depending upon the requirement the RNC Identifier can be provided at the desired granularity.

**Example**

The following command configures the HNB-GW service to return an RNC identifier as 102 when an HNB-REGISTRATION request is received:

```
global rnc-id 102
```
Chapter 168
HSS Peer Service Configuration Mode Commands

The HSS Peer Service Configuration Mode is used to create and manage the Home Subscriber Server (HSS) Peer Service.

Mode

Exec > Global Configuration > Context Configuration > HSS Peer Service Configuration

configure > context context_name > hss-peer-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-hss-peer-service)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
**auth-request**

Configures the number of authentication vectors the MME/SGSN requests in an Authentication-Information-Request (AIR) message to the HSS for each UE requiring authentication.

**Product**
- MME
- SGSN

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > HSS Peer Service Configuration

```plaintext
configure > context context_name > hss-peer-service service_name
```

Entering the above command sequence results in the following prompt:

```plaintext
[context_name]host_name(config-hss-peer-service)#
```

**Syntax**

```plaintext
auth-request num-auth-vectors num

default auth-request num-auth-vectors

num-auth-vectors num
```

Specifies the number of vectors the MME/SGSN is requesting from the HSS as an integer.

*`num`* the valid range is 1 through 3. Default = 1.

**Usage**

Use this command to configure the number of authentication vectors the MME/SGSN requests in an Authentication-Information-Request (AIR) message to the HSS for each UE requiring authentication. Receiving multiple vectors from the HSS for a given UE helps reduce the number of messages across the diameter connection plus provides the MME/SGSN with additional vectors for the UE in the event that the connection or the HSS id disabled.

**Related Commands:**

- To view the current number of requested vectors, execute the `show hss-peer-service service name <name>` command in the Exec mode.

- To set the minimum number (low watermark) of vectors to be maintained at all times, execute `min-unused-auth-vector min_num` command from the call control profile configuration mode. (SGSN only)

- For troubleshooting, check the number of free, used, or in-use vectors displayed in the output of the `show subscribers [ gprs-only | sgsn-only ] full` command. (SGSN only).

**Example**

The following command sets the number of requested vectors to 2:

```plaintext
auth-request num-auth-vectors 2
```
diameter hss-dictionary

Specifies the Diameter Credit Control dictionary for the HSS peer service.

Product
MME
SGSN

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > HSS Peer Service Configuration
configure > context context_name > hss-peer-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-hss-peer-service)#!

Syntax

diameter hss-dictionary { custom1 | standard | standard-r9 } [ eir-dictionary { custom1 | standard | standard-r9 } ]

default diameter hss-dictionary

default
Sets the dictionary to default standard-r9 for HSS service.

custom1
Sets the Diameter dictionary to a customer-specific HSS Diameter dictionary. Default: Disabled

standard
Sets the Diameter dictionary to the standard (3GPP release 8) HSS peer dictionary. Default: Disabled

standard-r9
Sets the Diameter dictionary to the standard HSS peer dictionary for 3GPP release 9. Default: Enabled

eir-dictionary { custom1 | standard | standard-r9}
Specifies that an Equipment Identity Register (EIR) dictionary is to be used in conjunction with the HSS Diameter dictionary.
custom1: Sets the EIR Diameter dictionary to a customer-specific EIR Diameter dictionary.
standard: Sets the EIR Diameter dictionary to the standard HSS peer dictionary.
standard-r9: Sets the EIR Diameter dictionary to the standard HSS peer dictionary for release 9.

Usage
Use this command to select the Diameter dictionary for the HSS peer service.

Example
The following command sets the Diameter dictionary to IETF RFC 4006 specific:
diameter hss-dictionary standard
**diameter hss-endpoint**

 Associates a preconfigured Diameter origin endpoint with this HSS peer service.

**Product**
MME
SGSN

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > HSS Peer Service Configuration

**Syntax**
```
diameter hss-endpoint endpoint_name [ eir-endpoint eir_endpoint_name ] [ auc-endpoint auc_endpoint_name ]
```

**Usage**
Use this command to associated a Diameter origin endpoint to create a Diameter-based S6a or S6d (SGSN) interface association in this HSS peer service to provide AAA functionality to the EPS bearer context. Optionally, use this command to associate a Diameter origin endpoint to create a Diameter-based S13 or S13’ (SGSN) interface association in this HSS peer service to provide IMEI query capability between the MME and an EIR.
Important: The configuration of all endpoints is only valid when all necessary endpoint configuration has been completed. All endpoint listed above must also be defined as valid endpoints using the commands in the Diameter Endpoint configuration mode (refer to the Diameter Endpoint Configuration Mode Commands chapter in the Command Line Interface Reference manual) for more information on Diameter endpoint configuration parameters.

Example

The following command associates the preconfigured Diameter endpoint `hss_1` with this HSS peer service for HSS interface support.

```
diameter hss-endpoint hss_1
```
**diameter suppress**

Configures the MME to restrict the sending of the Notify-Request-Message to the HSS. By default, the Notify-Request-Message is sent to the HSS.

**Product**

MME

**Privilege**

Administrator

**Mode**

Exec > Global Configuration > Context Configuration > HSS Peer Service Configuration

```
command > context context_name > hss-peer-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-hss-peer-service)#
```

**Syntax**

```
[ no ] diameter suppress notify-request
```

no

Sets the command to the default value where the Notify-Request-Message is sent to the HSS.

**Usage**

Use this command to restrict the MME from sending the Notify-Request-Message to the HSS. This can be used to control whether handover to non-3GPP access can occur.
**diameter update-dictionary-avps**

Specifies which release of 3GPP TS 29.272 is to be used for the HSS peer service.

**Product**

MME  
SGSN

**Privilege**

Administrator

**Mode**

Exec > Global Configuration > Context Configuration > HSS Peer Service Configuration  
**configure** > context context_name > hss-peer-service service_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-hss-peer-service)#
```

**Syntax**

```
diameter update-dictionary-avps { 3gpp-r10 | 3gpp-r9 }
no diameter update-dictionary-avps
```

**Syntax**

**Usage**

Use this command to configure the 3GPP release that should be supported for this HSS peer service. This command is only applicable for the ‘standard’ diameter dictionary as defined in the **diameter hss-dictionary** command.
dynamic-destination-realm

Enables the MME to construct the destination realm using the MCC and MNC of foreign subscribers.

Product
MME

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > HSS Peer Service Configuration

configure > context context_name > hss-peer-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-hss-peer-service)#

Syntax

[ default | no ] dynamic-destination-realm

default

Returns the configuration to the default setting, where the MME uses the configured peer realm as the destination realm.

no

Disables the dynamic destination realm configuration. This provides the same behavior as the default keyword.

Usage

This command configures the MME to derive the EPC Home Network Realm/Domain based on the user's IMSI (MNC and MCC values) and use it as the Destination Realm in all diameter messages.

For a foreign subscriber, the MME does not know the HSS nodes in all the foreign PLMNs. In this case the MME routes S6a/S6d requests directed to foreign PLMNs via a Diameter Routing Agent (DRA) using only the destination realm. The DRA in turn routes the request to the correct HSS based on the destination realm. In order to accomplish this, the MME needs to dynamically construct requests to the DRA/HSS with a Destination Realm representing the foreign PLMN of the UE.

Refer to Configuring Dynamic Destination Realm Construction for Foreign Subscribers in Chapter 2 of the MME Administration Guide for more information about configuring this feature.

Example

The following command configures the MME to derive the destination realm for foreign subscribers based on the user’s IMSI (MNC/MCC).

dynamic-destination-realm
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```text
exit
```

**Usage**
Use this command to return to the parent configuration mode.
failure-handling

Configures failure handling behavior in the event of a failure with the HSS peer service. It also defines the action on various error codes on the Diameter interface during authentication or session activities.

**Product**
- MME
- SGSN

**Privilege**
- Security Administrator
- Administrator

**Mode**
- Exec > Global Configuration > Context Configuration > HSS Peer Service Configuration
- ```configure > context context_name > hss-peer-service service_name```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-hss-peer-service)#
```

**Syntax**

```
failure-handling { authentication-information-request | check-identity-request | notify-request | purge-ue-request | update-location-request } { diameter-result-code start_error_code [ to end_error_code ] | request-timeout } action { continue | retry-and-terminate | terminate }

no failure-handling { authentication-information-request | check-identity-request | notify-request | purge-ue-request | update-location-request } diameter-result-code start_error_code [ to end_error_code ]

default failure-handling { authentication-information-request | check-identity-request | notify-request | purge-ue-request | update-location-request } request-timeout

no
```

Removes the preconfigured failure handling procedures for calls in an HSS peer service.

```
default
```

Sets the default action for failure handling procedure for calls in an HSS peer service.

For default actions on Diameter result/error codes see the *Usage* section below.

**authentication-information-request**

Configures the MME-HSS service to handle the failures in an Auth-Information-Request message.
Configures the SGSN-HSS service to handle the failures in an Auth-Information-Request message.

**check-identity-request**

Configures the MME-HSS service to handle the failures in a Check-Identity-Information-Request message.
Configures the SGSN-HSS service to handle the failures in a Check-Identity-Information-Request message.
notify-request

Configures the MME-HSS service to handle the failures in a Notify-Request message.
This option is not supported on SGSN.

purge-ue-request

Configures the MME-HSS service to handle the failures in a Purge-UE-Request message.
Configures the SGSN-HSS service to handle the failures in a Purge-UE-Request message.

update-location-request

Configures the HSS peer service to handle the failures in an Update-Location-Request message.

diameter-result-code start_error_code [to end_error_code]

Configures the HSS peer service to handle the failures for various request messages having specific single or range of Diameter result codes in a request message.

*start_error_code* specifies an individual error code for Diameter protocol as an integer from 3000 through 5999. This will be the starting of code if a range of error codes is specified with the optional keyword *to end_error_code*.

to *end_error_code* is used to specify a range of error codes to handle by this command.

*end_error_code* specifies the end error code for Diameter protocol as an integer from 3000 through 5999.

request-timeout

Configures the HSS peer service to handle the failures for various request messages if response to that message is not received before timeout duration exhausted.

action { continue | retry-and-terminate | terminate }

Specifies the action to be taken on failure of any message as a policy for failure handling.

• **continue**: This option works differently for each system.

  For the SGSN: On receipt of any error for MICR session request, the SGSN allows the HSS peer service to continue with the session procedure without any interruption. For all other request/message types, the SGSN behaves as it would if configured for the **retry-and-terminate** option.

  For the MME: The MME does not support this option and if **continue** is included in the command, the MME behaves as it would if configured for the **retry-and-terminate** option.

  For 12.0 and earlier releases the **continue** option in failure handling on SGSN for IMEI procedures has the same behavior as that of the **retry-and-terminate** option.

  **Important**: For releases after 14.0, the **continue** option for IMEI procedure on SGSN can be configured in case of timeout and error responses requests from HSS so that the requests will be re-trying on a second peer (if configured) and the call is continued. The configuration of **continue** option for IMEI procedure is as follows:

  ```
  configure
  
  context <name>
  
  hss-peer-service <name>
  ```
HSS Peer Service Configuration Mode Commands

**failure-handling**

```
failure-handling check-identity-request request-timeout
action continue

failure-handling check-identity-request diameter-result-code
<range1> to <range2> action continue

failure-handling check-identity-request diameter-result-code
<range1> action continue

exit

exit

exit
```

- **retry-and-terminate**: On receipt of any error, once the configured condition (either the request timeout or receipt of the specified result code) occurs, the system retries sending the request (AIR/ULR/NOR/PUR/MICR) to another peer that is configured in the same endpoint. If no response is received for AIR or ULR from the second peer, then the system allows the HSS peer service to terminate the session.

- **terminate**: On receipt of any error, once the configured condition (either the request timeout or receipt of the specified result code) is met, the system allows the HSS peer service to immediately terminate the session (AIR/ULR/MICR) without any further action.

---

**Usage**

Use this command to configure the failure handling behavior in the event of a communication failure with the HSS peer service.

The following are the default actions for Diameter result codes:

- For all protocol error codes 3000 to 3999, the default action is terminate. For all transient error codes 4000, 4001, 4004 to 4180, and 4182 to 4999, the default action is continue.
- For transient error codes 4002, 4003, and 4181, the default action is retry.
- For error code 4001, the default action is terminate.
- For permanent error codes 5000 to 5999, the default action is terminate.

---

**Example**

The following command will allow HSS peer service to continue if any failure in Auth-Information-Request message occurred with Diameter error code 3050:

```
failure-handling authentication-information-request diameter-result-code
3050 action continue
```
request timeout

Configures the application request timeout between the HSS peer service and HSS node. The MME/SGSN waits for this duration before retransmitting the request to corresponding HSS node.

**Product**
MME
SGSN

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > HSS Peer Service Configuration

```
configure > context context_name > hss-peer-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-hss-peer-service)#
```

**Syntax**

```
request timeout dur
[ no | default ] request timeout
```

- **no**
  Disables the configured application request timeout value.

- **default**
  Sets the application request time out duration to default value of 300 seconds.

- **dur**
  Specifies the application request timeout duration (in seconds) as an integer from 1 through 300. The MME/SGSN will wait for this duration before retrying the request with corresponding HSS. Default: 20

**Usage**
Use this command to set the waiting period for HSS peer service in seconds after which the request is deemed to have failed or system will resend the request.

**Example**

The following example configures the application request timeout duration to 20 seconds:

```
default request timeout
```
zone-code-format

Configures how the MME must interpret the received zone-code values from the HSS.

Product
MME

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > HSS Peer Service Configuration

```
configure > context context_name > hss-peer-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-hss-peer-service)#
```

Syntax

```
zone-code-format { ascii-string }
```

[ default ] zone-code-format

----------

`default`

Returns the command to the default setting, where the MME interprets the zone-code as an octet string.

----------

`ascii-string`

Configures the MME to interpret the zone-code as an ascii string. This option is provided to maintain backward compatibility.

When configured as ascii-string, the MME interprets the received zone-code as an ASCII string (coded in hexadecimal representation) and converts it byte by byte to an integer value. For example, if the HSS sends the zone-code value as 3032, the MME converts this to 02 (ASCII value of 0 in Hex is 0x30, ASCII value of 2 in Hex is 0x32). With this configuration, the MME accepted zone-codes only within the range of 0 to 99.

----------

Usage

This new command specifies the format of the zone-code value received from HSS to MME. The MME uses this configuration to interpret and convert the received zone-code value to an integer value and validate it against the list of allowed zone-code configured for the zone-code restriction feature.

By default, the MME interprets the received zone-code value from HSS as a octet-string (2 bytes) which is coded in full hexadecimal representation. The MME converts the entire 2 byte octet string coded in hexadecimal to integer value and it uses the same for validation for zone-code restriction feature. For example, if the HSS sends the zone-code value as 3032, MME converts this to 12338 (which is the equivalent of 0x3032).

Example

The following command configures the HSS Peer Service to interpret the zone-code received from the HSS as an ASCII string.

```
zone-code-format ascii-string
```
Chapter 169
IGMP Profile Configuration Mode Commands

The Internet Group Management Protocol (IGMP) Profile Configuration Mode is used to create and manage the IGMP parameters for an Ethernet interface.

Mode

Exec > Global Configuration > Context Configuration > IGMP Profile Configuration

```bash
configure > context context_name > ip igmp profile profile_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-igmp-profile-<profile_name>)#
```

**Important:** Available commands or keywords/variables vary based on platform type, product version, and installed license(s).
default ip igmp

Configures default IGMP parameters.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > IGMP Profile Configuration

```bash
configure > context context_name > ip igmp profile profile_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-igmp-profile-<profile_name>)#
```

**Syntax**

```
default ip igmp { query | require | robustness | unsolicited-report-interval | version }
```

**Usage**
Specify the IGMP parameters for the default profile. Refer to the remaining command description in this chapter for additional information.

**Example**
To apply enable echo mode on this interface, use the following command:

```
bfd echo
```
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Use this command to return to the parent configuration mode.
ip igmp query

Configures the maximum response time for IGMP queries.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > IGMP Profile Configuration
configure > context context_name > ip igmp profile profile_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-igmp-profile-<profile_name>)#

Syntax

ip igmp query max-response-time seconds

**max-response-time seconds**

Specify the maximum number of seconds that the system will wait for an IGMP response as an integer from 1 through 25.

Usage

Specify the maximum response time for IGMP queries.

Example

    ip igmp query max-response-time 10
ip igmp require router-alert

Sets the router alert flag to ON in IP IGMP packets.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > IGMP Profile Configuration

configure > context context_name > ip igmp profile profile_name

Entering the above command sequence results in the following prompt:

/context_name host_name(config-igmp-profile-<profile_name>)#

Syntax

[ no ] ip igmp require router-alert

no

Sets the router alert flag to OFF in IP IGMP packets.

Usage
Sets the router alert flag to ON in IP IGMP packets.

Example

ip igmp require router-alert
ip igmp robustness

Sets the Robustness value in IP IGMP packets. The Robustness variable allows tuning for the expected packet loss on a subnet. If a subnet is expected to be lossy, the Robustness variable may be increased. IGMP is robust to packet losses. The Robustness variable should not be set to 1 (one).

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > IGMP Profile Configuration

configure > context context_name > ip igmp profile profile_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-igmp-profile-<profile_name>)#

Syntax

ip igmp robustness value

value

Sets the robustness value as an integer from 1 through 10. Default: 2

Usage

Sets the robustness value in IP IGMP packets.

Example

ip igmp robustness 7
**ip igmp unsolicited-report-interval**

Sets the Unsolicited Report Interval which is the time between repetitions of a host's initial report of membership in a group.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > IGMP Profile Configuration

```
configure > context context_name > ip igmp profile profile_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-igmp-profile-<profile_name>)#
```

**Syntax**

```
ip igmp unsolicited-report-interval seconds
```

**seconds**
Specifies the number of seconds between repetitions of a host's initial report of membership in a group as an integer from 1 through 25. Default: 10

**Usage**
Set the Unsolicited Report Interval which is the time between repetitions of a host's initial report of membership in a group.

**Example**

```
ip igmp unsolicited-report-interval 15
```
ip igmp version

Sets the IGMP version to be supported by this interface.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > IGMP Profile Configuration

```
configure context context_name ip igmp profile profile_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-igmp-profile-<profile_name>)#
```

**Syntax**

```
ip igmp version { v1 | v2 | v3 }
```

<table>
<thead>
<tr>
<th>v1</th>
<th>v2</th>
<th>v3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the IGMP Version number:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>•v1: Version 1, RFC 1112</td>
<td></td>
<td></td>
</tr>
<tr>
<td>•v2: Version 2, RFC 2236</td>
<td></td>
<td></td>
</tr>
<tr>
<td>•v3: Version 3, RFC 4604</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Usage**
Set the IGMP version to be supported by this interface.

**Example**

```
ip igmp version v2
```
Chapter 170
IKEv2 Security Association Configuration Mode
Commands

The IKEv2 Security Association Configuration Mode is used to configure a Security Association (SA) at the outset of an IPSec session. A security association is the collection of algorithms and parameters (such as keys) that is being used to encrypt and authenticate a particular flow in one direction. In normal bi-directional traffic, the flows are secured by a pair of security associations.

Mode

Exec > Global Configuration > Context Configuration > IKEv2 Security Association Configuration

configure > context context_name > ikev2-ikesa transform-set set_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(cfg-ctx-ikev2ikesa-tran-set)#

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
**default**

Sets the default properties for the selected parameter.

**Product**

ePDG
PDIF

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > IKEv2 Security Association Configuration

configure > context context_name > ikev2-ikesa transform-set set_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-ctx-ikev2ikesa-tran-set)#
```

**Syntax**

```
default { encryption | group | hmac | lifetime | prf }
```

Set the defaults for the following parameters:

- **encryption**: Default algorithm for the IKEv2 IKE SA is AES-CBC-128.
- **group**: Default Diffie-Hellman group is Group 2.
- **hmac**: Default IKEv2 IKE SA hashing algorithm is SHA1-96.
- **lifetime**: Default lifetime for SAs derived from this transform-set is 86400 seconds.
- **prf**: Default PRF for the IKEv2 IKE SA is SHA1.

**Usage**

Configure default parameters for the IKEv2 IKE SA transform-set.

**Example**

Use the following configuration to set the default encryption algorithm:

```
default encryption
```
encryption

Configures the appropriate encryption algorithm and encryption key length for the IKEv2 IKE security association. AES-CBC-128 is the default.

Product
ePDG
PDIF

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > IKEv2 Security Association Configuration

configure > context context_name > ikev2-ikesa transform-set set_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(cfg-ctx-ikev2ikesa-tran-set)#

Syntax

encryption { 3des-cbc | aes-cbc-128 | aes-cbc-256 | des-cbc | null }

default encryption

3des-cbc
Data Encryption Standard Cipher Block Chaining encryption applied to the message three times using three different cipher keys (triple DES).

aes-cbc-128
Advanced Encryption Standard Cipher Block Chaining with a key length of 128 bits.

aes-cbc-256
Advanced Encryption Standard Cipher Block Chaining with a key length of 256 bits.

des-cbc

null
Configures no IKEv2 IKE Security Association Encryption Algorithm. All IKEv2 IPsec Child Security Association protected traffic will be sent in the clear.

Usage

IKEv2 requires a confidentiality algorithm to be applied in order to work. In cipher block cryptography, the plaintext is broken into blocks usually of 64 or 128 bits in length. In cipher block chaining (CBC) each encrypted block is chained into the next block of plaintext to be encrypted. A randomly-generated vector is applied to the first block of plaintext in lieu of an encrypted block. CBC provides confidentiality, but not message integrity.
Because RFC 4307 calls for interoperability between IPSec and IKEv2, the IKEv2 confidentiality algorithms must be the same as those configured for IPSec in order for there to be an acceptable match during the IKE message exchange. Because of RFC4307, in IKEv2, there is no viable NULL option, it is available for testing only.

**Example**

The following command configures the encryption to be aes-cbc-128:

```
encryption aes-cbc-128
```
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Use this command to return to the parent configuration mode.
**group**

Configures the appropriate key exchange cryptographic strength by applying a Diffie-Hellman group. Default is Group 2.

**Product**

ePDG

PDIF

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > IKEv2 Security Association Configuration

```
configure > context context_name > ikev2-ikesa transform-set set_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-ctx-ikev2ikesa-tran-set)#
```

**Syntax**

```
group { 1 | 2 | 5 | 14 }
default group
```

**1**

Configures crypto strength at the Group 1 level. Lowest security.

**2**

Configures crypto strength at the Group 2 (default) level. Medium security. This is the default setting for this command.

**5**

Configures crypto strength at the Group 5 level. Higher security.

**14**

Configures crypto strength at the Group 14 level. Highest security

**Usage**

Diffie-Hellman groups are used to determine the length of the base prime numbers used during the key exchange process in IKEv2. The cryptographic strength of any key derived depends, in part, on the strength of the Diffie-Hellman group upon which the prime numbers are based.

Group 1 provides 768 bits of keying strength, Group 2 provides 1024 bits, Group 5 provides 1536 bits and Group 14 provides 2048 bits of encryption strength.

Configuring a DH group also enables Perfect Forward Secrecy, which is disabled by default.

**Example**

This command configures crypto strength at the Group 14 level. Highest security group 14:
default group
**hmac**

Configures the IKEv2 IKE SA integrity algorithm. Default is SHA1-96.

**Product**
ePDG
PDIF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > IKEv2 Security Association Configuration

```plaintext
configure > context context_name > ikev2-ikesa transform-set set_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-ctx-ikev2ikesa-tran-set)##
```

**Syntax**

```
hmac { aes-xcbc-96 | md5-96 | sha1-96 | sha2-256-128 | sha2-384-192 | sha2-512-256 }
```

**default hmac**

<table>
<thead>
<tr>
<th>hmac</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aes-xcbc-96</td>
<td>HMAC-AES-XCBC uses a 128-bit secret key and produces a 128-bit authenticator value.</td>
</tr>
<tr>
<td>md5-96</td>
<td>HMAC-MD5 uses a 128-bit secret key and produces a 128-bit authenticator value.</td>
</tr>
<tr>
<td>sha1-96</td>
<td>HMAC-SHA-1 uses a 160-bit secret key and produces a 160-bit authenticator value. This is the default setting for this command.</td>
</tr>
<tr>
<td>sha2-256-128</td>
<td>HMAC-SHA-256 uses a 256-bit secret key and produces a 128-bit authenticator value.</td>
</tr>
<tr>
<td>sha2-384-192</td>
<td>HMAC-SHA-384 uses a 384-bit secret key and produces a 192-bit authenticator value.</td>
</tr>
<tr>
<td>sha2-512-256</td>
<td>HMAC-SHA-512 uses a 512-bit secret key and produces a 256-bit authenticator value.</td>
</tr>
</tbody>
</table>

**Usage**

IKEv2 requires an integrity algorithm be configured in order to work. A keyed-Hash Message Authentication Code, or HMAC, is a type of message authentication code (MAC) calculated using a cryptographic hash function in combination with a secret key to verify both data integrity.
and message authenticity. A hash takes a message of any size and transforms it into a message of a fixed size: the authenticator value. This is truncated and transmitted. The authenticator value is reconstituted by the receiver and the first truncated bits are compared for a 100 percent match.

**Example**

This command configures HMAC value md5-96:

```
hmac md5-96
```
**lifetime**

Configures the lifetime of a security association (SA) in seconds.

**Product**
- ePDG
- PDIF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > IKEv2 Security Association Configuration

```
configure > context context_name > ikev2-ikesa transform-set set_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-ctx-ikev2ikesa-tran-set)#
```

**Syntax**

```
lifetime sec
```

**default lifetime**

```
lifetime sec
```

Sets the value of the timeout parameter in seconds as an integer from 60 through 86400. Default: 86400

**Usage**
The secret keys that are used for various aspects of a configuration should only be used for a limited amount of time before timing out. This exposes a limited amount of data to the possibility of hacking. If the SA expires, the options are then to either close the SA and open a new one, or renew the existing SA.

**Example**
The following command sets the lifetime timeout to 120 seconds:

```
lifetime 120
```
**prf**

Selects one of the HMAC integrity algorithms to act as the IKE Pseudo-Random Function. A PRF produces a string of bits that an attacker cannot distinguish from random bit string without knowledge of the secret key. The default is SHA1.

**Product**
ePDG
PDIF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > IKEv2 Security Association Configuration

```
configure > context context_name > ikev2-ikesa transform-set set_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-ctx-ikev2ikesa-tran-set)#
```

**Syntax**

```
prf { aes-xcbc-128 | md5 | sha1 | sha2-256 | sha2-384 | sha2-512 }
```

**default prf**

---

**aes-xcbc-128**

Configure IKEv2 IKE Security Association Pseudo Algorithm to be AES-XCBC-128.

**md5**

MD5 uses a 128-bit secret key and produces a 128-bit authenticator value.

**sha1**

SHA-1 uses a 160-bit secret key and produces a 160-bit authenticator value. SHA-1 is considered cryptographically stronger than MD5, but it takes more CPU cycles to compute. This is the default setting for this command.

**sha2-256**

PRF-HMAC-SHA-256 uses a 256-bit secret key.

**sha2-384**

PRF-HMAC-SHA-384 uses a 384-bit secret key.

**sha2-512**

PRF-HMAC-SHA-512 uses a 512-bit secret key.
Usage
This command generates keying material for all the cryptographic algorithms used in both the IKE_SA and the CHILD_SAs.

Example
This configuration sets the PRF to be value sha2-256:

```
prf sha2-256
```
Chapter 171
IMEI Profile Configuration Mode

The IMEI profile configuration mode defines a set of parameters controlling the SGSN behavior when a Request is received from a device in the specified IMEI (International Mobile Equipment Identity) range. An IMEI profile is a key element in the Operator Policy feature and an IMEI profile is not used or valid unless it is associated with an IMEI range and this association is specified in an operator policy (see the Operator Policy Configuration Mode Commands chapter elsewhere in the Command Line Interface Reference).

Essentially, an IMEI profile is a template which groups a set of device-specific commands that may be applicable to one or more IMEIs. The same IMEI profile can be associated with multiple IMEI ranges and multiple operator policies.

An SGSN supports a total of 1000 IMEI profile configurations.

Mode

Exec > Global Configuration > IMEI Profile Configuration

configure > imei-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-imei-profile-profile_name)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
associate

Associate an APN remap table with this IMEI profile.

Note that an APN remap table can be associated with an IMEI profile before the table has actually been created/configured.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > IMEI Profile Configuration

configure > imei-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-imei-profile-profile_name)#

Syntax

associate apn-remap-table table_name

no associate apn-remap-table

no

Disables the configured remap table association.

table_name

Define the name of an APN remap table that is to be associated with this IMEI profile for call routing based in IMEI.

Usage

Use this command to associate an APN remap table with this IMEI profile. With such an association, it is possible to override an APN call-routing based on an IMEI.

For example, with the APN exceptions defined in an APN remap table (refer to the APN Remap Table Configuration Mode chapter), a blank APN or an incorrect APN could be overridden. So during PDP Activation for in incoming call, the call could be rerouted based on an IMEI in the range defined for the IMEI profile.

Example

Associate the APN remap table ‘remapHO’ (remaps all calls with blank APNS to the head-office) to this IMEI profile:

associate apn-remap-table remapHO
blacklist

Blacklist all mobile devices that fit the IMEI definitions associated with this IMEI profile.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > IMEI Profile Configuration
configure > imei-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-imei-profile-profile_name)#

Syntax

blacklist

remove blacklist

remove

Including this keyword with the command, removes the blacklist command from the IMEI profile configuration.

Usage
Blacklists subscribers whose devices bear IMEI that match the defined IMEI range for this profile.

Example
Use this command to blacklist all subscribers with IMEI that fall within the range set for this IMEI profile:

blacklist
description

Define a descriptive string relevant to the specific APN profile.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > IMEI Profile Configuration

configure > imei-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-imei-profile-profile_name)#

Syntax

description description

remove description

remove

Removes the configured description from this APN profile.

description

Enter an alphanumeric string of 1 to 100 alphanumeric characters. The string may include spaces, punctuation, and case-sensitive letters if the string is enclosed in double quotes (" ").

Usage

Define information that identifies this particularly APN profile.

Example

Indicate that this IMEI profile IMEIprof1 is to be used for customers in the United Kingdom and that the profile:

description "IMEIprof1 defines routing actions based on IMEI for customers in the UK."
**direct-tunnel**

Instruct the SGSN to enable/disable a direct tunnel between the RNC and the GGSN based on the IuPS service configuration.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > IMEI Profile Configuration

```configure > imei-profile profile_name```

**Syntax**

```direct-tunnel check-iups-service```

```
no direct-tunnel
```

```
no direct-tunnel
```

This command instructs the SGSN to disable the direct tunnel function between the GGSN and the RNC.

**Usage**

Direct tunnel is enabled by default on the GGSN and often on the RNC. This leaves it to the SGSN’s configuration to actually enable or disable a direct tunnel. With the SGSN, the options for configuring a direct tunnel are complex -- enable/disable on the basis of APNs, or RNCs, or GGSNs, or on the basis of the IMEI range. Refer to the SGSN Administration Guide for configuration details.

**Example**

Assuming the IuPS service configuration has enabled DT for associated RNCs, then use this command to enable DT from the RNC to the GGSN associated with this IMEI profile:

```direct tunnel check-iups-service```
end

Exits the current configuration mode and returns to the Exec mode.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

end

Usage
Return to the Exec mode.
**exit**

Exits the current configuration mode and returns to the context configuration mode.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**
Move to the previous configuration mode.
ggsn-address

Identify the target GGSN for traffic being managed by this IMEI profile.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > IMEI Profile Configuration

configure > imei-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-imei-profile-profile_name)#

Syntax

```
ggsn-address IPv4/IPv6_address
```

Enter the IP address of the target GGSN. Enter the address in either standard IPv4 dotted decimal format or in standard IPv6 colon notation format.

Usage

Use this command to define the IP address of the target GGSN to be associated with this IMEI profile.

Example

The following command identifies the address of the GGSN associated with this IMEI profile as 123.123.11.1

```
ggsn-address 123.123.11.1
```
pdp-activate

This command enables the operator to configure the SGSN to reject Secondary PDP Activation Requests from the UE based on IMEI range.

Product
SGSN

Privilege
Administrator

Mode
Exec > Global Configuration > IMEI Profile Configuration
configure > imei-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-imei-profile-profile_name)#

Syntax

[ remove ] pdp-activate { drop | restrict } secondary-activation access-type { gprs | umts }

<table>
<thead>
<tr>
<th>remove</th>
</tr>
</thead>
<tbody>
<tr>
<td>Removes the configured value and returns the pdp-activate configuration to the default ‘not configured’ state.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>drop</th>
</tr>
</thead>
<tbody>
<tr>
<td>This keyword causes the GSN to ignore the Request.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>restrict</th>
</tr>
</thead>
<tbody>
<tr>
<td>This keyword instructs the SGSN to reject Secondary PDP Activation Requests.</td>
</tr>
</tbody>
</table>

| access-type { gprs | umts } |
|-----------------------------|
| This keyword instructs the SGSN to ignore or reject Secondary PDP Activation Requests on the basis of the UE’s access network type: |

  * **gprs** : from a 2G network.
  * **umts** : from a 3G network.

Usage

The SGSN administrator can use this command to configure the IMEI profile in the operator policy to either ignore or reject Secondary PDP Activation Requests from UEs based on an IMEI range and UE access-type. Restricting secondary PDP activation based on the IMEI (in the IMEI profile) takes precedence over secondary PDP activation that might be configured in the call control profile.

Example

Enable rejection of Secondary PDP Activation Requests for 2G callers:

    pdp-activate restrict secondary-activation access-type gprs
Chapter 172
IMS Authorization Service Configuration Mode Commands

The IMS Authorization Service Configuration Mode enables to configure IP Multimedia Subsystem (IMS) authorization services to manage policy control functions and Gx interface support.

Mode

Exec > Global Configuration > Context Configuration > IMS Authorization Service Configuration

configure > context context_name > ims-auth-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-imsa-service)#

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
**end**

Exits the current configuration mode and returns to the Exec mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**

Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Use this command to return to the parent configuration mode.
p-cscf discovery

This command defines the method of Proxy-Call Session Control Function (P-CSCF) discovery to be used.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > IMS Authorization Service Configuration

configure > context context_name > ims-auth-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-imsa-service)#

Syntax

p-cscf discovery { table { 1 | 2 } [ algorithm { ip-address-modulus | msisdn-modulus | round-robin } ] | diameter-configured }

[ default | no ] p-cscf discovery

default
Sets the P-CSCF discovery to default parameter.

no
Removes/deletes configured parameters for P-CSCF discovery.

table { 1 | 2 }
Specifies that which P-CSCF table is to be used to obtain the primary and secondary P-CSCF addresses. Total 2 tables can be configured for P-CSCF discovery.

algorithm { ip-address-modulus | msisdn-modulus | round-robin }
Specifies the algorithm to select the row from the P-CSCF table to be used for P-CSCF discovery.

  • ip-address-modulus: This algorithm divides the IP address, in binary, of the subscriber by the number of rows in the table, and the remainder is used as an index into the specified table to select the row.

  • msisdn-modulus: This algorithm divides the MSISDN value, in binary without the leading “+”, of the subscriber by the number of rows in the table, and the remainder is used as an index in the specific table to select the row.

  • round-robin: This algorithm rotates all rows in the active table for selection of the row in round-robin way. If no algorithm is specified this is the default behavior.

Default: round-robin
diameter-configured

This option enables the table number and algorithm specified by the `diameter host-select table` configuration in Policy Control Configuration mode.

Usage

Use this command to configure the table and row selection methods to select IP address/host address for P-CSCF discovery.

Example

The following command specifies table 1 with `round-robin` algorithm to select the rows with IP address for P-CSCF discovery.

```
p-cscf discovery table 1 algorithm round-robin
```
**p-cscf table**

This command adds/appends rows with primary and/or secondary IPv4/IPv6 addresses to a P-CSCF discovery table with precedence for P-CSCF discovery.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > IMS Authorization Service Configuration

```
configure > context context_name > ims-auth-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-imsa-service)#
```

**Syntax**

In releases prior to 18:

```
p-cscf table { 1 | 2 } row-precedence precedence_value { address ipv4_address | ipv6-address ipv6_address } [ secondary { address ipv4_address | ipv6-address ipv6_address } ] [ weight value ]
```

```
no p-cscf table { 1 | 2 } row-precedence precedence_value
```

In 18 and later releases:

```
p-cscf table { 1 | 2 } row-precedence precedence_value { ipv4-address ipv4_address [ ipv6-address ipv6_address ] | ipv6-address ipv6_address [ ipv4-address ipv4_address ] } [ secondary { ipv4-address ipv4_address [ ipv6-address ipv6_address ] | ipv6-address ipv6_address [ ipv4-address ipv4_address ] } [ weight value ]
```

```
no p-cscf table { 1 | 2 } row-precedence precedence_value
```

**no**
Removes/deletes configured row with precedence in specified table for P-CSCF discovery address.

```
{ 1 | 2 }
```

Specifies which P-CSCF table is to be used to add/append the primary and secondary P-CSCF addresses. Two tables can be configured for P-CSCF discovery address.

**row-precedence precedence_value**

This keyword adds/appends the row with the specified row-precedence to the P-CSCF address table. In 8.1 and later releases, `precedence_value` must be an integer from 1 through 128, and a maximum of 128 rows can be added to a table. In release 8.0, `precedence_value` must be an integer from 1 through 100, and a maximum of 16 rows can be added to a table.
secondary
Specifies the secondary IPv4/IPv6 address to be entered in P-CSCF table rows.

address ip_address
Specifies the primary and/or secondary IPv4 address for P-CSCF discovery table. This keyword, if used with secondary keyword, specifies the secondary IPv4 address.
ip_address must be entered in IPv4 dotted-decimal notation.

ipv6-address ipv6_address
Specifies the primary and/or secondary IPv6 address for P-CSCF discovery table. This keyword, if used with secondary keyword, specifies the secondary IPv6 address.
ipv6_address must be entered in IPv6 colon-separated-hexadecimal notation.

weight value
This keyword designates weight to a row-precedence relative to other row-precedences configured under this table, Default value is 1. value must be an integer from 1 through 10.
Within the IMS Authorization configuration, the P-CSCF address is selected based on round robin fashion. This feature allows the customer to perform P-CSCF selection based on weight factor. With this CLI option, the user can configure and add weight (in the scale of 1 to 10) to each row, and the rows are selected based on weighted round-robin. That is, the row with higher weight parameter is selected more number of times than the row with less number of weights.

Usage
Use this command to add rows with primary and/or secondary IP addresses for P-CSCF discovery. The row is added with the specified row-precedence.
The operator can add/remove rows to the table that is not currently selected by the diameter host-select table command in Policy Control Configuration Mode.

Example
The following command adds a row in table 2 with primary IP address 10.2.3.4, secondary IP address as 50.6.7.8, and row-precedence value as 20 for P-CSCF discovery.

```
p-cscf table 2 row-precedence 20 address 10.2.3.4 secondary 50.6.7.8
```
policy-control

This command enters the Policy Control Configuration mode for Diameter Policy Control Application (DPCA) to configure Diameter authorization and policy control parameter for IMS authorization.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > IMS Authorization Service Configuration

```
configure > context context_name > ims-auth-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-imsa-service)#
```

**Syntax**

```
[ no ] policy-control
```

- **no**
  Disables the pre-configured policy control parameters for IMS authorization in this IMS authorization service.

**Usage**

Use this command to enter the Policy Control Configuration Mode to configure the policy control parameters for Diameter authorization and charging policy in IMS Authorization Service. Entering this command results in the following prompt:

```
[context_name]host_name(config-imsa-dpca)#
```

Policy Control configuration commands are described in the *Policy Control Configuration Mode Commands* chapter.
qos-update-timeout

This command is obsolete in release 11.0 and later releases. This command sets the Quality of Service update timeout for a subscriber in IMS authorization service.

Product
GGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > IMS Authorization Service Configuration

configure > context context_name > ims-auth-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-imsa-service)#

Syntax

qos-update-timeout timeout_duration

no qos-update-timeout

no

Disables the pre-configured QoS update timeout parameter in this IMS authorization service.

timeout_duration

Specifies the duration of timeout in seconds as an integer from 0 through 3600.
Default: 60

Usage

Use this command to set the maximum time to wait for a subscriber to initiate the update QoS procedure in IMS authorization service.

Example

The following command sets the QoS update timeout to 90 seconds.

qos-update-timeout 90
signaling-flag

This command specifies whether a request for a PDP context dedicated to signaling (for IMS sessions) should be granted or denied.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > IMS Authorization Service Configuration

```
configure > context context_name > ims-auth-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-imsa-service)#
```

**Syntax**

```
signaling-flag { deny | permit }
```

**default signaling-flag**

```
default
```

Sets the signaling flag to default mode of deny.

```
deny
```

Denies the request for a signaling PDP context for IMS session and keeps signaling co-existed with other traffic on PDP contexts. Default: Enabled

```
permit
```

Permits the request for a signaling PDP context for IMS session and a separate signaling context activated. Default: Disabled

**Usage**

Use this command to allow or deny the activation of a dedicated PDP context for signaling. The user equipment (UE) may indicate that the PDP context should be dedicated for IP multimedia (IM) signaling by setting the IP Multimedia Core Network (IM-CN) signaling flag in the Protocol Configuration Options (PCO).

The **deny** option causes the system to inform the UE that the PDP context will not be dedicated for IM signaling and signaling will co-exist with other traffic on PDP context.

The **permit** option is used to activate the signaling context for signal traffic and the other traffic uses other PDP context for traffic with the following destinations:

- Towards the DHCP and DNS servers for the IMS domain
- Towards the P-CSCF(s)

The UE is not trusted to follow these restrictions, and the system monitors and restricts the traffic from the dedicated PDP context. The **signaling-flow class-map** command is used to configure the restrictions.
Example

The following command denies the request for a signaling PDP context for IMS session.

```
default signaling-flag
```
**signaling-flow**

This command specifies the packet filters and policy servers for bandwidth control and signaling context enforcement that define the traffic that is allowed through the dedicated signaling context.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > IMS Authorization Service Configuration

`configure > context context_name > ims-auth-service service_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-imsa-service)#
```

**Syntax**

```
signaling-flow permit server-address ipv4/ipv6_address [ server-port { port_num | range start_port to end_port } ] [ description STRING ]
```

```
no signaling-flow permit server-address ipv4/ipv6_address [ server-port { port_num | range start_port to end_port } ]
```

**no**

Disables the signaling flow option configured with this command.

**server-address ipv4/ipv6_address**

The server address refers to the destination IP address in uplink packets, and the source IP address in downlink packets.

`ipv4/ipv6_address` is an IP address in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation and can be used with a subnet mask.

A maximum of 16 signaling server addresses can be configured per IMS Authorization service.

**server-port { port_num | range start_port to end_port }**

Specifies the TCP/UDP port number(s) of the server to be used for communication.

`port_num` must be an integer from 1 through 65535.

`range start_port to end_port` provides the option to configure the range of ports on server for communication.

`start_port` must be an integer from 1 through 65535 but lesser than `end_port`, and `end_port` must be an integer from 1 through 65535 but greater than `start_port`.

**description STRING**

Specifies the customized description for configured signaling server as an alphanumeric string of 1 through 63 characters.
Usage
Traffic that matches any instance of the signaling-flow command will be forwarded via the signaling PDP context. In addition, the policy server gives policy gates to use for the signaling PDP context.

Example
The following command sets the packet filter server address to 10.2.3.4 with port number 1234 for packet filtering.

```
    signaling-flow server-address 10.2.3.4 server-port 1234
```
traffic-policy

This command specifies the action on packets which do not match any policy gates in the general purpose PDP context.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > IMS Authorization Service Configuration

```bash
configure > context context_name > ims-auth-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-imsa-service)#
```

**Syntax**

```bash
traffic-policy general-pdp-context no-matching-gates direction { downlink | uplink } { forward | discard }
```

```bash
default traffic-policy general-pdp-context no-matching-gates direction { downlink | uplink }
```

**default**
Sets the default traffic policy for packets without any policy gate match in general purpose PDP context. By default packets which do not have any matching policy gate are forwarded.

**no-matching gates**
Applies traffic policy for packets which do not match any policy gate.

**direction { downlink | uplink }**
Specifies the direction of traffic to apply this traffic policy in general PDP context.

downlink: Specifies the traffic from system to MN. Default is set to forward.
uplink: Specifies the traffic from MN to system. Default is set to forward.

**forward**
Forwards the packets which do not match any policy gates. Default: Enabled

**discard**
Discards the packets which do not match any policy gates. Default: Disabled

**Usage**

This command provides configuration on traffic policy applied on packets which are not matching any policy gate in general PDP context. Packets can either be forwarded or discarded on the basis of operator’s configuration.

This command needs to be configured once for downlink and once for uplink separately.
Example

The following command discards uplink packets which do not match any policy gate in general purpose PDP context.

```
traffic-policy general-pdp-context no-matching-gates direction uplink discard
```
Chapter 173
IMS Sh Service Configuration Mode Commands

The IMS Sh Interface Configuration Mode is used to configure various Diameter parameters in order for:
PDIF to communicate with the HSS server. HSS server is used for MAC address validation in the IKEv2 exchanges to set up SAs and for storing part of the user profile. SCM to communicate with the HSS server. HSS server is used for retrieval and update of call feature parameters and call restriction data.

Mode

Exec > Global Configuration > Context Configuration > IMS Sh Interface Configuration
configure > context context_name > ims-sh-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ims-sh-service)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
diameter

This command configures Diameter parameters.

Product
PDIF
SCM

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > IMS Sh Interface Configuration
configure > context context_name > ims-sh-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ims-sh-service)#

Syntax

diameter { dictionary { custom1 | standard | endpoint string } }
default diameter { dictionary | endpoint }
no diameter endpoint

no
Removes previously configured endpoint.

default
Configures parameters to the default value.

dictionary
Specifies the dictionary to use.
  •custom1: A custom dictionary
  •standard: The standard dictionary

Important: SCM uses only the standard dictionary.

depoint string
Selects an endpoint to use in the configuration.
string must be the endpoint name, and must be an alpha and/or numeric string of 1 through 63 characters in length.

Usage
The Diameter endpoint contains information on the peer names and IP addresses and port, and the local IP address to use for Diameter.
You can have more than one Diameter endpoint configured on the chassis and the ims-sh-service needs to know which Diameter endpoint to use. This command is to select the appropriate Diameter endpoint, even if only one has been configured.

**Example**

The following example selects a diameter endpoint `diam1`:

```
diameter endpoint diam1
```
end

Exits the current mode and returns to the Exec Mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to change to the Exec Mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
exit
```

**Usage**
Use this command to return to the parent configuration mode.
failure-handling

This command configures the action to take in the event of an HSS server request failure.

Product
- PDIF
- SCM

Privilege
- Administrator

Mode
- Exec > Global Configuration > Context Configuration > IMS Sh Interface Configuration
- configure > context context_name > ims-sh-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ims-sh-service)#

Syntax

[ default ] failure-handling { profile-update-request | user-data-request } { { diameter-result-code result_code [ to result_code ] } | timeout } action { continue | retry-and-terminate | terminate } }

- default
  Resets configuration for the specified keyword to the default setting.

- profile-update-request
  Configures failure-handling as a result of a profile update request error.

- user-data-request
  Configures failure-handling as a result of a user data request.

- diameter-result-code result_code [ to result_code ]
  The Result-Code data field contains a space representing errors. Diameter provides the following classes of errors, all identified by the thousands digit in the decimal notation:
  - 3xxx (Protocol Errors)
  - 4xxx (Transient Failures)
  - 5xxx (Permanent Failure)
  result_code specifies either a result code value (diameter-result-code 3001) or a range of result code values (diameter-result-code 3000 to 9999) to which the failure-handling applies.

- action
  Configures the action to take depending on the diameter-result-code:
  - Continue the session
  - Retry and then terminate
- Terminate the session

**request-timeout action**

Configures the action to take as a result of a request timeout error:

- Continue the session
- Retry and then terminate
- Terminate the session

**Usage**

Configures all failure-handling parameters.

**Example**

The following command configures profile-update-request failure-handling using a result-code configuration with the terminate session option:

```bash
failure-handling profile-update-request diameter-result-code 3005 to 3600 action terminate
```
# request

Configures application request timeout.

## Product

- PDIF
- SCM

## Privilege

Administrator

## Mode

Exec > Global Configuration > Context Configuration > IMS Sh Interface Configuration

```
configure > context context_name > ims-sh-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ims-sh-service)#
```

## Syntax

```
request timeout secs

[ no | default ] request timeout
```

- **no**
  
  Disables a configured timeout request.

- **default**
  
  Default: 300 seconds
  
  Resets configuration to the default setting.

```
request timeout secs
```

Configures the request timeout in seconds.

- `secs` must be an integer from 1 through 300.

## Usage

Specifies the session request timeout period in seconds after which the request is deemed to have failed.

## Example

The following example configures the default timeout request of 300 seconds:

```
default request timeout
```
Chapter 174
IP VRF Context Configuration Mode Commands

The IP VRF Context Configuration Mode is used to create and manage the Virtual Routing and Forwarding (VRF) context instance for BGP/MPLS VPN, GRE, IPSec tunneling or service interfaces for virtual routing, addresses, address resolution options, etc.

Mode

Exec > Global Configuration > Context Configuration > IP VRF Context Configuration

configure > context context_name > ip vrf vrf_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-context-vrf)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
associate l2-mapping-table

Associates a global QoS-to-Level 2 mapping table with this VRF.

**Product**
ePDG
HSGW
P-GW
SAEGW
S-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > IP VRF Context Configuration

`configure > context context_name > ip vrf vrf_name`

Entering the above command sequence results in the following prompt:

```
[context_name] host_name(config-context-vrf)
```

**Syntax**

```
associate l2-mapping-table { name table_name | system-default }

no associate l2-mapping-table
```

**Usage**

Use this command to associates a global QoS-to-Level 2 mapping table with this VRF. Internal-QoS will be mapped to an actual L2 value (either or both of 802.1p/MPLS) using a per-VRF based table.

**Important:** If an l2-mapping-table association is made at both the VRF and VPN level, the VRF level takes precedence.
The mapping table is configured via the Global Configuration mode `qos l2-mapping-table` command.

The following command associates this VRF with Qos-to-L2 mapping table `vrf10`.

```
associate l2-mapping-table name vrf10
```
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

`exit`

**Usage**

Use this command to return to the parent configuration mode.
**ip guarantee**

Enables and disables local switching of framed route packets.

**Product**
- GGSN
- P-GW
- SAEGW

**Privilege**
- Administrator

**Mode**
- Exec > Global Configuration > Context Configuration
- `configure > context context_name`

Entering the above command sequence results in the following prompt:

```
[context_name] host_name(config-ctx)#
```

**Syntax**

```
[no] ip guarantee framed-route local-switching
```

- **no**
  
  Disables local switching of framed route packets.

- **framed-route local-switching**
  
  Enables local switching of framed route packets. By default, this functionality is disabled.

**Usage**

Use this command to enable and disable local switching of framed route packets. This functionality will be applicable only when there are some NEMO/framed route sessions in a context.

**Example**

The following command enables local switching of framed route packets:

```
ip guarantee framed-route local-switching
```
ip maximum-routes

This command configures the maximum number of routes in an IP VRF routing table configured in this context.

**Important:** This command should only be used for framed or NEMO (Network Mobility) routes of the VRF.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > IP VRF Context Configuration

```configure > context context_name > ip vrf vrf_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-context-vrf)#
```

**Syntax**

```
ip maximum-routes max_routes

no ip maximum-routes
```

- **no**
  Disables the configured maximum routes in specific IP VRF context.

- **max_routes**
  Sets the maximum number of routes in a specific IP VRF context.

  *`max_routes` must be an integer from 1 through 32768 or 65536 (release 17.0+).*

**Usage**

Use this command to configure the maximum number of routes in a particular VRF routing table. When the number of routes in the VRF is more than the maximum limit configured, a critical log is generated indicating that the number of routes is over the limit. Once the number of routes in the VRF goes under the limit, a clear log is generated.

The maximum routes configured using this command will be sent to the threshold configuration logic for appropriate action. For more information on threshold configuration, refer to descriptions of the `threshold route-service bgp-routes` and `threshold poll route-service interval` commands in the `Global Configuration Mode Commands` chapter.

**Example**

The following command sets 1000 routes as a maximum limit for specific VRF context:

```
    ip maximum-routes 1000
```
**mpls map-dscp-to-exp**

This command maps the final differentiated services code point (DSCP) bit value in the IP packet header to the final Experimental (EXP) bit value in the MPLS header for incoming traffic.

---

**Important**: This command has been deprecated beginning with Release 15.0.

**Product**

GGSN

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > IP VRF Context Configuration

```text
configure > context context_name > ip vrf vrf_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-context-vrf)#
```

**Syntax**

```text
[ no ] mpls map-dscp-to-exp dscp dscp_bit_value exp exp_bit_value
```

- **no**
  
  Disables the configured DSCP bit value mapping to the EXP bit value from a specific IP VRF context.

- **dscp dscp_bit_value**
  
  Specifies the final DSCP bit value which is to map with the final EXP bit value in MPLS header for incoming traffic.
  
  - *dscp_bit_value* specifies the value of DSCP bit values separated in eight groups and represented with integers from 0 through 7.
  
  The default representation of DSCP value in eight groups is given in the following table:

<table>
<thead>
<tr>
<th>DSCP Marking Value</th>
<th>DSCP Map Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>0-7</td>
<td>0</td>
</tr>
<tr>
<td>8-15</td>
<td>1</td>
</tr>
<tr>
<td>16-23</td>
<td>2</td>
</tr>
<tr>
<td>24-31</td>
<td>3</td>
</tr>
<tr>
<td>32-39</td>
<td>4</td>
</tr>
<tr>
<td>40-47</td>
<td>5</td>
</tr>
<tr>
<td>48-55</td>
<td>6</td>
</tr>
<tr>
<td>56-63</td>
<td>7</td>
</tr>
</tbody>
</table>
exp exp_bit_value

Specifies the final EXP bit value in MPLS header to which the final DSCP bit value 0 to 7 (represented in eight values) coming from incoming traffic will be mapped.

exp_bit_value is the value of EXP bit in MPLS header and must be an integer between 0 through 7.

Usage

Use this command to map the final DSCP value coming from incoming IP traffic to a final EXP value in MPLS header. This mapping determines the QoS and service parameters to which the packet is assigned.

Example

The following command maps the DSCP value 3 (24 to 31) to EXP bit 3 in MPLS header:

    mpls map-dscp-to-exp dscp 3 exp 3
**mpls map-exp-to-dscp**

Maps incoming the Experimental (EXP) bit value in MPLS header to the internal differentiated services code point (DSCP) bit value in IP packet headers for outgoing traffic.

**Important:** This command has been deprecated beginning with Release 15.0.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > IP VRF Context Configuration

```
configure > context context_name > ip vrf vrf_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-context-vrf)#
```

**Syntax**
```
[ no ] mpls map-exp-to-dscp exp exp_bit_value dscp dscp_bit_value
```

- **no**
  Disables the configured EXP bit value mapping to DSCP bit value from specific IP VRF context.

- **exp** `exp_bit_value`
  Specifies the incoming EXP bit value in MPLS header to which the internal DSCP bit value 0 to 7 (represented in 8 values) in IP traffic will be mapped.
  `exp_bit_value` is the value of the EXP bit in an MPLS header and must be an integer from 0 through 7.

- **dscp** `dscp_bit_value`
  Maps the DSCP bit value with the incoming EXP bit value in an MPLS header.
  `dscp_bit_value` specifies the value of the DSCP bit values separated in eight groups and represented with integers between 0 through 7.

The default representation of DSCP value in eight groups is given in the following table:

<table>
<thead>
<tr>
<th>DSCP Marking Value</th>
<th>DSCP Map Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>0-7</td>
<td>0</td>
</tr>
<tr>
<td>8-15</td>
<td>1</td>
</tr>
<tr>
<td>16-23</td>
<td>2</td>
</tr>
<tr>
<td>24-31</td>
<td>3</td>
</tr>
<tr>
<td>32-39</td>
<td>4</td>
</tr>
<tr>
<td>40-47</td>
<td>5</td>
</tr>
</tbody>
</table>
Usage
Use this command to map the incoming EXP bit value in MPLS headers to the DSCP bit value in IP traffic. This mapping determines the QoS and service parameters to which the packet is assigned.

Example
The following command maps the EXP bit value 4 to DSCP value 6 (48 to 55) in IP header:

```
mpls map-exp-to-dscp exp 4 dscp 6
```
Chapter 175
IPMS Client Configuration Mode Commands

The IPMS Client Configuration Mode is used to enable the Intelligent Packet Monitoring System (IPMS) client service on an Access Gateway and to set basic service-wide options in a context.

**Important:** This is a license enabled external application support. For more information on this product, refer to the *IPMS Installation and Administration Guide*.

**Mode**

Exec > Global Configuration > Context Configuration > IPMS Configuration

```
configure > context context_name > ipms
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-ipms)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

end

**Usage**

Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

exit

Usage
Use this command to return to the parent configuration mode.
export keys

Enables the encryption key export in specific key exchange events to IPMS server from IPMS-enabled AGW.

**Important:** This is a license enabled customer specific command.

**Product**
IPMS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > IPMS Configuration

```
configure > context context_name > ipms
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-ipms)#
```

**Syntax**

```
no
```

Removes the configured source IP address from this context for IPMS client communication with IPMS server.

```
ikeyv2
```

Enables the security association (SA) key export for Internet Key Exchange (IKEv2) protocol to IPMS server.

**Usage**
Monitor subscribers which have complaints of service availability or to monitor a test user for system verification.

**Example**
The following command assigns the IP address 10.2.3.4 to the IPMS client service in context to communicate with IPMS server. This is the IP address allocated for IPMS client service on chassis.

```
source address 10.2.3.4
```
heartbeat

Configures the IPMS heartbeating between the IPMS-enabled AGW and the IPMS server.

**Product**
IPMS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > IPMS Configuration

`configure > context context_name > ipms`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-ipms) #
```

**Syntax**

```
heartbeat period dur [ permitted-failure no_of_failures ]
[ no | default ] heartbeat
```

---

**default**

Configures the heartbeat period and permitted number of failures to the default values of 10 seconds and 1 failure respectively.

---

**no**

Disables/removes the configured heartbeat period and permitted number of failures.

---

**period dur**

Specifies the periodicity (in seconds) between heartbeat messages as an integer from 1 through 3600. Default: 10

---

**permitted-failure no_of_failures**

Specifies the number of errors/failures allowed before declaring an IPMS server as dead/unreachable as an integer from 1 through 10. Default: 1

---

**Usage**

Use this command to configure the heartbeat message periodicity and permissible failure of heartbeat message response before declaring an IPMS server as dead or unreachable. When an IPMS server is declared down an SNMP trap is sent.

---

**Example**

Following command configures the heartbeat message periodicity to 5 second and number of failures allowed as 3 to determine an IPMS server as dead.

```
heartbeat period 5 permitted-failure 3
```
server

Configures the IPMS server address and ports on which the IPMS client on an IPMS-enabled AGW communicates. This is the IP address and port range of the IPMS server.

Product
IPMS

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > IPMS Configuration
configure > context context_name > ipms

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx-ipms)#

Syntax

server address ip_address [ secondary ] [ start-port start_port [ end-port end_port ]][
secondary]

no server address ip_address

no

Removes the configured IPMS server IP address and port range from this context.

address ip_address

Specifies the IP address of the IPMS server to which the IPMS client service communicates in IPv4 dotted-decimal notation.
A maximum of 4 IPMS servers can be configured with this command in one context.

[ start-port start_port[ end-port end_port ]]

Default: 45001 source port
45005 end port

Specifies the range of UDP ports on which IPMS client communicates with the IPMS server.

start-port start_port: Specifies starting port number as an integer from 1 through 65535 that is less than end_port, if end-port is specified.
end-port end_port: Specifies the end port number as an integer from 1 through 65535 that is more than start_port.

secondary

The secondary keyword is used to configure the specified server address as secondary IP address on the IPMS client interface.
Usage
Use this command to configure/remove the IPMS servers. Up to 4 different IPMS servers can be configured with this command. UDP port number can also be configured with this command. IPMS client will search for this IP address to push the event and traffic logs.

Example
The following command configures IPMS server having IP address 10.2.3.4 in the IPMS client service export the event and traffic logs for intelligent packet monitoring functionality. It also specifies the UDP port range from 48000 to 48005 for communication.

server address 10.2.3.4 start-port 48000 end-port 48005
**source**

Configures the source address of the IPMS client in this context to communicate with the IPMS server. This is the IP address for IPMS client on the chassis.

**Product**

IPMS

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > IPMS Configuration

```
configure > context context_name > ipms
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-ipms)#
```

**Syntax**

```
source address ip_address
```

**address ip_address**

Specifies the IP address of the IPMS client on the AGW in this context. This is the address which is bound to the IPMS client service in this context. _ip_address_ is expressed in IPv4 dotted-decimal notation.

**Usage**

Monitor subscribers which have complaints of service availability or to monitor a test user for system verification.

**Example**

The following command assigns the IP address 10.2.3.4 to the IPMS client service in context to communicate with IPMS server. This is the IP address allocated for IPMS client service on chassis.

```
source address 10.2.3.4
```
Chapter 176
IPSec Transform Set Configuration Mode Commands

The IPSec Transform Set Configuration Mode is used to configure IPSec security parameters. There are two core protocols, the Authentication Header (AH) and Encapsulating Security Payload (ESP). AH may be considered redundant as ESP can provide the same authentication services that AH does.

Mode
Exec > Global Configuration > Context Configuration > IPSec Transform Set Configuration

configure > context context_name > ipsec transform-set set_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-context-vrf)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
encryption

Configures the appropriate IPSec ESP encryption algorithm and encryption key length. AES-CBC-128 is the default.

**Product**
- ePDG
- PDIF
- SCM

**Privilege**
- Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > IPSec Transform Set Configuration
configure > context context_name > ipsec transform-set set_name

Entering the above command sequence results in the following prompt:

```
[context_name] host_name(config-context-vrf)#
```

**Syntax**

```
encryption { 3des-cbc | aes-cbc-256 | des-cbc | null }
```

**default encryption**

<table>
<thead>
<tr>
<th>Encryption Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3des-cbc</td>
<td>Data Encryption Standard Cipher Block Chaining encryption applied to the message three times using three different cypher keys (triple DES).</td>
</tr>
<tr>
<td>aes-cbc-128</td>
<td>Advanced Encryption Standard Cipher Block Chaining with a key length of 128 bits. This is the default setting for this command.</td>
</tr>
<tr>
<td>aes-cbc-256</td>
<td>Advanced Encryption Standard Cipher Block Chaining with a key length of 256 bits.</td>
</tr>
<tr>
<td>null</td>
<td>The NULL encryption algorithm represents the optional use of applying encryption within ESP. ESP can then be used to provide authentication and integrity without confidentiality.</td>
</tr>
<tr>
<td>default</td>
<td>Sets the default IPSec ESP algorithm to AES-CBC-128.</td>
</tr>
</tbody>
</table>
Usage

In cipher block cryptography, the plaintext is broken into blocks usually of 64 or 128 bits in length. In cipher block chaining (CBC) each encrypted block is chained into the next block of plaintext to be encrypted. A randomly generated vector is applied to the first block of plaintext in lieu of an encrypted block. CBC provides confidentiality, but not message integrity. Because RFC 4307 calls for interoperability between IPSec and IKEv2, the IKEv2 confidentiality algorithms must be the same as those configured for IPsec in order for there to be an acceptable match during the IKE message exchange. In IKEv2, there is no NULL option.

Example

The following command configures the encryption to be the default aes-cbc-128:

```bash
default encryption
```
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Use this command to return to the parent configuration mode.
**group**

Configures the appropriate key exchange cryptographic strength and activate Perfect Forward Secrecy by applying a Diffie-Hellman group.

**Product**
- ePDG
- PDIF
- SCM

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration > Context Configuration > IPSec Transform Set Configuration

**Syntax**

```plaintext
configure > context context_name > ipsec transform-set set_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-context-vrf)#
```

**Syntax**

```plaintext
group { 1 | 2 | 5 | 14 | none }
```

- **default group**
  
  Configures the default crypto strength to be `none` and disables Perfect Forward Secrecy.

- **1**
  
  Configures crypto strength at the Group 1 level. Lowest security.

- **2**
  
  Configures crypto strength at the Group 2 level. Medium security.

- **5**
  
  Configures crypto strength at the Group 5 level. Higher security.

- **14**
  
  Configures crypto strength at the Group 14 level. Highest security.

- **none**
  
  Applies no group and disables Perfect Forward Secrecy. This is the default.

- **default**
  
  Sets the default Diffie-Hellman group algorithm to none. This also deactivates PFS.
Usage

Diffie-Hellman groups are used to determine the length of the base prime numbers used during the key exchange process. The cryptographic strength of any key derived depends, in part, on the strength of the Diffie-Hellman group upon which the prime numbers are based. Group 1 provides 768 bits of keying strength, Group 2 provides 1024 bits, Group 5 provides 1536 bits and Group 14 2048 bits. Selecting a group automatically activates Perfect Forward Secrecy. The default value is none, which disables PFS.

Example

This command configures security at Group 2 and activates PFS:

```
    group 2
```
hmac

Configures the IPsec ESP integrity algorithm using a Hash-based Message Authentication Code (HMAC).

**Product**
- ePDG
- PDIF
- SCM

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > IPSec Transform Set Configuration

```
configure > context context_name > ipsec transform-set set_name
```

Entering the above command sequence results in the following prompt:

```
[context_name] host_name(config-context-vrf)#
```

**Syntax**

```
hmac { aes-xcbc-96 | md5-96 | none | null | sha1-96 }
```

**default hmac**

```
default hmac
```

Sets the default IPSec hashing algorithm to SHA1-96.

**aes-xcbc-96**

AES-XCBC-96 uses a 128-bit secret key and produces a 128-bit authenticator value.

**md5-96**

MD5-96 uses a 128-bit secret key and produces a 128-bit authenticator value.

**null**

Configures the HMAC value to be null. The NULL encryption algorithm represents the optional use of applying encryption within ESP. ESP can then be used to provide authentication and integrity without confidentiality.

**sha1-96**

SHA-1 uses a 160-bit secret key and produces a 160-bit authenticator value. This is the default setting for this command.

**Usage**

HMAC is an encryption technique used by IPsec to make sure that a message has not been altered. A keyed-Hash-based Message Authentication Code (HMAC), is a type of message authentication code that is calculated using a cryptographic hash function in combination with a secret key to verify both data integrity
and message authenticity. A hash takes a message of any size and transforms it into a message of a fixed size: the authenticator value. This is truncated to 96 bits and transmitted. The authenticator value is reconstituted by the receiver and the first 96 bits are compared for a 100 percent match.

Example

The following command configures the default HMAC value (SHA1-96):

```
default hmac
```
mode

Configures the security of IP datagrams based on header placement. Tunnel mode applies security to a completely encapsulated IP datagram, while Transport does not. Default is Tunnel mode.

Product

- ePDG
- PDIF
- SCM

Privilege

- Security Administrator, Administrator

Mode

- Exec > Global Configuration > Context Configuration > IPSec Transform Set Configuration
- `configure > context context_name > ipsec transform-set set_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-context-vrf)#
```

Syntax

```
mode { transport | tunnel }
```

**default mode**

transport

In Transport mode, the IPSec header is applied only over the IP payload, not over the IP header in front of it. The AH and/or ESP headers appear between the original IP header and the IP payload, as follows:
- Original IP header, IPSec headers (AH and/or ESP), IP payload (including transport header).
- Transport mode is used for host-to-host communications and is generally unsuited to PDIF traffic.

---

tunnel

In Tunnel mode, the original IP header is left intact, so a complete IP datagram is encapsulated, forming a virtual tunnel between IPSec-capable devices. The IP datagram is passed to IPSec, where a new IP header is created ahead of the AH and/or ESP IPSec headers, as follows:
- New IP header, IPSec headers (AH and/or ESP), old IP header, IP payload.
- Tunnel mode is used for network-to-network communications (secure tunnels between routers) or host-to-host communications over the Internet.
- This is the default setting for this command.

---

**default mode**

Sets the default IPSec Mode to Tunnel.

---

**Usage**

IPSec modes are closely related to the function of the two core protocols, the Authentication Header (AH) and Encapsulating Security Payload (ESP). Both of these protocols provide protection by adding to a datagram a header (and possibly other fields) containing security information. The choice of mode does not
affect the method by which each generates its header, but rather, changes what specific parts of the IP datagram are protected and how the headers are arranged to accomplish this.

**Example**

The following command configures the default Tunnel mode:

```
default mode
```
Chapter 177
IPSG RADIUS Server Configuration Mode Commands

The IP Services Gateway (IPSG) RADIUS Server Configuration Mode is used to create and configure IPSG RADIUS Server/eWAG services in the current context. This mode enables configuring the system to receive RADIUS accounting requests as if it is a RADIUS accounting server, and reply after accessing those requests for subscriber information.

Mode

Exec > Global Configuration > Context Configuration > IPSG RADIUS Server Configuration

configure > context context_name > ipsg-service service_name mode radius-server

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ipsg-service-radius-server)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
accounting-context

This command allows you to specify the GTPP accounting context.

Product
eWAG

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > IPSG RADIUS Server Configuration

configure > context context_name > ipsg-service service_name mode radius-server

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ipsg-service-radius-server)#

Syntax

accounting-context context_name

no accounting-context

no

If previously configured, removes the accounting context configuration.

context_name

Specifies name of the GTPP accounting context.
context_name must be an alphanumeric string of 1 through 79 characters in length.

Usage

Use this command to specify the GTPP accounting context.

Example

The following command specifies to use the GTPP accounting context context12 for the eWAG service:

accounting-context context12
associate sgtp-service

This command allows you to associate an SGTP service with the current eWAG service.

**Product**
eWAG

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > IPSG RADIUS Server Configuration

```shell
configure > context context_name > ipsg-service service_name mode radius-server
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipsg-service-radius-server)#
```

**Syntax**

```bash
associate sgtp-service sgtp_service_name [ context sgtp_context_name ]
```

**no associate sgtp-service**

If previously configured, removes the service association from the configuration.

**sgtp-service sgtp_service_name**

Specifies name of the SGTP service to associate with this service.

*sgtp_service_name* must be the name of an SGTP service, and must be an alphanumeric string of 1 through 63 characters in length.

**context sgtp_context_name**

Specifies name of the context in which the SGTP service is configured.

*sgtp_context_name* must be the name of the context, and must be an alphanumeric string of 1 through 63 characters in length.

If a context is not specified, the current context is used.

**Usage**

Use this command to associate an SGTP service with the IPSG service. This enables the GTP functionality for eWAG supporting GTP-C (GTP Control Plane) messaging and GTP-U (GTP User Data Plane) messaging between eWAG and GGSN over the Gn' interface.

**Important:** Any change to this configuration will result in restart of the eWAG service.

**Example**

The following command associates an SGTP service named *service1*, configured in the context named *context2*, with the IPSG service:
associate sgtp-service service1 context context2


**bind**

This command allows you to bind the current IPSG/eWAG service to a logical AAA interface, and specify the number of subscriber sessions allowed.

**Product**
eWAG
IPSG

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > IPSG RADIUS Server Configuration

configure > context context_name > ipsg-service service_name mode radius-server

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ipsg-service-radius-server)#

**Syntax**

```bash
bind accounting-proxy address ipv4/ipv6_address [ max-subscribers max_sessions | port port_number | source-context source_context ]

bind address ipv4/ipv6_address [ disconnect-message [ src-port source_port_number ] | max-subscribers max_sessions | port port_number | source-context source_context ]+

bind authentication-proxy address ipv4/ipv6_address [ acct-port port_number | auth-port port_number | max-subscribers max_sessions | source-context source_context ]

no bind
```

**no**

If previously configured, removes the binding for the service.

```bash
bind accounting-proxy address ipv4/ipv6_address [ max-subscribers max_sessions | port port_number | source-context source_context ]

• accounting-proxy address ipv4/ipv6_address: Specifies the IP address of the interface where accounting proxy requests are received by this service in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

• max-subscribers max_sessions: Specifies the maximum number of subscriber sessions allowed for the service. If this option is not configured, the system defaults to the license limit.

  In StarOS 9.0 and later releases, max_sessions must be an integer from 0 through 4000000.

  In StarOS 8.3 and earlier releases, max_sessions must be an integer from 0 through 3000000.

• port port_number: Specifies the port number of the interface where accounting requests are received by this service.

  port_number must be an integer from 1 through 65535.

  Default: 1813
```
**source-context** *source_context*: Specifies the source context where RADIUS accounting requests are received.

*source_context* must be an alphanumeric string of 1 through 79 characters.

This keyword should be configured if the source of the RADIUS requests is in a different context than the IPSG service. If this keyword is not configured, the system will default to the context in which the IPSG service is configured.

```
bind address ipv4/ipv6_address [ disconnect-message [ src-port source_port_number ] | max-subscribers max_sessions | port port_number | source-context source_context ]+
```

- **address** *ipv4/ipv6_address*: Specifies the IP address of the interface where accounting requests are received by this service in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

- **disconnect-message** [ *src-port* source_port_number ]: Specifies to send RADIUS disconnect message to the configured RADIUS accounting client in call failure scenarios.

  *src-port* *source_port_number*: Specifies the port number to which the disconnect message must be sent.

  *source_port_number* must be an integer from 1 through 65535.

- **max-subscribers** *max_sessions*: Specifies the maximum number of subscriber sessions allowed for the service. If this option is not configured, the system defaults to the license limit.

  In StarOS 9.0 and later releases, *max_sessions* must be an integer from 0 through 4000000.

  In StarOS 8.3 and earlier releases, *max_sessions* must be an integer from 0 through 3000000.

- **port** *port_number*: Specifies the port number of the interface where accounting requests are received by this service.

  *port_number* must be an integer from 1 through 65535.

  Default: 1813

- **source-context** *source_context*: Specifies the source context where RADIUS accounting requests are received.

  *source_context* must be an alphanumeric string of 1 through 79 characters.

  This keyword should be configured if the source of the RADIUS requests is in a different context than the IPSG service. If this keyword is not configured, the system will default to the context in which the IPSG service is configured.

```
bind authentication-proxy address ipv4/ipv6_address [ acct-port port_number | auth-port port_number | max-subscribers max_sessions | source-context source_context ]
```

- **authentication-proxy address** *ipv4/ipv6_address*: Specifies the IP address of the interface where authentication proxy requests are received by this service in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

**Important**: Enabling authentication proxy also enables accounting proxy.

- **acct-port** *port_number*: Specifies the port number of the interface where accounting proxy requests are received by this service.

  *port_number* must be an integer from 0 through 65535.
Default: 1813

• **auth-port** *port_number*: Specifies the port number of the interface where authentication proxy requests are received by this service.

  *port_number* must be an integer from 0 through 65535.

  Default: 1812

• **max-subscribers** *max_sessions*: Specifies the maximum number of subscriber sessions allowed for the service. If this option is not configured, the system defaults to the license limit.

  In StarOS 9.0 and later releases, *max_sessions* must be an integer from 0 through 4000000.

  In StarOS 8.3 and earlier releases, *max_sessions* must be an integer from 0 through 3000000.

• **source-context** *source_context*: Specifies the source context where RADIUS accounting requests are received.

  *source_context* must be an alphanumeric string of 1 through 79 characters.

  This keyword should be configured if the source of the RADIUS requests is in a different context then the IPSG service. If this keyword is not configured, the system will default to the context in which the IPSG service is configured.

### Usage

Use this command to bind the IPSG RADIUS Server/eWAG service to a logical AAA interface and specify the number of allowed subscriber sessions. If the AAA interface is not located in this context, configure the **source-context** parameter.

Use the accounting and authentication proxy settings to enable RADIUS proxy server functionality on the IPSG. These commands are used when the NAS providing the RADIUS request messages is incapable of sending them to two separate devices. The IPSG in RADIUS Server mode proxies the RADIUS request and response messages while performing the user identification task in order to provide services to the session.

### Example

The following command binds the service to a AAA interface with and IP address of 10.2.3.4 located in the source context named **aaa ingress**:

```shell
bind address 10.2.3.4 source-context aaa_ingress
```
connection authorization

This command allows you to configure the RADIUS authorization password that must be matched by the RADIUS accounting requests received by the current IPSG service.

Product

IPSG

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > Context Configuration > IPSG RADIUS Server Configuration
configure > context context_name > ipsg-service service_name mode radius-server

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ipsg-service-radius-server)#

Syntax

connection authorization [ encrypted ] password password

no connection authorization

no

Deletes the RADIUS authorization from the current IPSG RADIUS Server service.

[ encrypted ] password password

- encrypted: Specifies that the RADIUS authorization password is encrypted.
- password password: Specifies the password that must be matched by incoming RADIUS accounting requests.

In StarOS 12.2 and later releases, password with encryption must be an alphanumeric string of 1 through 132 characters, and without encryption an alphanumeric string of 1 through 63 characters.

In StarOS 12.1 and earlier releases, password must be an alphanumeric string of 1 through 63 characters.

Usage

The IPSG RADIUS server service does not terminate RADIUS user authentication so the user password is unknown.

Use this command to configure the authorization password that the RADIUS accounting requests must match in order for the service to examine and extract user information.

Example

The following command sets the RADIUS authorization password that must be matched by the RADIUS accounting requests sent to this service. The password is encrypted, and the password used in this example is “secret”.

connection authorization encrypted password secret
**end**

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
```
end
```

**Usage**
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

`exit`

**Usage**

Use this command to return to the parent configuration mode.
gtp max-contexts-per-imsi

This command allows you to configure multiple primary contexts having the same IMSI number.

Product eWAG
Privilege Security Administrator, Administrator
Mode Exec > Global Configuration > Context Configuration > IPSG RADIUS Server Configuration configure > context context_name > ipsg-service service_name mode radius-server

Entering the above command sequence results in the following prompt:
[context_name]host_name(config-ipsg-service-radius-server)#

Syntax

```
gtp max-contexts-per-imsi max_value min-nsapi min_nsapi_value
default gtp max-contexts-per-imsi
```

**default gtp max-contexts-per-imsi**

```
default
Configures this command to disable use of multiple primary contexts. Only one PDP context per user is allowed.
max-contexts-per-imsi: 1
min-nsapi: 15
```

**max-contexts-per-imsi max_value**

Specifies the limit for the maximum number of contexts per IMSI.
```
max_value must be an integer from 1 through 11.
```

**min-nsapi min_nsapi_value**

Specifies the range of NSAPI values to be assigned to different PDP context of the same subscriber.
```
min_nsapi_value must be an integer from 5 through 15.
```

**Usage**

Use this command to configure the maximum number of contexts per IMSI, and the range of NSAPI values to be assigned to different PDP context.

**Example**

The following command configures the maximum contexts per IMSI to 5 and specify the range of values NSAPI value to 7.
```
gtp max-context-per-imsi 5 min-nsapi 7
```
**gtp peer-ip-address**

This command allows you to configure GGSN IP address under the eWAG service.

**Product**
eWAG

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > IPSG RADIUS Server Configuration

```
configure > context context_name > ipsg-service service_name mode radius-server
```

Entering the above command sequence results in the following prompt:

```
/context_name/host_name(config-ipsg-service-radius-server)#
```

**Syntax**

```
gtp peer-ip-address ipv4_address

no gtp peer-ip-address
```

**Usage**

Use this command to configure the GGSN IP address under the eWAG service.

This command replaces the hidden mode command

```
[ no ] ggsn-ip-address ipv4_address
```

**Example**

The following command configures the GGSN IP address 1.2.3.4 under the current eWAG service.

```
gtp peer-ip-address 1.2.3.4
```
ip

This command enables you to configure IP parameters for the current eWAG service.

**Product**
eWAG

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > IPSG RADIUS Server Configuration

configure > context context_name > ipsg-service service_name mode radius-server

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ipsg-service-radius-server)#

**Syntax**

```plaintext
ip { gnp-qos-dscp | qos-dscp } qci { { { 1 | 2 | 3 | 4 | 9 } | { 5 | 6 | 7 | 8 } allocation-retention-priority { 1 | 2 | 3 } } { af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be | ef | pt } } +

default ip { gnp-qos-dscp | qos-dscp }

no ip { gnp-qos-dscp | qos-dscp } qci { { { 1 | 2 | 3 | 4 | 9 } | { 5 | 6 | 7 | 8 } allocation-retention-priority { 1 | 2 | 3 } } +

default
```

- **QCI-based DSCP map:**
  - qci 1: ef
  - qci 2: ef
  - qci 3: af11
  - qci 4: af11
  - qci 5: ef
  - qci 6: ef
  - qci 7: af21
  - qci 8: af21
  - qci 9: be

- **ARP-based DSCP map for interactive class:**
  - qci 5 allocation-retention-priority 1: ef
  - qci 5 allocation-retention-priority 2: ef
  - qci 5 allocation-retention-priority 3: ef
  - qci 6 allocation-retention-priority 1: ef
• qci 6 allocation-retention-priority 2: ef
• qci 6 allocation-retention-priority 3: ef
• qci 7 allocation-retention-priority 1: af21
• qci 7 allocation-retention-priority 2: af21
• qci 7 allocation-retention-priority 3: af21
• qci 8 allocation-retention-priority 1: af21
• qci 8 allocation-retention-priority 2: af21
• qci 8 allocation-retention-priority 3: af21

no

Resets configured value for specified QCI with its default setting.

gnp-qos-dscp

Specifies, for uplink direction, the DiffServ Code Point marking to be used for sending packets of a particular 3GPP QoS class.

qos-dscp

Specifies, for downlink direction, the DiffServ Code Point marking to be used for sending packets of a particular 3GPP QoS class.

qci { 1 | 2 | 3 | 4 | 9 }

Specifies the QCI attribute of QoS.

• 1: QCI 1 attribute of QoS
• 2: QCI 2 attribute of QoS
• 3: QCI 3 attribute of QoS
• 4: QCI 4 attribute of QoS
• 9: QCI 9 attribute of QoS

qci { 5 | 6 | 7 | 8 } allocation-retention-priority { 1 | 2 | 3 }

Specifies the QCI attribute of QoS with ARP.

• 5: QCI 5 attribute of QoS
• 6: QCI 6 attribute of QoS
• 7: QCI 7 attribute of QoS
• 8: QCI 8 attribute of QoS

allocation-retention-priority { 1 | 2 | 3 }: Specifies the ARP.

af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be | ef | pt

Specifies the Per-Hop Forwarding Behavior (PHB) to use.

• af11: Assured Forwarding 11 PHB
• af12: Assured Forwarding 12 PHB
• af13: Assured Forwarding 13 PHB
- af21: Assured Forwarding 21 PHB
- af22: Assured Forwarding 22 PHB
- af23: Assured Forwarding 23 PHB
- af31: Assured Forwarding 31 PHB
- af32: Assured Forwarding 32 PHB
- af33: Assured Forwarding 33 PHB
- af41: Assured Forwarding 41 PHB
- af42: Assured Forwarding 42 PHB
- af43: Assured Forwarding 43 PHB
- be: Best Effort Forwarding PHB
- ef: Expedited Forwarding PHB
- pt: Pass Through (do not modify the ToS)

Usage
Use this command to configure IP parameters for the eWAG service.

Example
The following command specifies to configure the DiffServ Code Point marking to be used for sending packets specifying QCI as 1 and Assured Forwarding 11 PHB:

```
ip gnp-qos-dscp qci 1 af11
```
map ue-mac-to-imei

This command allows you to map the UE MAC received in the Calling-Station-Id RADIUS attribute to IMEIsV in order to forward it in the GTP CPC message to the GGSN.

Product

eWAG

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > Context Configuration > IPSG RADIUS Server Configuration

configure > context context_name > ipsg-service service_name mode radius-server

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ipsg-service-radius-server)#

Syntax

[ default | no ] map ue-mac-to-imei

default

If previously configured, disables mapping of UE MAC address to IMEIsV IE of GTP message in order to forward it to GGSN.
Default: Mapping is disabled.

no

If previously configured, disables mapping of UE MAC address to IMEIsV IE of GTP message in order to forward it to GGSN.

Usage

Use this command to enable or disable mapping of UE MAC address to IMEIsV IE of GTP message in order to forward it to GGSN.
overlapping-ip-address

This command allows you to enable or disable overlapping of IP addresses which enables multiple users to use the same IP address.

Product
IPSG

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > IPSG RADIUS Server Configuration
configure > context context_name > ipsg-service service_name mode radius-server

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ipsg-service-radius-server)#

Syntax

[ default | no ] overlapping-ip-address

<table>
<thead>
<tr>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>If previously configured, disables IPSG support of overlapping IP addresses. Using overlapping IP addresses is disabled by default.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>no</th>
</tr>
</thead>
<tbody>
<tr>
<td>If previously configured, disables IPSG support of overlapping IP addresses.</td>
</tr>
</tbody>
</table>

Usage
Use this command to enable or disable overlapping IP addresses for subscribers on different networks that are independent of each other.

Example
The following command enables IPSG overlapping of IP addresses:

overlapping-ip-address
plmn id

This command allows you to configure Public Land Mobile Network (PLMN) identifier for the current eWAG service.

Product

eWAG

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > Context Configuration > IPSG RADIUS Server Configuration

configure > context context_name > ipsg-service service_name mode radius-server

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ipsg-service-radius-server)#

Syntax

plmn id mcc mcc_number mnc mnc_number

no plmn id

If previously configured, deletes the PLMN ID configuration.

mcc mcc_number

Specifies the mobile country code (MCC) part of the PLMN identifier for the eWAG service. mcc_number must be a three-digit number ranging from 200 to 999.

mnc mnc_number

Specifies the mobile network code (MNC) part of the PLMN identifier for the eWAG service. mnc_number must be a two- or three-digit number ranging from 00 to 999.

Usage

Use this command to configure the location-specific mobile network identifiers included in the Routing Area Identity (RAI) field of the PDP Create Request messages sent to the GGSN.

Important: Any change to this configuration will result in restart of the eWAG service.

Example

The following command configures the PLMN identifier for the eWAG service as MCC 333 and MNC 99:

plmn id mcc 333 mnc 99
profile

This command allows you to configure the IPSG/eWAG service to use APN or subscriber profile.

**Important:** In release 14.0, eWAG service uses only the APN profile. In release 15.0, ReWAG uses the APN profile and DeWAG uses the subscriber profile. Whereas, the IPSG service uses both APN and subscriber profiles.

**Product**

eWAG

**IPSG**

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > IPSG RADIUS Server Configuration

configure > context context_name > ipsg-service service_name mode radius-server

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipsg-service-radius-server)#
```

**Syntax**

```
profile { APN [ default-apn apn_name ] | subscriber }
```

**default profile**

```
default
```

Configures this command with its default setting.

Default: APN

**APN**

Specifies to use APN profile for the service.

```
default-apn apn_name
```

**Important:** This option is supported only for the eWAG service.

Specifies the default APN to be used for the eWAG service.

`apn_name` must be the name of an APN, it must be an alphanumeric string of 1 through 62 characters in length, and can consist only of the alphabetic characters (A–Z and a–z), digits (0–9), dot (.), and the hyphen (-).

**subscriber**

**Important:** This option is supported only for the IPSG RADIUS Server service, and in release 15.0 for DeWAG service. For the DeWAG service, this command must be configured with the `subscriber` option. This is because
DeWAG will operate based on subscriber template profile selection only for connecting users. If the APN profile selection is configured, the DeWAG service will not be started.

Specifies to use subscriber profile for the service.

Usage
Use this command to set the service to support APN profiles (supporting Gx through the enabling of `ims-auth-service`) or for basic subscriber profile lookup.
For the DeWAG service, this command must be configured with the `subscriber` option. This is because DeWAG will operate based on subscriber template profile selection only for connecting users. If the APN profile selection is configured, the DeWAG service will not be started.

Example
The following command specifies to use the subscriber profile:

```
profile subscriber
```
radius accounting

This command allows you to specify the IP address and shared secret of the RADIUS accounting client from which RADIUS accounting requests are received. The RADIUS client can be either the access gateway or the RADIUS accounting server depending on which device is sending accounting requests.

Product
- eWAG
- IPSG

Privilege
- Security Administrator
- Administrator

Mode
- Exec > Global Configuration > Context Configuration > IPSG RADIUS Server Configuration
- configure > context context_name > ipsg-service service_name mode radius-server

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ipsg-service-radius-server)#

Syntax

radius accounting { client { ipv4/ipv6_address | ipv4/ipv6_address/mask } [ encrypted ] key key [ acct-onoff [ aaa-context aaa_context_name ] [ aaa-group aaa_server_group_name ] [ clear-sessions ] + ] [ dictionary dictionary ] [ disconnect-message [ release-on-acct-stop acct_stop_wait_timeout ] [ dest-port destination_port_number ] + ] [ interim create-new-call | validate-client-ip ]

no radius accounting { client { ipv4/ipv6_address | ipv4/ipv6_address/mask } | interim create-new-call | validate-client-ip }

default radius accounting { interim create-new-call | validate-client-ip }

no

If previously configured, removes the specified configuration.

ipv4/ipv6_address | ipv4/ipv6_address/mask

Specifies the IP address, and optionally subnet mask of the RADIUS client from which RADIUS accounting requests are received.

ipv4/ipv6_address/ipv4/ipv6_address/mask must be in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

A maximum of 16 IP addresses can be configured.

[ encrypted ] key key

- **encrypted**: Specifies that the shared key between the RADIUS client and this service is encrypted.
- **key key**: Specifies the shared key between the RADIUS client and this service.

In StarOS 12.2 and later releases, **key** with encryption must be an alphanumeric string of 1 through 236 characters, and without encryption an alphanumeric string of 1 through 127 characters. Note that **key** is case sensitive.
radius accounting

In StarOS 12.1 and earlier releases, key must be an alphanumerical string of 1 through 127 characters and is case sensitive.

```
acct-onoff [ aaa-context aaa_context_name ] [ aaa-group aaa_server_group_name ] [ clear-sessions ] +
```

**Important:** In release 12.3 and earlier releases, this option is applicable only to the IPSG Proxy Mode.

**Important:** In release 14.0 and later releases, this option is applicable to the IPSG Proxy and Server Modes.

Specifies to proxy accounting On/Off messages to AAA server.
- **aaa-context aaa_context_name**: Specifies the context to find AAA server groups. If not specified, by default, the AAA context will be the source context.
  
  `aaa_context_name` must be the name of a AAA context, and must be an alphanumerical string of 1 through 79 characters.

- **aaa-group aaa_server_group_name**: Specifies the AAA server group. If not specified, by default, the AAA server group will be `default`.
  
  `aaa_server_group_name` must be the name of AAA server group, and must be an alphanumerical string of 1 through 63 characters.

- **clear-sessions**: Specifies to clear eWAG or IPSG sessions on receiving accounting On/Off messages.

- **+**: Indicates that more than one of the preceding options may be specified in a single command.

**dictionary dictionary**

Specifies the dictionary to use.

**Important:** In this release, eWAG supports only the `starent-vas1` dictionary.

**dictionary** can be one of the following:

<table>
<thead>
<tr>
<th>Dictionary</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3gpp2</td>
<td>This dictionary consists not only of all of the attributes in the standard dictionary, but also all of the attributes specified in IS-835-A.</td>
</tr>
<tr>
<td>3gpp2-835</td>
<td>This dictionary consists not only of all of the attributes in the standard dictionary, but also all of the attributes specified in IS-835.</td>
</tr>
<tr>
<td>customX</td>
<td>These are customized dictionaries. For information on custom dictionaries, please contact your Cisco account representative. X is the integer value of the custom dictionary.</td>
</tr>
<tr>
<td>standard</td>
<td>This dictionary consists only of the attributes specified in RFC 2865, RFC 2866, and RFC 2869.</td>
</tr>
<tr>
<td>starent</td>
<td>This dictionary consists of all of the attributes in the starent-vas1 dictionary and incorporates additional Starent Networks VSAs by using a two-byte VSA Type field. This dictionary is the master-set of all of the attributes in all of the dictionaries supported by the system.</td>
</tr>
</tbody>
</table>
Dictionary | Description
--- | ---
starent-835 | This dictionary consists of all of the attributes in the starent-va1-835 dictionary and incorporates additional Starent Networks VSAs by using a two-byte VSA Type field. This dictionary is the master-set of all of the attributes in all of the -835 dictionaries supported by the system.

Important: In StarOS 12.0 and later releases, no new attributes can be added to the starent-va1 dictionary. If there are new attributes to be added, you can only add them to the starent dictionary. For more information, please contact your Cisco account representative.

starent-va1 | This dictionary consists not only of the 3GPP2 dictionary, but also includes Starent Networks vendor-specific attributes (VSAs) as well. The VSAs in this dictionary support a one-byte wide VSA Type field in order to support certain RADIUS applications. The one-byte limit allows support for only 256 VSAs (0–255). This is the default dictionary.

Important: For information on the specific dictionary to use for your deployment contact your Cisco account representative.

starent-va1-835 | This dictionary consists not only of the 3GPP2-835 dictionary, but also includes Starent Networks vendor-specific attributes (VSAs) as well. The VSAs in this dictionary support a one-byte wide VSA Type field in order to support certain RADIUS applications. The one-byte limit allows support for only 256 VSAs (0–255). This is the default dictionary.

### disconnect-message

```
[ release-on-acct-stop acct_stop_wait_timeout ] [ dest-port destination_port_number ]
```

Specifies to send RADIUS disconnect message to the configured RADIUS accounting client in call failure scenarios.

- **release-on-acct-stop acct_stop_wait_timeout**: Specifies to wait for the accounting stop request after sending the Packet of Disconnect (PoD) to the client for the specified time. This keyword is disabled by default.
  - `acct_stop_wait_timeout` must be an integer from 10 through 300 seconds. This indicates the time to wait to clear the call in case IPSG does not receive any accounting stop for the subscriber after sending the PoD.
  - This keyword is configured on a per RADIUS accounting client basis and not for the entire service.

- **dest-port destination_port_number**: Specifies the port number to which the disconnect message must be sent.
  - `destination_port_number` must be an integer from 1 through 65535.

### interim create-new-call

**Important**: This option does not apply to the IPSG Proxy Mode.

Specifies to create a new session upon receipt of a RADIUS interim message.

Default: Disabled

---

**validate-client-ip**

Specifies to enable the ipsgmgr to validate RADIUS accounting messages from different configured RADIUS client IP address, and forward requests to the session manager.
Default: The RADIUS client IPs are validated.

Usage

Use this command to configure the communication parameters for the RADIUS client from which RADIUS accounting requests are received.

Example

The following command configures the service to communicate with a RADIUS client with an IP address of 10.2.3.4 and an encrypted shared secret of key1234:

```
radius accounting client 10.2.3.4 encrypted key key1234
```
radius dictionary

This command allows you to specify the RADIUS dictionary for the current IPSG/eWAG service.

Product
- eWAG
- IPSG

Privilege
- Security Administrator
- Administrator

Mode
- Exec > Global Configuration > Context Configuration > IPSG RADIUS Server Configuration
- configure > context context_name > ipsg-service service_name mode radius-server

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ipsg-service-radius-server)#

Syntax

radius dictionary  dictionary_name

default radius dictionary

default
- Specifies to use the default dictionary.
- Default: starent-vsa1

dictionary  dictionary_name
- Specifies the dictionary to use.

Important: In 15.0 and later releases, for DeWAG use the starent dictionary.

dictionary_name must be one of the following.

<table>
<thead>
<tr>
<th>Dictionary</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3gpp2</td>
<td>This dictionary consists not only of all of the attributes in the standard dictionary, but also all of the attributes specified in IS-835-A.</td>
</tr>
<tr>
<td>3gpp2-835</td>
<td>This dictionary consists not only of all of the attributes in the standard dictionary, but also all of the attributes specified in IS-835.</td>
</tr>
<tr>
<td>customXX</td>
<td>These are customized dictionaries. For information on custom dictionaries, please contact your Cisco account representative. xx is the integer value of the custom dictionary.</td>
</tr>
<tr>
<td>standard</td>
<td>This dictionary consists only of the attributes specified in RFC 2865, RFC 2866, and RFC 2869.</td>
</tr>
<tr>
<td>starent</td>
<td>This dictionary consists of all of the attributes in the starent-vsa1 dictionary and incorporates additional Starent Networks VSAs by using a two-byte VSA Type field. This dictionary is the master-set of all of the attributes in all of the dictionaries supported by the system.</td>
</tr>
</tbody>
</table>
**radius dictionary**

<table>
<thead>
<tr>
<th>Dictionary</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>starent-835</td>
<td>This dictionary consists of all of the attributes in the starent-vsa1-835 dictionary and incorporates additional Starent Networks VSAs by using a two-byte VSA Type field. This dictionary is the master-set of all of the attributes in all of the -835 dictionaries supported by the system.</td>
</tr>
<tr>
<td>starent-vs1</td>
<td>This dictionary consists not only of the 3GPP2 dictionary, but also includes Starent Networks vendor-specific attributes (VSAs) as well. The VSAs in this dictionary support a one-byte wide VSA Type field in order to support certain RADIUS applications. The one-byte limit allows support for only 256 VSAs (0–255). This is the default dictionary.</td>
</tr>
<tr>
<td>starent-vs1-835</td>
<td>This dictionary consists not only of the 3GPP2-835 dictionary, but also includes Starent Networks vendor-specific attributes (VSAs) as well. The VSAs in this dictionary support a one-byte wide VSA Type field in order to support certain RADIUS applications. The one-byte limit allows support for only 256 VSAs (0–255). This is the default dictionary.</td>
</tr>
</tbody>
</table>

**Important:** For information on the specific dictionary to use for your deployment contact your Cisco account representative.

**Usage**

Use this command to specify the RADIUS dictionary to use for the IPSG RADIUS Server/eWAG service.

**Example**

The following command specifies to use the `custom10` RADIUS dictionary:

```
radius dictionary custom10
```
**sess-replacement**

This command allows you to enable/disable the Session Replacement feature for eWAG and IPSG services.

**Product**
- eWAG
- IPSG

**Privilege**
- Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > IPSG RADIUS Server Configuration

```bash
configure > context context_name > ipsg-service service_name mode radius-server
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipsg-service-radius-server)#
```

**Syntax**

```bash
 sess-replacement { with-diff-acct-sess-id | with-diff-ip | with-diff-key [ with-diff-acct-sess-id ] }

{ default | no } sess-replacement
```

- **default**
  - Configures this command with its default setting.
  - Default: Disabled.

- **no**
  - If previously configured, deletes the configuration.

- **with-diff-acct-sess-id**
  - Specifies to replace current session when a new session request comes with same IP address and same user name/IMSI but different accounting session ID.

- **with-diff-ip**
  - Specifies to replace current session when a new session request comes with same user name/IMSI but different IP address.

- **with-diff-key**
  - Specifies to replace current session when a new session request comes with same IP address but different user name/IMSI.

For IPSG, you can also use a combination of replacement options of different key and different account session ID.
Usage
Use this command to enable/disable the Session Replacement feature. By default, the Session Replacement feature is disabled.

Example
The following command enables session replacement specifying to replace the current session when a new session request comes with same user name/IMSI but different IP address:

```
sess-replacement with-diff-ip
```
setup-timeout

This command allows you to configure a timeout for session setup attempts for the current IPSG/eWAG service.

**Product**
eWAG
IPSG

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > IPSG RADIUS Server Configuration

```
configure > context context_name > ipsg-service service_name mode radius-server
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipsg-service-radius-server)#
```

**Syntax**

```
setup-timeout setup_timeout_seconds
```

**default setup-timeout**

```
default
```

Configures this command with its default setting.
Default: 60 seconds

```
setup_timeout_seconds
```

Specifies the time period, in seconds, for which a session setup attempt is allowed to continue before being terminated.

`setup_timeout_seconds` must be an integer from 1 through 1000000.

**Usage**

Use this command to configure a timeout for IPSG/eWAG session setup attempts.

**Example**

The following command configures the timeout for session setup attempts to 30 seconds:

```
setup-timeout 30
```
w-apn

This command allows you to configure the W-APNs that can be connected through DeWAG, and the default-gateway IP addresses to be used by the UEs for connecting to the W-APN network.

Product:
eWAG

Privilege:
Security Administrator, Administrator

Mode:
Exec > Global Configuration > Context Configuration > IPSG RADIUS Server Configuration
configure > context context_name > ipsg-service service_name mode radius-server

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ipsg-service-radius-server)#

Syntax:

w-apn apn_name default-gw ipv4/ipv6_address/maskbits +

no w-apn apn_name

If previously configured, removes the specified configuration.

apn-name apn_name

Specifies the APN name.

apn_name must be the name of an APN and must be a string of 1 to 62 characters in length consisting of alphabetic characters (A-Z and a-z), digits (0-9), dot(.) and the dash (-). This value is compared against the subscribed APN returned by the AAA server or locally configured APN in the subscriber-template configuration to find the default-gateway IP address to be used in DHCP signaling packets.

default-gw ipv4/ipv6_address/maskbits

Specifies the IP address of the default gateway to be used by UE for W-APN access. You can configure a maximum of four default gateways per W-APN. Multiple default-gateways are possible as the APN can have different pools of different subnet with different default-gateway IP addresses.

ipv4/ipv6_address/maskbits must be an IPv4/IPv6 address and subnet-mask, for example 192.168.1.1/24.

This value should be in the same subnet as that of UE allocated IP address from GGSN for the W-APN. GGSN does not supply subnet-mask along with IP address. Therefore, the identification of whether GGSN-allocated IP address is in same subnet or not is done with the help of configured “/maskbits”. This default-gateway value is sent to the UE as default-gateway IP address using “Router” option in DHCP-OFFER message. The maskbits is sent to the UE as subnet-mask using the “Subnet Mask” option in DHCP-OFFER message.
Usage

Use this command to configure the list of W-APN names that can be connected through DeWAG and the default-gateway IP addresses to be used by UE for connecting to the W-APN network. During DHCP signaling the configured default-gateway value will be notified to UE as the router. This command also configures the subnet-mask to be used for the respective default-gateway IP address in order to find the network prefix of the default-gateway.

Note that DeWAG will be acting as 'default-gateway' for the UE in its connected network.

Important: This command can be configured a maximum of four times to configure four different APNs and the corresponding default-gateways.

Example

The following command configures an APN named apn123 with the default gateway IP address and mask 192.168.1.1/24:

```
  w-apn apn123 default-gw 192.168.1.1/24
```
Chapter 178
IPSG RADIUS Snoop Configuration Mode Commands

The IP Services Gateway (IPSG) RADIUS Snoop Configuration Mode is used to create and configure IPSG services within the current context. The IPSG RADIUS Snoop Mode configures the system to inspect RADIUS accounting requests on the way to the RADIUS accounting server and extract user information.

Mode

Exec > Global Configuration > Context Configuration > IPSG RADIUS Snoop Configuration

```
configure > context context_name > ipsg-service service_name mode radius-snoop
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipsg-service-radius-snoop)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
bind

This command allows you to configure the service to accept data on any interface configured in the context. Optionally, you can also configure the system to limit the number of sessions processed by this service.

Product
IPSG

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > IPSG RADIUS Snoop Configuration
configure > context context_name > ipsg-service service_name mode radius-snoop

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ipsg-service-radius-snoop)#

Syntax

bind [ max-subscribers max_sessions ]

no bind

If previously configured, deletes the binding configuration for the service.

max-subscribers max_sessions

Specifies the maximum number of subscriber sessions allowed for the service. If this option is not configured, the system defaults to the license limit.
In StarOS 9.0 and later releases, max_sessions must be an integer from 0 through 4000000.
In StarOS 8.3 and earlier releases, max_sessions must be an integer from 0 through 3000000.

Usage

Use this command to initiate the service and begin accepting data on any interface configured in the context.

Example

The following command prepares the system to receive subscriber sessions on any interface in the context and limits the sessions to 10000:

    bind max-subscribers 10000
connection authorization

This command allows you to configure the RADIUS authorization password that must be matched by the RADIUS accounting requests “snooped” by this service.

**Product**
IPSG

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > IPSG RADIUS Snoop Configuration

```
configure > context context_name > ipsg-service service_name mode radius-snoop
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipsg-service-radius-snoop)#
```

**Syntax**

```
connection authorization [ encrypted ] password password

no connection authorization
```

- **no**

  Deletes the RADIUS connection authorization configuration from the current IPSG RADIUS snoop service.

  ```
  [ encrypted ] password password
  ```

- **encrypted**: Specifies that the received RADIUS authorization password is encrypted.

- **password password**: Specifies the password that must be matched by incoming RADIUS accounting requests.

  In StarOS 12.2 and later releases, `password` with encryption must be an alphanumeric string of 1 through 132 characters, and without encryption an alphanumeric string of 1 through 63 characters.

  In StarOS 12.1 and earlier releases, `password` must be an alphanumeric string of 1 through 63 characters.

**Usage**

RADIUS accounting requests being examined by the IPSG RADIUS snoop service are destined for a RADIUS Accounting Server. Since the “snoop” service does not terminate user authentication, the user password is unknown.

Use this command to configure the authorization password that the RADIUS accounting requests must match in order for the service to examine and extract user information.

**Example**

The following command sets the RADIUS authorization password that must be matched by the RADIUS accounting requests “snooped” by this service. The password is encrypted, and the password used in this example is “secret”.

```
connection authorization encrypted password secret
```
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**
Use this command to return to the parent configuration mode.
profile

This command allows you to configure the service to use APN or subscriber profile.

Product
IPSG

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > IPSG RADIUS Snoop Configuration

configure > context context_name > ipsg-service service_name mode radius-snoop

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ipsg-service-radius-snoop)#

Syntax

profile { APN | subscriber }

default profile

default

Configures this command with its default setting.

APN

Specifies the service to support APN configuration required to enable Gx support.

subscriber

Specifies the service to support subscriber profile lookup.

Usage

Use this command to set the service to support APN profiles (supporting Gx through the enabling of ims-auth-service) or for basic subscriber profile lookup.

Example

The following command specifies to use the subscriber profile:

    profile subscriber
radius

This command allows you to specify the RADIUS accounting servers where accounting requests are sent after being “inspected” by this service.

**Product**
IPSG

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > IPSG RADIUS Snoop Configuration

```
configure > context context_name > ipsg-service service_name mode radius-snoop
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipseg-service-radius-snoop)#
```

**Syntax**

```
[ no ] radius { accounting server ipv4/ipv6_address [ port port_number | source-context context_name ] } | dictionary { 3gpp2 | 3gpp2-835 | custom XX | standard | starent | starent-835 | starent-vsai | starent-vsai-835 }
```

- **no**
  Removes the RADIUS accounting server identifier from this service.

- **radius accounting server ipv4/ipv6_address**
  Specifies the IP address of a RADIUS accounting server where accounting requests are sent after being “snooped” by this service in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation. Up to 16 addresses can be configured.

- **port port_number**
  Specifies the port number of the RADIUS Accounting Server where accounting requests are sent after being “snooped” by this service.
  
  `port_number` must be an integer from 1 through 65535.
  
  Default: 1813

- **source-context context_name**
  Specifies the source context where RADIUS accounting requests are received.
  
  `context_name` must be an alphanumeric string of 1 through 79 characters.
  
  If this keyword is not configured, the system will default to the context in which the IPSG service is configured.

- **dictionary { 3gpp2 | 3gpp2-835 | custom XX | standard | starent | starent-835 | starent-vsai | starent-vsai-835 }**
  Specifies what dictionary to use. The possible values are described in the following table:

<table>
<thead>
<tr>
<th>Dictionary</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Dictionary Description

<table>
<thead>
<tr>
<th>Dictionary</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3gpp</td>
<td>This dictionary consists not only of all of the attributes in the standard dictionary, but also all of the attributes specified in 3GPP 32.015.</td>
</tr>
<tr>
<td>3gpp2</td>
<td>This dictionary consists not only of all of the attributes in the standard dictionary, but also all of the attributes specified in IS-835-A.</td>
</tr>
<tr>
<td>3gpp2-835</td>
<td>This dictionary consists not only of all of the attributes in the standard dictionary, but also all of the attributes specified in IS-835.</td>
</tr>
</tbody>
</table>
| customXX     | These are customized dictionaries. For information on custom dictionaries, please contact your Cisco account representative.  
XX is the integer value of the custom dictionary. |
| standard     | This dictionary consists only of the attributes specified in RFC 2865, RFC 2866, and RFC 2869.                                                |
| starent      | This dictionary consists of all of the attributes in the starent-vsa1 dictionary and incorporates additional Starent Networks VSAs by using a two-byte VSA Type field. This dictionary is the master-set of all of the attributes in all of the dictionaries supported by the system. |
| starent-835  | This dictionary consists of all of the attributes in the starent-vsa1-835 dictionary and incorporates additional Starent Networks VSAs by using a two-byte VSA Type field. This dictionary is the master-set of all of the attributes in all of the -835 dictionaries supported by the system. |
| starent-vsa1 | This dictionary consists not only of the 3gpp2 dictionary, but also includes Starent Networks vendor-specific attributes (VSAs) as well. The VSAs in this dictionary support a one-byte wide VSA Type field in order to support certain RADIUS applications. The one-byte limit allows support for only 256 VSAs (0–255). This is the default dictionary. |
| starent-vsa1-835 | This dictionary consists not only of the 3gpp2-835 dictionary, but also includes Starent Networks vendor-specific attributes (VSAs) as well. The VSAs in this dictionary support a one-byte wide VSA Type field in order to support certain RADIUS applications. The one-byte limit allows support for only 256 VSAs (0–255). This is the default dictionary. |

### Usage
Use this command to specify the RADIUS Accounting Servers where accounting requests are sent after being snooped by this service.

### Example
The following command specifies the IP address (10.2.3.4) of a RADIUS Accounting Server whose accounting requests are to be “snooped”, and the source context (aaa_ingress) where the requests are received on the system:

```
radius accounting server 10.2.3.4 source-context aaa_ingress
```
sess-replacement

This command allows you to enable/disable session replacement.

Important: This command is not supported in this release. The Session Replacement feature is under development for future use.

Product
IPSG

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > IPSG RADIUS Snoop Configuration
configure > context context_name > ipsg-service service_name mode radius-snoop

Entering the above command sequence results in the following prompt:

/context_name>host_name(config-ipsg-service-radius-snoop)#

Syntax

```
(sess-replacement { with-diff-acct-sess-id | with-diff-ip | with-diff-key }
{ default | no } sess-replacement
```

- **default**
  Configures this command with its default setting.
  Default: Disabled.

- **no**
  If previously configured, deletes the configuration.

- **with-diff-acct-sess-id**
  Specifies to replace current session when a new session request comes with same IP address and same user name/IMSI but different accounting session ID.

- **with-diff-ip**
  Specifies to replace current session when a new session request comes with same user name/IMSI but different IP address.

- **with-diff-key**
  Specifies to replace current session when a new session request comes with same IP address but different user name/IMSI.
Usage
Use this command to enable/disable session replacement. By default, session replacement is disabled.

Example
The following command enables session replacement specifying to replace the current session when a new session request comes with same user name/IMSI but different IP address:

```
sess-replacement with-diff-ip
```
setup-timeout

This command allows you to configure the timeout value for IPSG session setup attempts.

Product
IPSG

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > IPSG RADIUS Snoop Configuration

configure > context context_name > ipsg-service service_name mode radius-snoop

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ipsg-service-radius-snoop)#

Syntax

setup-timeout setup_timeout

default setup-timeout

setup_timeout

Specifies the period of time (in seconds) the IPSG session setup is allowed to continue before the setup attempt is terminated.

setup_timeout must be an integer from 1 through 1000000.

Default: 60

Usage

Use this command to prevent IPSG session setup attempts from continuing without termination.

Example

The following command configures the session setup timeout setting to 20 seconds:

setup-timeout 20
Chapter 179
IPSP Configuration Mode Commands

The IPSP Configuration Mode is used to configure properties for the IP Pool Sharing Protocol (IPSP). System-based HA services use IPSP during an offline-software upgrade to avoid the assignment of duplicate IP addresses to sessions while allowing them to maintain the same address, and to preserve network capacity.

**Important:** For information on configuring and using IPSP refer to the *System Administration Guide*.

Exec > Global Configuration > Context Configuration > Ethernet Interface Configuration > IP Pool Sharing Protocol Configuration

```plaintext
configure > context context_name > interface interface_name broadcast > pool-share-protocol { primary ip_address | secondary ip_address }
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
dead-interval

Configures the retry time to connect to the remote system for the IP Pool Sharing Protocol.

Product

- PDSN
- HA

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > Context Configuration > Ethernet Interface Configuration > IP Pool Sharing Protocol Configuration

```
configure > context context_name > interface interface_name broadcast > pool-share-protocol { primary ip_address | secondary ip_address }
```

Syntax

```
dead-interval seconds

[ no | default ] dead-interval
```

<table>
<thead>
<tr>
<th>no</th>
</tr>
</thead>
</table>
| Disables the dead interval. On loss of connectivity to the remote system, no retries are attempted and the remote system is marked dead immediately on failure.

<table>
<thead>
<tr>
<th>default</th>
</tr>
</thead>
</table>
| Resets the dead interval to the default of 3600 seconds.

<table>
<thead>
<tr>
<th>seconds</th>
</tr>
</thead>
</table>
| Default: 3600 seconds
| The amount of time in seconds to wait before retrying the remote system. seconds must be an integer from 25 through 259200.

Usage

Use this command to set the amount of time to wait before retrying to connect with the remote system for the IP pool sharing protocol.

Example

Use the following command to set the interval to 180 seconds (3 minutes):

```
dead-interval 180
```
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
end
```

**Usage**
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

exit

**Usage**

Use this command to return to the parent configuration mode.
reserved-free-percentage

This command is used to set the amount of free addresses reserved for use on the primary HA.

Product
PDSN
HA

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Ethernet Interface Configuration > IP Pool Sharing Protocol Configuration

configure > context context_name > interface interface_name broadcast > pool-share-protocol { primary ip_address | secondary ip_address }

Syntax
reserved-free-percentage value

default reserved-free-percentage

value
Default: 100
value specifies the percentage of free addresses reserved for the use on the primary HA for IP pool sharing during upgrade. It must be an integer from 0 through 100.

Usage
This command is used with pool-sharing-protocol active mode on the primary HA. Before using this command, pool-sharing-protocol in the Ethernet Interface Configuration Mode must be configured. For more information, refer to the Ethernet Interface Configuration Mode Commands chapter in this guide.

Example
To reserve 40 percent of free addresses in primary HA for IP pool sharing, enter the following command:

reserved-free-percentage 40
Chapter 180
IPv6 ACL Configuration Mode Commands

The IPv6 Access Control List Configuration Mode is used to create and manage IPv6 access privileges.

Mode

Exec > Global Configuration > Context Configuration > IPv6 ACL Configuration

configure > context context_name > ipv6 access-list ipv6_acl_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ipv6-acl)#

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
deny/permit (by source IP address masking)

Used to filter subscriber sessions based on the IPv6 address mask sent by the source to the mobile node or the network.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > IPv6 ACL Configuration

```
configure > context context_name > ipv6 access-list ipv6_acl_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipv6-acl)#
```

**Syntax**

```
{ deny | permit } [ log ] source_address source_wildcard
after { deny | permit } [ log ] source_address source_wildcard
before { deny | permit } [ log ] source_address source_wildcard
no { deny | permit } [ log ] source_address source_wildcard
```

- **after**
  
  Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed. This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

- **before**
  
  Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed. This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

- **Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

- **no**
  
  Removes the rule which exactly matches the options specified.

- **deny | permit**
  
  Specifies the rule is either block (deny) or an allow (permit) filter.

- **Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.
- **deny**: Indicates the rule, when matched, drops the corresponding packets.
- **permit**: Indicates the rule, when matched, allows the corresponding packets.

**log**

Default: packets are not logged.
Indicates all packets which match the filter are to be logged.

**source_address**

The IP address(es) form which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the `source_wildcard` parameter.

**source_wildcard**

This option is used in conjunction with the `source_address` option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:
- Zero-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be ignored.

**Important**: The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

**Usage**

Define a rule when any packet from the IP addresses which fall into the group of addresses matching the IP address masking. This allows the reduction of filtering rules as it does not require a rule for each source and destination pair.

**Important**: The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the Engineering Rules appendix in the System Administration Guide.

**Example**

The following command defines two rules with the second logging filtered packets:

```
permit 2001:4A2B::1f3F
deny log 2001:4A2B::1f3F
```

The following sets the insertion point to before the first rule defined above:

```
before permit 2001:4A2B::1f3F
```

The following command sets the insertion point after the second rule defined above:

```
after deny log 2001:4A2B::1f3F
```
The following deletes the first rule defined above:

```
no permit 2001:4A2B::1f3F
```
deny/permit (any)

Used to filter subscriber sessions based on any packet received. This command is also used to set the access control list insertion point.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > IPv6 ACL Configuration

configure > context context_name > ipv6 access-list ipv6_acl_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ipv6-acl)#

Syntax

{ deny | permit } [ log ] any

after { deny | permit } [ log ] any

before { deny | permit } [ log ] any

no { deny | permit } [ log ] any

after

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

Important: If the options specified do not exactly match an existing rule, the insertion point does not change.

before

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

Important: If the options specified do not exactly match an existing rule, the insertion point does not change.

no

Removes the rule which exactly matches the options specified.
deny | permit

Specifies the rule is either block (deny) or an allow (permit) filter.

- **deny**: Indicates the rule, when matched, drops the corresponding packets.
- **permit**: Indicates the rule, when matched, allows the corresponding packets.

log

Default: packets are not logged.
Indicates all packets which match the filter are to be logged.

any

Indicates all packets will match the filter regardless of source and/or destination.

---

**Usage**

Define a catch all rule to place at the end of the list of rules.

**Important**: It is suggested that any rule which is added to be a catch all should also have the `log` option specified. The logged packets may be used to determine if the current list of rules is adequate or needs modification to ensure proper security. The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the Engineering Rules appendix in the System Administration Guide.

**Example**

The following command defines two rules with the second logging filtered packets:

```bash
permit any
deny log any
```

The following sets the insertion point to before the first rule defined above:

```bash
before permit any
```

The following command sets the insertion point after the second rule defined above:

```bash
after deny log any
```

The following deletes the first rule defined above:

```bash
no permit any
```
deny/permit (by host IP address)

Used to filter subscriber sessions based on the targeted host IP address sent by the source to the mobile node or the network.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > IPv6 ACL Configuration

```
configure > context context_name > ipv6 access-list ipv6_acl_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipv6-acl)#
```

**Syntax**

```
{ deny | permit } [ log ] host source_host_address
after { deny | permit } [ log ] host source_host_address
before { deny | permit } [ log ] host source_host_address
no { deny | permit } [ log ] host source_host_address
```

**after**
Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

**before**
Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

**no**
Removes the rule which exactly matches the options specified.
deny | permit

Specifies the rule is either block (deny) or an allow (permit) filter.

- **deny**: Indicates the rule, when matched, drops the corresponding packets.
- **permit**: Indicates the rule, when matched, allows the corresponding packets.

log

Default: packets are not logged.
Indicates all packets which match the filter are to be logged.

source_host_address

The IP address of the source host to filter against expressed in IPv6 colon notation.

### Usage

Define a rule when a very specific remote host is to be blocked. In simplified networks where the access controls need only block a few hosts, this command allows the rules to be very clear and concise.

**Important**: The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*.

### Example

The following command defines two rules with the second logging filtered packets:

```
permit host 2001:4A2B::1f3F
deny log host 2001:4A2B::1f3F
```

The following sets the insertion point to before the first rule defined above:

```
before permit host 2001:4A2B::1f3F
```

The following command sets the insertion point after the second rule defined above:

```
after deny log host 2001:4A2B::1f3F
```

The following deletes the first rule defined above:

```
no permit host 2001:4A2B::1f3F
```
deny/permit (by source ICMP packets)

Used to filter subscriber sessions based on the internet control message protocol packets sent by the source to the mobile node or the network.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > IPv6 ACL Configuration
configure > context context_name > ipv6 access-list ipv6_acl_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ipv6-acl)#

Syntax

{ deny | permit } [ log ] icmp { source_address source_wildcard | any | host source_host_address } { dest_address dest_wildcard | any | host dest_host_address } [ icmp_type [ icmp_code ] ]

after { deny | permit } [ log ] icmp { source_address source_wildcard | any | host source_host_address } { dest_address dest_wildcard | any | host dest_host_address } [ icmp_type [ icmp_code ] ]

before { deny | permit } [ log ] icmp { source_address source_wildcard | any | host source_host_address } { dest_address dest_wildcard | any | host dest_host_address } [ icmp_type [ icmp_code ] ]

no { deny | permit } [ log ] icmp { source_address source_wildcard | any | host source_host_address } { dest_address dest_wildcard | any | host dest_host_address } [ icmp_type [ icmp_code ] ]

after

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

Important: If the options specified do not exactly match an existing rule, the insertion point does not change.

before

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.
**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

- **no**
  Removes the rule which exactly matches the options specified.

- **deny | permit**
  Specifies the rule is either block (deny) or an allow (permit) filter.
  - **deny**: Indicates the rule, when matched, drops the corresponding packets.
  - **permit**: Indicates the rule, when matched, allows the corresponding packets.

- **log**
  Default: packets are not logged.
  Indicates all packets which match the filter are to be logged.

- **source_address**
  The IP address(es) from which the packet originated.
  This option is used to filter all packets from a specific IP address or a group of IP addresses.
  When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the **sourceWildcard** parameter.

- **sourceWildcard**
  This option is used in conjunction with the **source_address** option to specify a group of addresses for which packets are to be filtered.
  The mask must be entered as a complement:
  - Zero-bits in this parameter mean that the corresponding bits configured for the **source_address** parameter must be identical.
  - One-bits in this parameter mean that the corresponding bits configured for the **source_address** parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

- **any**
  Specifies that the rule applies to all packets.

- **host**
  Specifies that the rule applies to a specific host as determined by its IP address.

- **sourceHost_address**
  The IP address of the source host to filter against expressed in IPv6 hexadecimal-colon-separated notation.

- **destHost_address**
  The IP address of the destination host to filter against expressed in IPv6 hexadecimal-colon-separated notation.
**dest_address**

The IP address(es) to which the packet is to be sent. This option is used to filter all packets to a specific IP address or a group of IP addresses. When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the **dest_wildcard** parameter.

**dest_wildcard**

This option is used in conjunction with the **dest_address** option to specify a group of addresses for which packets are to be filtered. The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the **dest_address** parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the **dest_address** parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

**icmp_type**

Specifies that all ICMP packets of a particular type are to be filtered. The type is an integer from 0 through 255.

**icmp_code**

Specifies that all ICMP packets of a particular code are to be filtered. The type is an integer from 0 through 255.

**Usage**

Define a rule to block ICMP packets which can be used for address resolution and possible be a security risk. The IP filtering allows flexible controls for pairs of individual hosts or groups by IP masking which allows the filtering of entire subnets if necessary.

**Important:** The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*.

**Example**

The following command defines two rules with the second logging filtered packets:

```
permit icmp host 2001:4A2B::1f3F4 any 168
```

```
deny log icmp 2001:4A2B::1f3F 2001:4a2b::1f00 host fe80::a02:410 168 11
```

The following sets the insertion point to before the first rule defined above:

```
before permit icmp host 2001:4A2B::1f3F any 168
```

The following command sets the insertion point after the second rule defined above:
deny/permit (by source ICMP packets)

```
  after deny log icmp 2001:4A2B::1f3F 2001:4a2b::1f00 host fe80::a02:410
  168 11

  The following deletes the first rule defined above:

  no permit icmp host 2001:4A2B::1f3F any 168
```
deny/permit (by IP packets)

Used to filter subscriber sessions based on the internet protocol packets sent by the source to the mobile node or the network.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > IPv6 ACL Configuration

```
configure > context context_name > ipv6 access-list ipv6_acl_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipv6-acl)\#`

**Syntax**

```
{ deny | permit } [ log ] ip { source_address source_wildcard | any | host source_host_address } { dest_address dest_wildcard | any | host dest_host_address } [ fragment ] [ protocolnum ]
```

**after**
Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

**before**
Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.
deny/permit (by IP packets)

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Removes the rule which exactly matches the options specified.</td>
</tr>
<tr>
<td>deny</td>
<td>permit</td>
</tr>
<tr>
<td>log</td>
<td>Default: packets are not logged. Indicates all packets which match the filter are to be logged.</td>
</tr>
<tr>
<td>source_address</td>
<td>The IP address(es) form which the packet originated. This option is used to filter all packets from a specific IP address or a group of IP addresses. When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the source_wildcard parameter.</td>
</tr>
<tr>
<td>source_wildcard</td>
<td>This option is used in conjunction with the source_address option to specify a group of addresses for which packets are to be filtered. The mask must be entered as a complement:</td>
</tr>
<tr>
<td>any</td>
<td>Specifies that the rule applies to all packets.</td>
</tr>
<tr>
<td>host</td>
<td>Specifies that the rule applies to a specific host as determined by its IP address.</td>
</tr>
<tr>
<td>source_host_address</td>
<td>The IP address of the source host to filter against expressed in IPv6 colon notation.</td>
</tr>
<tr>
<td>dest_host_address</td>
<td>The IP address of the destination host to filter against expressed in IPv6 colon notation.</td>
</tr>
</tbody>
</table>

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.
IPv6 ACL Configuration Mode Commands

deny/permit (by IP packets)

---

**dest_address**

The IP address(es) to which the packet is to be sent. This option is used to filter all packets to a specific IP address or a group of IP addresses. When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the `dest_wildcard` parameter.

---

**dest_wildcard**

This option is used in conjunction with the `dest_address` option to specify a group of addresses for which packets are to be filtered. The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the `dest_address` parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the `dest_address` parameter must be ignored.

---

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

---

**fragment**

Indicates packet filtering is to be applied to IP packet fragments only.

---

**protocol num**

Indicates that the packet filtering is to be applied to a specific protocol number. `num` can be any integer ranging from 0 to 255.

---

**Usage**

Block IP packets when the source and destination are of interest.

---

**Important:** The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the Engineering Rules appendix in the System Administration Guide.

---

**Example**

The following command defines two rules with the second logging filtered packets:

```plaintext
permit ip host 2001:4A2B::1f3F any fragment
deny log ip 2001:4A2B::1f3F 2001:4a2b::1f00 host fe80::a02:410
```

The following sets the insertion point to before the first rule defined above:

```plaintext
before permit ip host 2001:4A2B::1f3F any fragment
```

The following command sets the insertion point after the second rule defined above:

```plaintext
after deny log ip 2001:4A2B::1f3F 2001:4a2b::1f00 host fe80::a02:410
```

The following deletes the first rule defined above:

```plaintext
no permit ip host 2001:4A2B::1f3F any fragment
```
deny/permit (by TCP/UDP packets)

Used to filter subscriber sessions based on the transmission control protocol/user datagram protocol packets sent by the source to the mobile node or the network.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > IPv6 ACL Configuration
configure > context context_name > ipv6 access-list ipv6_acl_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipv6-acl)#
```

**Syntax**

```
{ deny | permit } [ log ] { tcp | udp } { { source_address source_wildcard | any | host source_host_address } [ eq source_port | gt source_port | lt source_port | neq source_port ] } { { dest_address dest_wildcard | any | host dest_host_address } [ eq dest_port | gt dest_port | lt dest_port | neq dst_port ] }
```

```
{ { source_address source_wildcard | any | host source_host_address } [ eq source_port | gt source_port | lt source_port | neq source_port ] } { { dest_address dest_wildcard | any | host dest_host_address } [ eq dest_port | gt dest_port | lt dest_port | neq dst_port ] }
```

```
{ { { source_address source_wildcard | any | host source_host_address } [ eq source_port | gt source_port | lt source_port | neq source_port ] } [ eq dest_port | gt dest_port | lt dest_port | neq dst_port ] }
```

```
{ deny | permit } [ log ] { tcp | udp } { { source_address source_wildcard | any | host source_host_address } [ eq source_port | gt source_port | lt source_port | neq source_port ] } { { dest_address dest_wildcard | any | host dest_host_address } [ eq dest_port | gt dest_port | lt dest_port | neq dst_port ] }
```

**after**
Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.
before
Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

no
Removes the rule which exactly matches the options specified.

deny | permit
Specifies the rule is either block (deny) or an allow (permit) filter.
  *deny:* Indicates the rule, when matched, drops the corresponding packets.
  *permit:* Indicates the rule, when matched, allows the corresponding packets.

log
Default: packets are not logged.
Indicates all packets which match the filter are to be logged.

tcp | udp
Specifies the filter is to be applied to IP-based transmission control protocol or the user datagram protocol.
  *tcp:* Filter applies to TCP packets.
  *udp:* Filter applies to UDP packets.

source_address
The IP address(es) form which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the source wildcard parameter.

source wildcard
This option is used in conjunction with the source_address option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:
  *Zero-bits in this parameter mean that the corresponding bits configured for the source_address parameter must be identical.
  *One-bits in this parameter mean that the corresponding bits configured for the source_address parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

any
Specifies that the rule applies to all packets.
host
Specifies that the rule applies to a specific host as determined by its IP address.

source_host_address
The IP address of the source host to filter against expressed in IPv6 colon-separated-hexadecimal notation.

dest_host_address
The IP address of the destination host to filter against expressed in IPv6 colon-separated-hexadecimal notation.

eq source_port
Specifies a single, specific source TCP port number to be filtered.
source_port must be configured to an integer from 0 through 65535.

gt source_port
Specifies that all source TCP port numbers greater than the one specified are to be filtered.
source_port must be configured to an integer from 0 through 65535.

lt source_port
Specifies that all source TCP port numbers less than the one specified are to be filtered.
source_port must be configured to an integer from 0 through 65535.

neq source_port
Specifies that all source TCP port numbers not equal to the one specified are to be filtered.
source_port must be configured to an integer from 0 through 65535.

dest_address
The IP address(es) to which the packet is to be sent.
This option is used to filter all packets to a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the dest_wildcard parameter.

dest_wildcard
This option is used in conjunction with the dest_address option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:
- Zero-bits in this parameter mean that the corresponding bits configured for the dest_address parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the dest_address parameter must be ignored.

Important: The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

eq dest_port
Specifies a single, specific destination TCP port number to be filtered.
**deny/permit (by TCP/UDP packets)**

`dest_port` must be configured to an integer from 0 through 65535.

---

`gt dest_port`

Specifies that all destination TCP port numbers greater than the one specified are to be filtered.
`dest_port` must be configured to an integer from 0 through 65535.

---

`lt dest_port`

Specifies that all destination TCP port numbers less than the one specified are to be filtered.
`dest_port` must be configured to an integer from 0 through 65535.

---

`neq dest_port`

Specifies that all destination TCP port numbers not equal to the one specified are to be filtered.
`dest_port` must be configured to an integer from 0 through 65535.

---

**Usage**

Block IP packets when the source and destination are of interest but for only a limited set of ports.

---

**Important:** The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the Engineering Rules appendix in the System Administration Guide.

---

**Example**

The following command defines four rules with the second and fourth rules logging filtered packets:

```plaintext
permit tcp host 2001:4A2B::1f3F any
deny log udp 2001:4A2B::1f3F 2001:4a2b::1f00 host fe80::a02:410
permit tcp host 2001:4A2B::1f3F gt 1023 any
```

The following sets the insertion point to before the first rule defined above:

```plaintext
before permit tcp host 2001:4A2B::1f3F any
```

The following command sets the insertion point after the second rule defined above:

```plaintext
after deny log udp 2001:4A2B::1f3F 2001:4a2b::1f00 host fe80::a02:410
```

The following deletes the third rule defined above:

```plaintext
no permit tcp host 2001:4A2B::1f3F gt 1023 any
```
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
dend
```

**Usage**

Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

`exit`

**Usage**

Use this command to return to the parent configuration mode.
readdress server

Alter the destination address and port number in TCP or UDP packet headers to redirect packets to a different server.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > IPv6 ACL Configuration

```bash
configure > context context_name > ipv6 access-list ipv6_acl_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipv6-acl)#
```

**Syntax**

`after`
Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed. This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

`before`
Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed. This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

`no`
Removes the rule which exactly matches the options specified.

`redirect_address`
The IP address to which the IP packets are redirected. TCP or UDP packet headers are rewritten to contain the new destination address. This must expressed in IPv6 colon-separated-hexadecimal notation.

`port port_number`
The number of the port at the redirect address where the packets are sent. TCP or UDP packet headers are rewritten to contain the new destination port number.
IPv6 ACL Configuration Mode Commands

**tcp | udp**

Specifies the redirect is to be applied to the IP-based transmission control protocol or the user datagram protocol.

- **tcp**: Redirect applies to TCP packets.
- **udp**: Redirect applies to UDP packets.

**source_address**

The IP address(es) from which the packet originated. This option is used to filter all packets from a specific IP address or a group of IP addresses. When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the `source_wildcard` parameter.

**any**

Specifies that the rule applies to all packets.

**host**

Specifies that the rule applies to a specific host as determined by its IP address.

**source_host_address**

The IP address of the source host to filter against expressed in IPv6 colon notation.

**dest_host_address**

The IP address of the destination host to filter against expressed in IPv6 colon-separated-hexadecimal notation.

**eq source_port**

Specifies a single, specific source TCP port number to be filtered. `source_port` must be configured to an integer from 0 through 65535.

**gt source_port**

Specifies that all source TCP port numbers greater than the one specified are to be filtered. `source_port` must be configured to an integer from 0 through 65535.

**lt source_port**

Specifies that all source TCP port numbers less than the one specified are to be filtered. `source_port` must be configured to an integer from 0 through 65535.

**neq source_port**

Specifies that all source TCP port numbers not equal to the one specified are to be filtered. `source_port` must be configured to an integer from 0 through 65535.

**dest_address**

The IP address(es) to which the packet is to be sent. This option is used to filter all packets to a specific IP address or a group of IP addresses. When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the `dest_wildcard` parameter.
**eq dest_port**

Specifies a single, specific destination TCP port number to be filtered. `dest_port` must be configured to an integer from 0 through 65535.

**gt dest_port**

Specifies that all destination TCP port numbers greater than the one specified are to be filtered. `dest_port` must be configured to an integer from 0 through 65535.

**lt dest_port**

Specifies that all destination TCP port numbers less than the one specified are to be filtered. `dest_port` must be configured to an integer from 0 through 65535.

**neq dest_port**

Specifies that all destination TCP port numbers not equal to the one specified are to be filtered. `dest_port` must be configured to an integer from 0 through 65535.

**Usage**

Use this command to define a rule that redirects packets to a different destination address. The TCP and UDP packet headers are modified with the new destination address and destination port.

**Important:** The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the Engineering Rules appendix in the System Administration Guide. Also note that “redirect” rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

**Example**

The following command defines a rule that redirects packets to the server at `fe80::c0a8:a04`, UDP packets coming from any host with a destination of any host are matched:

```
readdress server fe80::c0a8:a04 udp any any
```

The following sets the insertion point to before the rule defined above:

```
before readdress server fe80::c0a8:a04 udp any any
```

The following deletes the rule defined above:

```
no readdress server fe80::c0a8:a04 udp any any
```
redirect context (by IP address masking)

Used to redirect subscriber sessions based on the IP address mask sent by the source to the mobile node or the network.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > IPv6 ACL Configuration

```
configure > context context_name > ipv6 access-list ipv6_acl_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipv6-acl)#
```

**Syntax**

```
redirect context context_id [ log ] source_address source_wildcard

after redirect context context_id [ log ] source_address source_wildcard

before redirect context context_id [ log ] source_address source_wildcard

no redirect context context_id [ log ] source_address source_wildcard
```

**after**
Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

**before**
Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

**no**
Removes the rule which exactly matches the options specified.
IPv6 ACL Configuration Mode Commands

redirect context (by IP address masking)

context context_id
Specifies the context identification number of the context to which packets are redirected. At the executive
mode prompt, use the show context all command to display context names and context IDs.

log
Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

source_address
Filters by the IP address(es) from which the packet originated. This option filters all packets from a specific
IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then
be configured using the source_wildcard parameter.

source_wildcard
Filters packets for a group of addresses specified in conjunction with the source_address option.
The mask must be entered as a complement:
• Zero-bits in this parameter mean that the corresponding bits configured for the source_address
  parameter must be identical.
• One-bits in this parameter mean that the corresponding bits configured for the source_address
  parameter must be ignored.

Important: The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

Usage
Define a rule when any packet from the IP addresses which fall into the group of addresses matching the IP
address masking. This allows the reduction of redirect rules as it does not require a rule for each source and
destination pair.

Important: The maximum number of rules that can be configured per ACL varies depending on how the ACL is
to be used. For more information, refer to the Engineering Rules appendix in the System Administration Guide. Also
note that “redirect” rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific
context.

Example
The following command defines a rule that redirects packets to the context with the context ID of 23 and the
source IP and wildcard of 2002::c6a2:1600 and 2002::c6a2:1600:

   redirect context 23 2002::c6a2:1600 2002::c6a2:1600

The following sets the insertion point to before the first rule defined above:

   before redirect context 23 2002::c6a2:1600 2002::c6a2:1600

The following command sets the insertion point after the second rule defined above:

   after redirect context 23 2002::c6a2:1600 2002::c6a2:1600
The following deletes the first rule defined above:

```
no redirect context 23 2002::c6a2:1600 2002::c6a2:1600
```
redirect context (any)

Used to redirect subscriber sessions based on any packet received. This command is also used to set the access control list insertion point.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > IPv6 ACL Configuration

```plaintext
configure > context context_name > ipv6 access-list ipv6_acl_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipv6-acl)#
```

**Syntax**

```
redirect context context_id [ log ] any
after redirect context context_id [ log ] any
before redirect context context_id [ log ] any
no redirect context context_id [ log ] any
```

**after**
Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

**before**
Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

**no**
Removes the rule which exactly matches the options specified.
redirect context (any)

context context_id
The context identification number of the context to which packets are redirected. At the executive mode prompt, use the `show context all` command to display context names and context IDs.

log
Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

any
Indicates all packets will match the redirect regardless of source and/or destination.

Usage
Define a catch all rule to place at the end of the list of rules to provide explicit handling of rules which do not fit any other criteria.

Important: It is suggested that any rule which is added to be a catch all should also have the log option specified. The logged packets may be used to determine if the current list of rules is adequate or needs modification to ensure proper security. The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the Engineering Rules appendix in the System Administration Guide. Also note that “redirect” rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example
The following command defines a rule that redirects packets to the context with the context ID of 23 and any source IP:

```
redirect context 23 any
```

The following sets the insertion point to before the first rule defined above:

```
before redirect context 23 any
```

The following command sets the insertion point after the second rule defined above:

```
after redirect context 23 any
```

The following deletes the first rule defined above:

```
no redirect context 23 any
```
redirect context (by host IP address)

Used to redirect subscriber sessions based on the targeted host IP address sent by the source to the mobile node or the network.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > IPv6 ACL Configuration

```bash
configure > context context_name > ipv6 access-list ipv6_acl_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipv6-acl)#
```

**Syntax**

```bash
redirect context context_id [ log ] host source_ip_address
after redirect context context_id [ log ] host source_ip_address
before redirect context context_id [ log ] host source_ip_address
no redirect context context_id [ log ] host source_ip_address
```

*after*
Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

*before*
Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

*no*
Removes the rule which exactly matches the options specified.
`context context_id`

The context identification number of the context to which packets are redirected. At the executive mode prompt, use the `show context all` command to display context names and context IDs.

`log`

Default: packets are not logged. Indicates all packets which match the redirect are to be logged.

`host`

Specifies that the rule applies to a specific host as determined by its IP address.

`source_host_address`

The IP address of the source host to filter against expressed in IPv6 colon-separated-hexadecimal notation.

### Usage

Define a rule when a very specific remote host is to be blocked. In simplified networks where the access controls need only block a few hosts, this command allows the rules to be very clear and concise.

**Important:** The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the `Engineering Rules` appendix in the `System Administration Guide`. Also note that “redirect” rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

### Example

The following command defines a rule that redirects packets to the context with the context ID of 23 and a host IP address of `fe80::c0a8:c80b`:

```
redirect context 23 host fe80::c0a8:c80b
```

The following sets the insertion point to before the first rule defined above:

```
before redirect context 23 host fe80::c0a8:c80b
```

The following command sets the insertion point after the second rule defined above:

```
after redirect context 23 host fe80::c0a8:c80b
```

The following deletes the first rule defined above:

```
no redirect context 23 host fe80::c0a8:c80b
```
redirect context (by source ICMP packets)

Used to redirect subscriber sessions based on the internet control message protocol packets sent by the source to the mobile node or the network.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > IPv6 ACL Configuration

        configure > context context_name > ipv6 access-list ipv6_acl_name

Entering the above command sequence results in the following prompt:

        [context_name]host_name(config-ipv6-acl)#

Syntax

    redirect context context_id [ log ] icmp { source_address source_wildcard | any | host source_host_address } { dest_address dest_wildcard | any | host dest_host_address } [ icmp_type [ icmp_code ] ]

    after redirect context context_id [ log ] icmp { source_address source_wildcard | any | host source_host_address } { dest_address dest_wildcard | any | host dest_host_address } [ icmp_type [ icmp_code ] ]

    before redirect context context_id [ log ] icmp { source_address source_wildcard | any | host source_host_address } { dest_address dest_wildcard | any | host dest_host_address } [ icmp_type [ icmp_code ] ]

    no redirect context context_id [ log ] icmp { source_address source_wildcard | any | host source_host_address } { dest_address dest_wildcard | any | host dest_host_address } [ icmp_type [ icmp_code ] ]

    after

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

    before

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.
**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

**no**
Removes the rule which exactly matches the options specified.

**context context_id**
The context identification number of the context to which packets are redirected. At the executive mode prompt, use the `show context all` command to display context names and context IDs.

**log**
Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

**source_address**
The IP address(es) form which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the `sourceWildcard` parameter.

**sourceWildcard**
This option is used in conjunction with the `source_address` option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:
- Zero-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

**any**
Specifies that the rule applies to all packets.

**host**
Specifies that the rule applies to a specific host as determined by its IP address.

**source_host_address**
The IP address of the source host to filter against expressed in IPv6 colon-separated-hexadecimal notation.

**dest_host_address**
The IP address of the destination host to filter against expressed in IPv6 colon-separated-hexadecimal notation.
**dest_address**

The IP address(es) to which the packet is to be sent.
This option is used to filter all packets to a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the **dest_wildcard** parameter.

**dest_wildcard**

This option is used in conjunction with the **dest_address** option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:
- Zero-bits in this parameter mean that the corresponding bits configured for the **dest_address** parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the **dest_address** parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

**icmp_type**

Specifies that all ICMP packets of a particular type are to be filtered. Type is an integer from 0 through 255.

**icmp_code**

Specifies that all ICMP packets of a particular code are to be filtered. Type is an integer from 0 through 255.

**Usage**

Define a rule to block ICMP packets which can be used for address resolution and possibly be a security risk.
The IP redirecting allows flexible controls for pairs of individual hosts or groups by IP masking which allows the redirecting of entire subnets if necessary.

**Important:** The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the Engineering Rules appendix in the System Administration Guide. Also note that “redirect” rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

**Example**

The following command defines a rule that redirects packets to the context with the context ID of 23, and ICMP packets coming from the host with the IP address 2002::c6a2:6419:

```
redirect context 23 icmp host 2002::c6a2:6419
```

The following sets the insertion point to before the first rule defined above:

```
before redirect context 23 icmp host 2002::c6a2:6419
```

The following command sets the insertion point after the second rule defined above:

```
after redirect context 23 icmp host 2002::c6a2:6419
```
The following deletes the first rule defined above:

```
no redirect context 23 icmp host 2002:c6a2:6419
```
redirect context (by IP packets)

Used to redirect subscriber sessions based on the internet protocol packets sent by the source to the mobile node or the network.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > IPv6 ACL Configuration

```
configure > context context_name > ipv6 access-list ipv6_acl_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipv6-acl)#
```

**Syntax**

```
redirect context context_id [ log ] ip { source_address source_wildcard | any | host source_host_address } { dest_address dest_wildcard | any | host dest_host_address } [ fragment ] [ protocol num ]
```

```
after redirect context context_id [ log ] ip { source_address source_wildcard | any | host source_host_address } { dest_address dest_wildcard | any | host dest_host_address } [ fragment ] [ protocol num ]
```

```
before redirect context context_id [ log ] ip { source_address source_wildcard | any | host source_host_address } { dest_address dest_wildcard | any | host dest_host_address } [ fragment ] [ protocol num ]
```

```
oredirect context context_id [ log ] ip { source_address source_wildcard | any | host source_host_address } { dest_address dest_wildcard | any | host dest_host_address } [ fragment ] [ protocol num ]
```

**after**

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

**before**

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.
**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

- **no**
  Removes the rule which exactly matches the options specified.

- **context context_id**
  The context identification number of the context to which packets are redirected. At the executive mode prompt, use the `show context all` command to display context names and context IDs.

- **log**
  Default: packets are not logged.
  Indicates all packets which match the redirect are to be logged.

- **source_address**
  The IP address(es) from which the packet originated.
  This option is used to filter all packets from a specific IP address or a group of IP addresses.
  When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the `source wildcard` parameter.

- **source wildcard**
  This option is used in conjunction with the `source address` option to specify a group of addresses for which packets are to be filtered.
  The mask must be entered as a complement:
  - Zero-bits in this parameter mean that the corresponding bits configured for the `source address` parameter must be identical.
  - One-bits in this parameter mean that the corresponding bits configured for the `source address` parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

- **any**
  Specifies that the rule applies to all packets.

- **host**
  Specifies that the rule applies to a specific host as determined by its IP address.

- **source_host_address**
  The IP address of the source host to filter against expressed in IPv6 colon-separated-hexadecimal notation.

- **dest_host_address**
  The IP address of the destination host to filter against expressed in IPv6 colon-separated-hexadecimal notation.
IPv6 ACL Configuration Mode Commands

**redirect context (by IP packets)**

**dest_address**

The IP address(es) to which the packet is to be sent. This option is used to filter all packets to a specific IP address or a group of IP addresses. When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the **dest_wildcard** parameter.

**dest_wildcard**

This option is used in conjunction with the **dest_address** option to specify a group of addresses for which packets are to be filtered. The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the **dest_address** parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the **dest_address** parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

**fragment**

Indicates packet redirection is to be applied to IP packet fragments only.

**protocol** **num**

Indicates that the packet filtering is to be applied to a specific protocol number. **num** is an integer from 0 through 255.

**Usage**

Block IP packets when the source and destination are of interest.

**Important:** The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the *Engineering Rules* appendix in the *System Administration Guide*. Also note that “redirect” rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

**Example**

The following command defines a rule that redirect packets to the context with the context ID of 23, and IP packets coming from the host with the IP address 2002::c6a2:6419, and fragmented packets for any destination are matched:

```
redirect context 23 ip host 2002::c6a2:6419 any fragment
```

The following sets the insertion point to before the first rule defined above:

```
befor redirect context 23 ip host 198.162.100.25 any fragment
```

The following command sets the insertion point after the second rule defined above:

```
afte redirect context 23 ip host 2002::c6a2:6419 any fragment
```
The following deletes the first rule defined above:

```plaintext
do redirect context 23 ip host 2002::c6a2:6419 any fragment
```
Redirect context (by TCP/UDP packets)

Redirect context is used to redirect subscriber sessions based on the transmission control protocol/user datagram protocol packets sent by the source to the mobile node or the network.

**Product**: All

**Privilege**: Security Administrator, Administrator

**Mode**: Exec > Global Configuration > Context Configuration > IPv6 ACL Configuration

```
configure > context context_name > ipv6 access-list ipv6_acl_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipv6-acl)#
```

**Syntax**

```
redirect context context_id [ log ] { tcp | udp } { { source_address source_wildcard | any | host source_host_address } [ eq source_port | gt source_port | lt source_port | neq source_port ] } { { dest_address dest_wildcard | any | host dest_host_address } [ eq dest_port | gt dest_port | lt dest_port | neq dest_port ] }
```

```
after redirect context context_id [ log ] { tcp | udp } { { source_address source_wildcard | any | host source_host_address } [ eq source_port | gt source_port | lt source_port | neq source_port ] } { { dest_address dest_wildcard | any | host dest_host_address } [ eq dest_port | gt dest_port | lt dest_port | neq dest_port ] }
```

```
before redirect context context_id [ log ] { tcp | udp } { { source_address source_wildcard | any | host source_host_address } [ eq source_port | gt source_port | lt source_port | neq source_port ] } { { dest_address dest_wildcard | any | host dest_host_address } [ eq dest_port | gt dest_port | lt dest_port | neq dest_port ] }
```

```
no redirect context context_id [ log ] { tcp | udp } { { source_address source_wildcard | any | host source_host_address } [ eq source_port | gt source_port | lt source_port | neq source_port ] } { { dest_address dest_wildcard | any | host dest_host_address } [ eq dest_port | gt dest_port | lt dest_port | neq dest_port ] }
```

**Important**: If the options specified do not exactly match an existing rule, the insertion point does not change.
**IPv6 ACL Configuration Mode Commands**

### redirect context (by TCP/UDP packets)

#### before
Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

---

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

---

#### no
Removes the rule which exactly matches the options specified.

---

#### context context_id
The context identification number of the context to which packets are redirected. At the executive mode prompt, use the `show context all` command to display context names and context IDs.

---

#### log
Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

---

#### tcp | udp
Specifies the redirect is to be applied to IP-based transmission control protocol or the user datagram protocol.
- **tcp**: Redirect applies to TCP packets.
- **udp**: Redirect applies to UDP packets.

---

#### source_address
The IP address(es) from which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the `source wildcard` parameter.

---

#### source wildcard
This option is used in conjunction with the `source_address` option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:
- Zero-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be ignored.

---

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

---

#### any
Specifies that the rule applies to all packets.
host
Specifies that the rule applies to a specific host as determined by its IP address.

source_host_address
The IP address of the source host to filter against expressed in IPv6 colon-separated-hexadecimal notation.

dest_host_address
The IP address of the destination host to filter against expressed in IPv6 colon-separated-hexadecimal notation.

eq source_port
Specifies a single, specific source TCP port number to be filtered.
source_port must be configured to an integer from 0 through 65535.

gt source_port
Specifies that all source TCP port numbers greater than the one specified are to be filtered.
source_port must be configured to an integer from 0 through 65535.

lt source_port
Specifies that all source TCP port numbers less than the one specified are to be filtered.
source_port must be configured to an integer from 0 through 65535.

neq source_port
Specifies that all source TCP port numbers not equal to the one specified are to be filtered.
source_port must be configured to an integer from 0 through 65535.

dest_address
The IP address(es) to which the packet is to be sent.
This option is used to filter all packets to a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the dest_wildcard parameter.

dest_wildcard
This option is used in conjunction with the dest_address option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:
  ● Zero-bits in this parameter mean that the corresponding bits configured for the dest_address parameter must be identical.
  ● One-bits in this parameter mean that the corresponding bits configured for the dest_address parameter must be ignored.

Important: The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

eq dest_port
Specifies a single, specific destination TCP port number to be filtered.
IPv6 ACL Configuration Mode Commands

redirect context (by TCP/UDP packets)

---

dest_port must be configured to an integer from 0 through 65535.

---

**gt dest_port**

Specifies that all destination TCP port numbers greater than the one specified are to be filtered.

*dest_port* must be configured to an integer from 0 through 65535.

---

**lt dest_port**

Specifies that all destination TCP port numbers less than the one specified are to be filtered.

*dest_port* must be configured to an integer from 0 through 65535.

---

**neq dest_port**

Specifies that all destination TCP port numbers not equal to the one specified are to be filtered.

*dest_port* must be configured to an integer from 0 through 65535.

---

**Usage**

Block IP packets when the source and destination are of interest but for only a limited set of ports.

---

**Important:** The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the Engineering Rules appendix in the System Administration Guide. Also note that “redirect” rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

---

**Example**

The following command defines a rule that redirects packets to the context with the context ID of 23, and UDP packets coming from any host are matched:

```
redirect context 23 udp any
```

The following sets the insertion point to before the rule defined above:

```
before redirect context 23 udp any
```

The following command sets the insertion point after the rule defined above:

```
after redirect context 23 udp any
```

The following deletes the rule defined above:

```
no redirect context 23 udp any
```
redirect css delivery-sequence

This is a restricted command. In StarOS 9.0 and later, this command is obsoleted.
**redirect css service (any)**

Used to redirect subscriber sessions based on any packet received with Content Service Steering (CSS) enabled. This command is also used to set the access control list insertion point.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > IPv6 ACL Configuration
configure > context context_name > ipv6 access-list ipv6_acl_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipv6-acl) #
```

**Syntax**

```
redirect css service svc_name [ log ] any
after redirect css service svc_name [ log ] any
before redirect css service svc_name [ log ] any
no redirect css service svc_name [ log ] any
```

**after**
Indicates all rule definitions defined subsequent to this command are to be inserted after the command identified by the exact options listed. This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

**before**
Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed. This moves the insertion point to be immediately before the rule definitions which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

**no**
Removes the rule definition which exactly matches the options specified.
**redirect css service (any)**

css service *svc_name*

The name of the CSS service to which packets are to be redirected. At the executive mode prompt, use the `show css service all` command to display the names of all configured CSS services. *svc_name* must be a string of 1 through 15 characters.

log

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

any

Indicates all packets will match the redirect regardless of source and/or destination.

**Usage**

Define a catch all rule definitions to place at the end of the list of rule definitions to provide explicit handling of rule definitions which do not fit any other criteria.

**Important:** It is suggested that any rule definition which is added to be a catch all should also have the `log` option specified. The logged packets may be used to determine if the current list of rule definitions is adequate or needs modification to ensure proper security.

**Important:** A maximum of 16 rule definitions can be configured per ACL.

**Important:** Also note that “redirect” rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

**Example**

The following command defines a rule definition that redirects packets to the CSS service with the name `css-svcl` and any source IP:

```
redirect css service css-svcl any
```

The following sets the insertion point to before the first rule definition above:

```
before redirect css service css-svcl any
```

The following command sets the insertion point after the second rule definitions above:

```
after redirect css service css-svcl any
```

The following deletes the first rule definition above:

```
no redirect css service css-svcl any
```
redirect css service (by host IP address)

Used to redirect subscriber sessions based on the targeted host IP address sent by the source to the mobile node or the network.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > IPv6 ACL Configuration
configure > context context_name > ipv6 access-list ipv6_acl_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ipv6-acl)#

Syntax

redirect css service svc_name [ log ] host source_host_address
after redirect css service svc_name [ log ] host source_host_address
before redirect css service svc_name [ log ] host source_host_address
no redirect css service svc_name [ log ] host source_host_address

after
Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

Important: If the options specified do not exactly match an existing rule definition, the insertion point does not change.

before
Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

Important: If the options specified do not exactly match an existing rule definition, the insertion point does not change.

no
Removes the rule definition which exactly matches the options specified.
**redirect css service (by host IP address)**

**css service svc_name**

The name of the Content Service Steering (CSS) service to which packets are to be redirected. At the executive mode prompt, use the `show css service all` command to display the names of all configured CSS services. `svc_name` must be an alphanumeric string of 1 through 15 characters.

**log**

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

**host**

Specifies that the rule definition applies to a specific host as determined by its IP address.

**source_host_address**

The IP address of the source host to filter against expressed in IPv6 colon-separated-hexadecimal notation.

**Usage**

Define a rule definition when a very specific remote host is to be blocked. In simplified networks where the access controls need only block a few hosts, this command allows the rule definitions to be very clear and concise.

**Important:** A maximum of 16 rule definitions can be configured per ACL. Also note that “redirect” rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

**Example**

The following command defines a rule definition that redirects packets to the CSS service with the name `css-svcl` and a host IP address of `fe80::c0a8:c80b`:

```
redirect css service css-svcl host fe80::c0a8:c80b
```

The following sets the insertion point to before the first rule definition above:

```
before redirect css service css-svcl host fe80::c0a8:c80b
```

The following command sets the insertion point after the second rule definition above:

```
after redirect css service css-svcl host fe80::c0a8:c80b
```

The following deletes the first rule definition above:

```
no redirect css service css-svcl host fe80::c0a8:c80b
```
redirect css service (by ICMP packets)

Used to redirect subscriber sessions based on the internet control message protocol packets sent by the source to the mobile node or the network.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > IPv6 ACL Configuration

configure > context context_name > ipv6 access-list ipv6_acl_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ipv6-acl)#

**Syntax**

```plaintext
redirect css service svc_name [ log ] icmp { any | host source_host_address | source_address source_wildcard } { any | host dest_host_address | dest_address dest_wildcard } [ icmp_type [ icmp_code ] ]

after redirect css service svc_name [ log ] icmp { any | host source_host_address | source_address source_wildcard } { any | host dest_host_address | dest_address dest_wildcard } [ icmp_type [ icmp_code ] ]

before redirect css service svc_name [ log ] icmp { any | host source_host_address | source_address source_wildcard } { any | host dest_host_address | dest_address dest_wildcard } [ icmp_type [ icmp_code ] ]

no redirect css service svc_name [ log ] icmp { any | host source_host_address | source_address source_wildcard } { any | host dest_host_address | dest_address dest_wildcard } [ icmp_type [ icmp_code ] ]
```

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

```plaintext
after
Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed. This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

before
Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed. This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.
```
**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

```plaintext
no
```
Removes the rule definition which exactly matches the options specified.

```plaintext
css service svc_name
```
The name of the Content Service Steering (CSS) service to which packets are to be redirected. At the executive mode prompt, use the `show css service all` command to display the names of all configured charging services.

*svc_name* must be an alphanumeric string of 1 through 15 characters.

```plaintext
log
```
Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

```plaintext
source_address
```
The IP address(es) form which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the *source wildcard* parameter.

```plaintext
source wildcard
```
This option is used in conjunction with the *source_address* option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:
- Zero-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *source_address* parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

```plaintext
any
```
Specifies that the rule definition applies to all packets.

```plaintext
host
```
Specifies that the rule definition applies to a specific host as determined by its IP address.

```plaintext
source host address
```
The IP address of the source host to filter against expressed in IPv6 colon-separated-hexadecimal notation.
IPv6 ACL Configuration Mode Commands

redirect css service (by ICMP packets)

**dest_host_address**
The IP address of the destination host to filter against expressed in IPv6 colon-separated-hexadecimal notation.

**dest_address**
The IP address(es) to which the packet is to be sent.
This option is used to filter all packets to a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the dest_wildcard parameter.

**dest_wildcard**
This option is used in conjunction with the dest_address option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:
- Zero-bits in this parameter mean that the corresponding bits configured for the dest_address parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the dest_address parameter must be ignored.

<table>
<thead>
<tr>
<th>Important:</th>
<th>The mask must contain a contiguous set of one-bits from the least significant bit (LSB).</th>
</tr>
</thead>
</table>

**icmp_type**
Specifies that all ICMP packets of a particular type are to be filtered. The type can be an integer value from 0 through 255.

**icmp_code**
Specifies that all ICMP packets of a particular code are to be filtered. The type is an integer from 0 through 255.

**Usage**
Define a rule definition to block ICMP packets which can be used for address resolution and possibly be a security risk.
The IP redirecting allows flexible controls for pairs of individual hosts or groups by IP masking which allows the redirecting of entire subnets if necessary.

<table>
<thead>
<tr>
<th>Important:</th>
<th>A maximum of 16 rule definitions can be configured per ACL. Also note that “redirect” rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.</th>
</tr>
</thead>
</table>

**Example**
The following command defines a rule definition that redirects packets to the CSS service named css-svc1, and ICMP packets coming from the host with the IP address 2002::c6a2:6419:

```
redirect css service css-svc1 icmp host 2002::c6a2:6419
```

The following sets the insertion point to before the first rule definition above:
before redirect css service css-svcl icmp host 2002::c6a2:6419

The following command sets the insertion point after the second rule definition above:

after redirect css service css-svcl icmp host 2002::c6a2:64195

The following deletes the first rule definition above:

no redirect css service css-svcl icmp host 2002::c6a2:6419
redirect css service (by IP packets)

Used to redirect subscriber sessions based on the internet protocol packets sent by the source to the mobile node or the network.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > IPv6 ACL Configuration

configure > context context_name > ipv6 access-list ipv6_acl_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ipv6-acl)#

**Syntax**

- `redirect css service svc_name [ log ] ip { any | host source_host_address | source_address source_wildcard } { any | host dest_host_address | dest_address dest_wildcard } [ fragment ]`

- `after redirect css service svc_name [ log ] ip { any | host source_host_address | source_address source_wildcard } { any | host dest_host_address | dest_address dest_wildcard } [ fragment ]`

- `before redirect css service svc_name [ log ] ip { any | host source_host_address | source_address source_wildcard } { any | host dest_host_address | dest_address dest_wildcard } [ fragment ]`

- `no redirect css service svc_name [ log ] ip { any | host source_host_address | source_address source_wildcard } { any | host dest_host_address | dest_address dest_wildcard } [ fragment ]`

**after**
Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

**Important**: If the options specified do not exactly match an existing rule definition, the insertion point does not change.

**before**
Indicates all rule definitions defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.
redirect css service (by IP packets)

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

- **no**
  Removes the rule definition which exactly matches the options specified.

- **css service svc_name**
  The name of the Content Service Steering (CSS) service to which packets are to be redirected. At the executive mode prompt, use the `show css service all` command to display the names of all configured CSS services.
  `svc_name` must be an alphanumeric string of 1 through 15 characters.

- **log**
  Default: packets are not logged.
  Indicates all packets which match the redirect are to be logged.

- **source_address**
  The IP address(es) from which the packet originated.
  This option is used to filter all packets from a specific IP address or a group of IP addresses.
  When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the `source_wildcard` parameter.

- **source_wildcard**
  This option is used in conjunction with the `source_address` option to specify a group of addresses for which packets are to be filtered.
  The mask must be entered as a complement:
  - Zero-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be identical.
  - One-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

- **any**
  Specifies that the rule definition applies to all packets.

- **host**
  Specifies that the rule definition applies to a specific host as determined by its IP address.

- **source_host_address**
  The IP address of the source host to filter against expressed in IPv6 colon-separated-hexadecimal notation.
**dest_host_address**

The IP address of the destination host to filter against expressed in IPv6 colon-separated-hexadecimal notation.

**dest_address**

The IP address(es) to which the packet is to be sent. This option is used to filter all packets to a specific IP address or a group of IP addresses. When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the **dest_wildcard** parameter.

**dest_wildcard**

This option is used in conjunction with the **dest_address** option to specify a group of addresses for which packets are to be filtered. The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the **dest_address** parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the **dest_address** parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.

**fragment**

Indicates packet redirection is to be applied to IP packet fragments only.

**Usage**

Block IP packets when the source and destination are of interest.

**Important:** A maximum of 16 rule definitions can be configured per ACL. Also note that “redirect” rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

**Example**

The following command defines a rule definition that redirects packets to the CSS service named **css-svc1**, and IP packets coming from the host with the IP address 2002::c6a2:6419, and fragmented packets for any destination are matched:

```
redirect css service css-svc1 ip host 2002::c6a2:6419 any fragment
```

The following sets the insertion point to before the first rule definition above:

```
before redirect css service css-svc1 ip host 2002::c6a2:6419 any fragment
```

The following command sets the insertion point after the second rule definition above:

```
after redirect css service css-svc1 ip host 2002::c6a2:6419 any fragment
```
The following deletes the first rule definition above:

```
no redirect css service css-svc1 ip host 2002::c6a2:6419 any fragment
```
redirect css service (by source IP address masking)

Used to redirect subscriber sessions based on the IP address mask sent by the source to the mobile node or the network.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > IPv6 ACL Configuration
configure > context context_name > ipv6 access-list ipv6_acl_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ipv6-acl)#

Syntax

redirect css service svc_name [ log ] source_address source_wildcard

after redirect css service svc_name [ log ] source_address source_wildcard

before redirect css service svc_name [ log ] source_address source_wildcard

no redirect css service svc_name [ log ] source_address source_wildcard

after
Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

Important: If the options specified do not exactly match an existing rule definition, the insertion point does not change.

before
Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

Important: If the options specified do not exactly match an existing rule definition, the insertion point does not change.

no
Removes the rule definition which exactly matches the options specified.
The name of the Content Service Steering (CSS) service to which packets are to be redirected. At the executive mode prompt, use the `show css service all` command to display the names of all configured CSS services. `svc_name` must be an alphanumeric string of 1 through 15 characters.

Indicates all packets which match the filter are to be logged.

The IP address(es) form which the packet originated. This option is used to filter all packets from a specific IP address or a group of IP addresses. When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the `source_wildcard` parameter.

This option is used in conjunction with the `source_address` option to specify a group of addresses for which packets are to be filtered. The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be ignored.

The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

Define a rule definition when any packet from the IP addresses which fall into the group of addresses matching the IP address masking. This allows the reduction of filtering rule definitions as it does not require a rule definition for each source and destination pair.

A maximum of 16 rule definitions can be configured per ACL.

The following command defines a rule definition to redirect packets to a CSS service named `css-svc1`:

```
redirect css service css=svc1 2002::c6a2:6419
```
redirect css service (by TCP/UDP packets)

Used to redirect subscriber sessions based on the transmission control protocol/user datagram protocol packets sent by the source to the mobile node or the network.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > IPv6 ACL Configuration

configure > context context_name > ipv6 access-list ipv6_acl_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipv6-acl) #
```

**Syntax**

```
redirect css service svc_name [ log ] { tcp | udp } { { source_address source_wildcard | any | host source_host_address } [ eq source_port | gt source_port | lt source_port | neq source_port | range start_source_port end_source_port ] } { { dest_address dest_wildcard | any | host dest_host_address } [ eq dest_port | gt dest_port | lt dest_port | neq dest_port | range start_dest_port end_dest_port ] }
```

```
after redirect css service svc_name [ log ] { tcp | udp } { { source_address source_wildcard | any | host source_host_address } [ eq source_port | gt source_port | lt source_port | neq source_port | range start_source_port end_source_port ] } { { dest_address dest_wildcard | any | host dest_host_address } [ eq dest_port | gt dest_port | lt dest_port | neq dest_port | range start_dest_port end_dest_port ] }
```

```
after redirect css service svc_name [ log ] { tcp | udp } { { source_address source_wildcard | any | host source_host_address } [ eq source_port | gt source_port | lt source_port | neq source_port | range start_source_port end_source_port ] } { { dest_address dest_wildcard | any | host dest_host_address } [ eq dest_port | gt dest_port | lt dest_port | neq dest_port | range start_dest_port end_dest_port ] }
```

```
o redirect css service svc_name [ log ] { tcp | udp } { { source_address source_wildcard | any | host source_host_address } [ eq source_port | gt source_port | lt source_port | neq source_port | range start_source_port end_source_port ] } { { dest_address dest_wildcard | any | host dest_host_address } [ eq dest_port | gt dest_port | lt dest_port | neq dest_port | range start_dest_port end_dest_port ] }
```

```
after
```

Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.
**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

**before**

Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed. This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

**no**

Removes the rule definition which exactly matches the options specified.

**css service svc_name**

The name of the Content Service Steering (CSS) service to which packets are to be redirected. At the executive mode prompt, use the `show css service all` command to display the names of all configured charging services. `svc_name` must be an alphanumeric string of 1 through 15 characters.

**log**

Default: packets are not logged. Indicates all packets which match the redirect are to be logged.

**tcp | udp**

Specifies the redirect is to be applied to IP-based transmission control protocol or the user datagram protocol.

- **tcp**: Redirect applies to TCP packets.
- **udp**: Redirect applies to UDP packets.

**source_address**

The IP address(es) form which the packet originated. This option is used to filter all packets from a specific IP address or a group of IP addresses. When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the `sourceWildcard` parameter.

**sourceWildcard**

This option is used in conjunction with the `source_address` option to specify a group of addresses for which packets are to be filtered. The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be ignored.
**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

- **any**
  Specifies that the rule definition applies to all packets.

- **host**
  Specifies that the rule definition applies to a specific host as determined by its IP address.

- **source_host_address**
  The IP address of the source host to filter against expressed in IPv6 colon notation.

- **dest_host_address**
  The IP address of the destination host to filter against expressed in IPv6 colon notation.

- **eq source_port**
  Specifies a single, specific source TCP port number to be filtered.
  `source_port` must be configured to an integer from 0 to 65535.

- **gt source_port**
  Specifies that all source TCP port numbers greater than the one specified are to be filtered.
  `source_port` must be configured to an integer from 0 to 65535.

- **lt source_port**
  Specifies that all source TCP port numbers less than the one specified are to be filtered.
  `source_port` must be configured to an integer from 0 to 65535.

- **neq source_port**
  Specifies that all source TCP port numbers not equal to the one specified are to be filtered.
  `source_port` must be configured to an integer from 0 to 65535.

- **range start_source_port end_source_port**
  Specifies that all source TCP ports within a specific range are to be filtered.
  `start_source_port` is the initial port in the range and `end_source_port` is the final port in the range.
  Both `start_source_port` and `end_source_port` can be configured to an integer from 0 to 65535.

- **dest_address**
  The IP address(es) to which the packet is to be sent.
  This option is used to filter all packets to a specific IP address or a group of IP addresses.
  When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the `dest_wildcard` parameter.

- **dest_wildcard**
  This option is used in conjunction with the `dest_address` option to specify a group of addresses for which packets are to be filtered.
  The mask must be entered as a complement:
IPv6 ACL Configuration Mode Commands

redirect css service (by TCP/UDP packets)

- Zero-bits in this parameter mean that the corresponding bits configured for the dest_address parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the dest_address parameter must be ignored.

### Important:
The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>eq dest_port</td>
<td>Specifies a single, specific destination TCP port number to be filtered. dest_port must be configured to an integer from 0 to 65535.</td>
</tr>
<tr>
<td>gt dest_port</td>
<td>Specifies that all destination TCP port numbers greater than the one specified are to be filtered. dest_port must be configured to an integer from 0 to 65535.</td>
</tr>
<tr>
<td>lt dest_port</td>
<td>Specifies that all destination TCP port numbers less than the one specified are to be filtered. dest_port must be configured to an integer from 0 to 65535.</td>
</tr>
<tr>
<td>neq dest_port</td>
<td>Specifies that all destination TCP port numbers not equal to the one specified are to be filtered. dest_port must be configured to an integer from 0 to 65535.</td>
</tr>
<tr>
<td>range start_dest_port end_dest_port</td>
<td>Specifies that all destination TCP ports within a specific range are to be filtered. start_dest_port is the initial port in the range and end_dest_port is the final port in the range. Both start_dest_port and end_dest_port can be configured to an integer from 0 to 65535.</td>
</tr>
</tbody>
</table>

### Usage
Block IP packets when the source and destination are of interest but for only a limited set of ports.

### Important:
A maximum of 16 rule definitions can be configured per ACL. Also note that “redirect” rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

### Example
The following command defines a rule definition that redirects packets to the CSS service named css-svcl, and UDP packets coming from any host are matched:

```
redirect css service css-svcl udp any
```

The following sets the insertion point to before the rule definition above:

```
before redirect css service css-svcl udp any
```

The following command sets the insertion point after the rule definition above:

```
```
after redirect css service css-svcl udp any

The following deletes the rule definition above:

no redirect css service css-svcl udp any
**redirect css service (for downlink, any)**

Used to redirect subscriber sessions based on any packet received in the downlink (from the Mobile Node) direction. This command is also used to set the access control list insertion point.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > IPv6 ACL Configuration

```
configure > context context_name > ipv6 access-list ipv6_acl_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipv6-acl)#
```

**Syntax**

```
redirect css service svc_name [ log ] downlink any

after redirect css service svc_name [ log ] downlink any

before redirect css service svc_name [ log ] downlink any

no redirect css service svc_name [ log ] downlink any
```

**after**
Indicates all rule definitions defined subsequent to this command are to be inserted after the command identified by the exact options listed. This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

**Important**: If the options specified do not exactly match an existing rule definition, the insertion point does not change.

**before**
Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed. This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

**Important**: If the options specified do not exactly match an existing rule definition, the insertion point does not change.

**no**
Removes the rule definition which exactly matches the options specified.
**css service svc_name**

The name of the Content Service Steering (CSS) service to which packets are to be redirected. At the executive mode prompt, use the `show css service all` command to display the names of all configured CSS services.

`svc_name` must be an alphanumeric string of 1 through 15 characters.

**downlink**

Apply this rule definition only to packets in the downlink (from the Mobile Node) direction.

**log**

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

**any**

Indicates all packets will match the redirect regardless of source and/or destination.

**Usage**

Define a catch all rule definition to place at the end of the list of rule definitions to provide explicit handling of rule definitions which do not fit any other criteria.

**Important:** It is suggested that any rule definition which is added to be a catch all should also have the `log` option specified. The logged packets may be used to determine if the current list of rule definitions is adequate or needs modification to ensure proper security.

**Important:** A maximum of 16 rule definitions can be configured per ACL.

**Important:** Also note that “redirect” rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

**Example**

The following command defines a rule definition that redirects packets to the CSS service with the name `css-svcl` and any source IP:

```plaintext
redirect css service css-svcl downlink any
```

The following sets the insertion point to before the first rule definition above:

```plaintext
before redirect service css-svcl downlink any
```

The following command sets the insertion point after the second rule definition above:

```plaintext
after redirect service css-svcl downlink any chgsvcl downlink any
```

The following deletes the first rule definition above:

```plaintext
no redirect service css-svcl downlink any
```
redirect css service (for downlink, by host IP address)

Used to redirect subscriber sessions based on the targeted host IP address in the downlink (from the Mobile Node) direction.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > IPv6 ACL Configuration

```
configure > context context_name > ipv6 access-list ipv6_acl_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipv6-acl)#
```

**Syntax**

- `redirect css service svc_name [ log ] downlink host source_host_address`
- `after redirect css service svc_name [ log ] downlink host source_host_address`
- `before redirect css service svc_name [ log ] downlink host source_host_address`
- `no redirect css service svc_name [ log ] downlink host source_host_address`

**after**
Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

**before**
Indicates all rule definitions defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

**no**
Removes the rule definition which exactly matches the options specified.
**css service svc_name**

The name of the Content Service Steering (CSS) service to which packets are to be redirected. At the executive mode prompt, use the `show css service all` command to display the names of all configured CSS services.

`svc_name` must be an alphanumeric string of 1 through 15 characters.

**downlink**

Apply this rule definition only to packets in the downlink (from the Mobile Node) direction.

**log**

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

**host**

Specifies that the rule definition applies to a specific host as determined by its IP address.

**source_host_address**

The IP address of the source host to filter against expressed in IPv6 colon-separated-hexadecimal notation.

**Usage**

Define a rule definition when a very specific remote host is to be blocked. In simplified networks where the access controls need only block a few hosts, this command allows the rule definitions to be very clear and concise.

**Important:** A maximum of 16 rule definitions can be configured per ACL. Also note that “redirect” rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

**Example**

The following command defines a rule definition that redirects packets to the charging service with the name `css-svc1` and a host IP address of `fe80::c0a8:c80b`:

```
redirect service css-svc1 downlink host fe80::c0a8:c80b
```

The following sets the insertion point to before the first rule definition above:

```
before redirect service css-svc1 downlink host fe80::c0a8:c80b
```

The following command sets the insertion point after the second rule definition above:

```
after redirect service css-svc1 downlink host fe80::c0a8:c80b
```

The following deletes the first rule definition above:

```
no redirect service css-svc1 downlink host fe80::c0a8:c80b
```
redirect css service (for downlink, by ICMP packets)

Used to redirect subscriber sessions based on the internet control message protocol packets in the downlink (from the Mobile Node) direction.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > IPv6 ACL Configuration

```
configure > context context_name > ipv6 access-list ipv6_acl_name
```

Entering the above command sequence results in the following prompt:

```
[context_name] host_name(config-ipv6-acl) #
```

**Syntax**

```
redirect css service svc_name [ log ] downlink icmp { any | host source_host_address | source_address source_wildcard } { any | host dest_host_address | dest_address dest_wildcard } [ icmp_type [ icmp_code ] ]
```

```
after redirect css service svc_name [ log ] downlink icmp { any | host source_host_address | source_address source_wildcard } { any | host dest_host_address | dest_address dest_wildcard } [ icmp_type [ icmp_code ] ]
```

```
before redirect css service svc_name [ log ] downlink icmp { any | host source_host_address | source_address source_wildcard } { any | host dest_host_address | dest_address dest_wildcard } [ icmp_type [ icmp_code ] ]
```

```
no redirect css service svc_name [ log ] downlink icmp { any | host source_host_address | source_address source_wildcard } { any | host dest_host_address | dest_address dest_wildcard } [ icmp_type [ icmp_code ] ]
```

---

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

```
before
```

Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.

This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.
**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

- **no**
  Removes the rule definition which exactly matches the options specified.

- **css service svc_name**
  The name of the Content Service Steering (CSS) service to which packets are to be redirected. At the executive mode prompt, use the `show css service all` command to display the names of all configured CSS services.
  `svc_name` must be an alphanumeric string of 1 through 15 characters.

- **downlink**
  Apply this rule definition only to packets in the downlink (from the Mobile Node) direction.

- **log**
  Default: packets are not logged.
  Indicates all packets which match the redirect are to be logged.

- **source_address**
  The IP address(es) from which the packet originated.
  This option is used to filter all packets from a specific IP address or a group of IP addresses.
  When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the `source_wildcard` parameter.

- **source_wildcard**
  This option is used in conjunction with the `source_address` option to specify a group of addresses for which packets are to be filtered.
  The mask must be entered as a complement:
  - Zero-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be identical.
  - One-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

- **any**
  Specifies that the rule definition applies to all packets.

- **host**
  Specifies that the rule definition applies to a specific host as determined by its IP address.

- **source_host_address**
  The IP address of the source host to filter against expressed in IPv6 colon-separated-hexadecimal notation.
IPv6 ACL Configuration Mode Commands

- **redirect css service** (for downlink, by ICMP packets)

**dest_host_address**
- The IP address of the destination host to filter against expressed in IPv6 colon-separated-hexadecimal notation.

**dest_address**
- The IP address(es) to which the packet is to be sent. This option is used to filter all packets to a specific IP address or a group of IP addresses. When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the **dest_wildcard** parameter.

**dest_wildcard**
- This option is used in conjunction with the **dest_address** option to specify a group of addresses for which packets are to be filtered. The mask must be entered as a complement:
  - Zero-bits in this parameter mean that the corresponding bits configured for the **dest_address** parameter must be identical.
  - One-bits in this parameter mean that the corresponding bits configured for the **dest_address** parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

**icmp_type**
- Specifies that all ICMP packets of a particular type are to be filtered. The type can be an integer value from 0 through 255.

**icmp_code**
- Specifies that all ICMP packets of a particular code are to be filtered. The type can be an integer value from 0 through 255.

**Usage**
- Define a rule definition to block ICMP packets which can be used for address resolution and possibly be a security risk.
- The IP redirecting allows flexible controls for pairs of individual hosts or groups by IP masking which allows the redirecting of entire subnets if necessary.

**Important:** A maximum of 16 rule definitions can be configured per ACL. Also note that “redirect” rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

**Example**

The following command defines a rule definition that redirects packets to the charging service named **css-svcl**, and ICMP packets coming in the downlink (from the Mobile Node) direction from the host with the IP address **2002::c6a2:6419**:

```
redirect css service css-svcl downlink icmp host 2002::c6a2:6419
```

The following sets the insertion point to before the first rule definition above:
IPv6 ACL Configuration Mode Commands

redirect cs service (for downlink, by ICMP packets)

before redirect cs service cs-svcl downlink icmp host 2002::c6a2:6419

The following command sets the insertion point after the second rule definition above:

after redirect cs service cs-svcl downlink icmp host 2002::c6a2:6419

The following deletes the first rule definition above:

no redirect cs service cs-svcl downlink icmp host 2002::c6a2:6419
redirect css service (for downlink, by IP packets)

Used to redirect subscriber sessions based on the internet protocol packets in the downlink (from the Mobile Node) direction.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > IPv6 ACL Configuration
configure > context context_name > ipv6 access-list ipv6_acl_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ipv6-acl)#

Syntax

redirect css service svc_name [ log ] downlink ip { any | host source_host_address | source_address sourceWildcard } { any | host dest_host_address | dest_address destWildcard } [ fragment ]

after redirect css service svc_name [ log ] downlink ip { any | host source_host_address | source_address sourceWildcard } { any | host dest_host_address | dest_address destWildcard } [ fragment ]

before redirect css service svc_name [ log ] downlink ip { any | host source_host_address | source_address sourceWildcard } { any | host dest_host_address | dest_address destWildcard } [ fragment ]

no redirect css service svc_name [ log ] downlink ip { any | host source_host_address | source_address sourceWildcard } { any | host dest_host_address | dest_address destWildcard } [ fragment ]

after
Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

Important: If the options specified do not exactly match an existing rule definition, the insertion point does not change.

before
Indicates all rule definitions defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.
**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

```plaintext
no
```

Removes the rule definition which exactly matches the options specified.

```plaintext
css service svc_name
```

The name of the Content Service Steering (CSS) service to which packets are to be redirected. At the executive mode prompt, use the `show css service all` command to display the names of all configured CSS services. `svc_name` must be a string of 1 through 15 characters.

```plaintext
downlink
```

Apply this rule definition only to packets in the downlink (from the Mobile Node) direction.

```plaintext
log
```

Default: packets are not logged. Indicates all packets which match the redirect are to be logged.

```plaintext
source_address
```

The IP address(es) form which the packet originated. This option is used to filter all packets from a specific IP address or a group of IP addresses. When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the `source wildcard` parameter.

```plaintext
source wildcard
```

This option is used in conjunction with the `source address` option to specify a group of addresses for which packets are to be filtered. The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.

```plaintext
any
```

Specifies that the rule definition applies to all packets.

```plaintext
host
```

Specifies that the rule definition applies to a specific host as determined by its IP address.
source_host_address
The IP address of the source host to filter against expressed in IPv6 colon notation.

dest_host_address
The IP address of the destination host to filter against expressed in IPv6 colon notation.

dest_address
The IP address(es) to which the packet is to be sent.
This option is used to filter all packets to a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the dest_wildcard parameter.

dest_wildcard
This option is used in conjunction with the dest_address option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:
- Zero-bits in this parameter mean that the corresponding bits configured for the dest_address parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the dest_address parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

fragment
Indicates packet redirection is to be applied to IP packet fragments only.

Usage
Block IP packets when the source and destination are of interest.

**Important:** A maximum of 16 rule definitions can be configured per ACL. Also note that “redirect” rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example
The following command defines a rule definition that redirects packets to the charging service named css-svc1, and downlink IP packets coming from the host with the IP address 2002::c6a2:6419, and fragmented packets for any destination are matched:

```
redirect css service css-svc1 downlink ip host 2002::c6a2:6419 any fragment
```

The following sets the insertion point to before the first rule definition above:

```
before redirect css service css-svc1 downlink ip host 2002::c6a2:6419 any fragment
```

The following command sets the insertion point after the second rule definition above:
after redirect css service css-svc1 downlink ip host 2002::c6a2:6419 any fragment

The following deletes the first rule definition above:

no redirect css service css-svc1 downlink ip host 2002::c6a2:6419 any fragment
redirect css service (for downlink, by source IP address masking)

Used to redirect subscriber sessions based on the IP address mask sent by the source in the downlink (from the Mobile Node) direction.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > IPv6 ACL Configuration

```
configure > context context_name > ipv6 access-list ipv6_acl_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipv6-acl)#
```

**Syntax**

- `redirect css service svc_name [ log ] downlink source_address source_wildcard`
- `after redirect css service svc_name [ log ] downlink source_address source_wildcard`
- `before redirect css service svc_name [ log ] downlink source_address source_wildcard`
- `no redirect css service svc_name [ log ] downlink source_address source_wildcard`

**after**
Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

**before**
Indicates all rule definitions defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.
no
Removes the rule definition which exactly matches the options specified.

css service svc_name
The name of the Content Service Steering (CSS) service to which packets are to be redirected. At the executive mode prompt, use the `show css service all` command to display the names of all configured CSS services. `svc_name` must be an alphanumeric string of 1 through 15 characters.

downlink
Apply this rule definition only to packets in the downlink (from the Mobile Node) direction.

log
Default: packets are not logged.
Indicates all packets which match the filter are to be logged.

source_address
The IP address(es) form which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the `source_wildcard` parameter.

source_wildcard
This option is used in conjunction with the `source_address` option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:
- Zero-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

Usage
Define a rule definition when any packet from the IP addresses which fall into the group of addresses matching the IP address masking. This allows the reduction of filtering rule definitions as it does not require a rule definition for each source and destination pair.

**Important:** A maximum of 16 rule definitions can be configured per ACL.

Example
The following command defines a rule definition to redirect packets to a charging service named `css-svcl`:

```
redirect css service css-svcl downlink fe80::c0a8:a04
```
redirect css service (for downlink, by TCP/UDP packets)

Used to redirect subscriber sessions to a charging service based on the transmission control protocol/user datagram protocol packets in the downlink (from the Mobile Node) direction.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > IPv6 ACL Configuration
configure > context context_name > ipv6 access-list ipv6_acl_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ipv6-acl)#

Syntax

redirect css service svc_name [ log ] downlink { tcp | udp } { { source_address
source_wildcard | any | host source_host_address } { eq source_port | gt source_port | lt
source_port | neq source_port | range start_source_port end_source_port } } { {
dest_address dest_wildcard | any | host dest_host_address } { eq dest_port | gt dest_port
| lt dest_port | neq dest_port | range start_dest_port end_dest_port } }

after redirect css service svc_name [ log ] downlink { tcp | udp } { { source_address
source_wildcard | any | host source_host_address } { eq source_port | gt source_port | lt
source_port | neq source_port | range start_source_port end_source_port } } { {
dest_address dest_wildcard | any | host dest_host_address } { eq dest_port | gt dest_port
| lt dest_port | neq dest_port | range start_dest_port end_dest_port } }

no redirect css service svc_name [ log ] downlink { tcp | udp } { { source_address
source_wildcard | any | host source_host_address } { eq source_port | gt source_port | lt
source_port | neq source_port | range start_source_port end_source_port } } { {
dest_address dest_wildcard | any | host dest_host_address } { eq dest_port | gt dest_port
| lt dest_port | neq dest_port | range start_dest_port end_dest_port } }

after

Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.
**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

**before**
Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

**no**
Removes the rule definition which exactly matches the options specified.

**css service svc_name**
The name of the Content Service Steering (CSS) service to which packets are to be redirected. At the executive mode prompt, use the `show css service all` command to display the names of all configured CSS services.
svc_name must be an alphanumeric string of 1 through 15 characters.

**downlink**
Apply this rule definition only to packets in the downlink (from the Mobile Node) direction.

**log**
Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

**tcp | udp**
Specifies the redirect is to be applied to IP-based transmission control protocol or the user datagram protocol.
- **tcp**: Redirect applies to TCP packets.
- **udp**: Redirect applies to UDP packets.

**source_address**
The IP address(es) from which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the `source_wildcard` parameter.

**source_wildcard**
This option is used in conjunction with the `source_address` option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:
- Zero-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

- `any` Specifies that the rule definition applies to all packets.
- `host` Specifies that the rule definition applies to a specific host as determined by its IP address.
  - `source_host_address` The IP address of the source host to filter against expressed in IPv6 colon-separated-hexadecimal notation.
  - `dest_host_address` The IP address of the destination host to filter against expressed in IPv6 colon-separated-hexadecimal notation.
- `eq source_port` Specifies a single, specific source TCP port number to be filtered.
  - `source_port` must be configured to an integer value from 0 to 65535.
- `gt source_port` Specifies that all source TCP port numbers greater than the one specified are to be filtered.
  - `source_port` must be configured to an integer value from 0 to 65535.
- `lt source_port` Specifies that all source TCP port numbers less than the one specified are to be filtered.
  - `source_port` must be configured to an integer value from 0 to 65535.
- `neq source_port` Specifies that all source TCP port numbers not equal to the one specified are to be filtered.
  - `source_port` must be configured to an integer value from 0 to 65535.
- `range start_source_port end_source_port` Specifies that all source TCP ports within a specific range are to be filtered.
  - `start_source_port` is the initial port in the range and `end_source_port` is the final port in the range.
  - Both `start_source_port` and `end_source_port` can be configured to an integer value from 0 to 65535.
- `dest_address` The IP address(es) to which the packet is to be sent.
  - This option is used to filter all packets to a specific IP address or a group of IP addresses.
  - When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the `dest_wildcard` parameter.
**IPv6 ACL Configuration Mode Commands**

**redirect css service (for downlink, by TCP/UDP packets)**

---

**dest_wildcard**

This option is used in conjunction with the *dest_address* option to specify a group of addresses for which packets are to be filtered. The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the *dest_address* parameter must be ignored.

---

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

---

**eq dest_port**

Specifies a single, specific destination TCP port number to be filtered. *dest_port* must be configured to an integer value from 0 to 65535.

---

**gt dest_port**

Specifies that all destination TCP port numbers greater than the one specified are to be filtered. *dest_port* must be configured to an integer value from 0 to 65535.

---

**lt dest_port**

Specifies that all destination TCP port numbers less than the one specified are to be filtered. *dest_port* must be configured to an integer value from 0 to 65535.

---

**neq dest_port**

Specifies that all destination TCP port numbers not equal to the one specified are to be filtered. *dest_port* must be configured to an integer value from 0 to 65535.

---

**range start_dest_port end_dest_port**

Specifies that all destination TCP ports within a specific range are to be filtered. *start_dest_port* is the initial port in the range and *end_dest_port* is the final port in the range. Both *start_dest_port* and *end_dest_port* can be configured to an integer value from 0 to 65535.

---

**Usage**

Block IP packets when the source and destination are of interest but for only a limited set of ports.

---

**Important:** A maximum of 16 rule definitions can be configured per ACL. Also note that “redirect” rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

---

**Example**

The following command defines a rule definition that redirects packets to the charging service named *css-svcl*, and UDP packets coming from any host are matched:

```
redirect css service css-svcl downlink udp any
```

The following sets the insertion point to before the rule definition above:

---

Cisco ASR 5x00 Command Line Interface Reference
before redirect css service css-svcl downlink udp any

The following command sets the insertion point after the rule definition above:

after redirect css service css-svcl downlink udp any

The following deletes the rule definition above:

no redirect css service css-svcl downlink udp any
redirect css service (for uplink, any)

Used to redirect subscriber sessions based on any packet received in the uplink (to the Mobile Node) direction. This command is also used to set the access control list insertion point.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > IPv6 ACL Configuration
configure > context context_name > ipv6 access-list ipv6_acl_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipv6-acl)#
```

**Syntax**

```
redirect css service svc_name [ log ] uplink any
after redirect css service svc_name [ log ] uplink any
before redirect css service svc_name [ log ] uplink any
no redirect css service svc_name [ log ] uplink any
```

**after**
Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

**before**
Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

**no**
Removes the rule definition which exactly matches the options specified.
**css service svc_name**

The name of the Content Service steering (CSS) service to which packets are to be redirected. At the executive mode prompt, use the `show css service all` command to display the names of all configured CSS services. `svc_name` must be an alphanumeric string of 1 through 15 characters.

**uplink**

Apply this rule definition only to packets in the uplink (to the Mobile Node) direction.

**log**

Default: packets are not logged. Indicates all packets which match the redirect are to be logged.

**any**

Indicates all packets will match the redirect regardless of source and/or destination.

**Usage**

Define a catch all rule definition to place at the end of the list of rule definitions to provide explicit handling of rule definitions which do not fit any other criteria.

**Important:** It is suggested that any rule definition which is added to be a catch all should also have the `log` option specified. The logged packets may be used to determine if the current list of rule definitions is adequate or needs modification to ensure proper security.

**Important:** A maximum of 16 rule definitions can be configured per ACL.

**Important:** Also note that “redirect” rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

**Example**

The following command defines a rule definition that redirects packets to the charging service with the name `css-svc1` and any source IP:

```
redirect css service css-svc1 uplink any
```

The following sets the insertion point to before the first rule definition above:

```
before redirect css service css-svc1 uplink any
```

The following command sets the insertion point after the second rule definition above:

```
after redirect css service css-svc1 uplink any
```

The following deletes the first rule definition above:

```
no redirect css service css-svc1 uplink any
```
redirect css service (for uplink, by host IP address)

Used to redirect subscriber sessions based on the targeted host IP address in the uplink (to the Mobile Node) direction.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > IPv6 ACL Configuration
configure > context context_name > ipv6 access-list ipv6_acl_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ipv6-acl)#

Syntax

redirect css service svc_name [ log ] uplink host source_host_address
after redirect css service svc_name [ log ] uplink host source_host_address
before redirect css service svc_name [ log ] uplink host source_host_address
no redirect css service svc_name [ log ] uplink host source_host_address

uplink
Apply this rule definition only to packets in the uplink (to the Mobile Node) direction.

after
Indicates all rule definitions defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

Important: If the options specified do not exactly match an existing rule definition, the insertion point does not change.

before
Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

Important: If the options specified do not exactly match an existing rule definition, the insertion point does not change.
redirect css service (for uplink, by host IP address)

no
Removes the rule definition which exactly matches the options specified.

css service svc_name
The name of the Content service Steering (CSS) service to which packets are to be redirected. At the executive mode prompt, use the show css service all command to display the names of all configured CSS services.
svc_name must be an alphanumeric string of 1 through 15 characters.

uplink
Apply this rule definition only to packets in the uplink (to the Mobile Node) direction.

log
Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

host
Specifies that the rule definition applies to a specific host as determined by its IP address.

source_host_address
The IP address of the source host to filter against expressed in IPv6 colon notation.

Usage
Define a rule definition when a very specific remote host is to be blocked. In simplified networks where the access controls need only block a few hosts, this command allows the rule definitions to be very clear and concise.

Important: A maximum of 16 rule definitions can be configured per ACL. Also note that “redirect” rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example
The following command defines a rule definition that redirects packets to the charging service with the name css-svc1 and a host IP address of fe80::c0a8:c80b:

    redirect service css-svc1 uplink host fe80::c0a8:c80b

The following sets the insertion point to before the first rule definition above:

    before redirect service css-svc1 uplink host fe80::c0a8:c80b

The following command sets the insertion point after the second rule definition above:

    after redirect service css-svc1 uplink host fe80::c0a8:c80b

The following deletes the first rule definition above:

    no redirect service css-svc1 uplink host fe80::c0a8:c80b
redirect css service (for uplink, by ICMP packets)

Used to redirect subscriber sessions based on the internet control message protocol packets in the uplink (to the Mobile Node) direction.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > IPv6 ACL Configuration
configure > context context_name > ipv6 access-list ipv6_acl_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ipv6-acl)#

Syntax

redirect css service svc_name [ log ] uplink icmp { any | host source_host_address | source_address source_wildcard } { any | host dest_host_address | dest_address dest_wildcard } [ icmp_type [ icmp_code ] ]

after
Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

Important: If the options specified do not exactly match an existing rule definition, the insertion point does not change.

before
Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

Important: If the options specified do not exactly match an existing rule definition, the insertion point does not change.

no
Removes the rule definition which exactly matches the options specified.
css service svc_name

The name of the Content Service Steering (CSS) service to which packets are to be redirected. At the executive mode prompt, use the show css service all command to display the names of all configured CSS services. svc_name must be an alphanumeric string of 1 through 15 characters.

uplink

Apply this rule definition only to packets in the uplink (to the Mobile Node) direction.

log

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

source_address

The IP address(es) from which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the source_wildcard parameter.

source_wildcard

This option is used in conjunction with the source_address option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:
• Zero-bits in this parameter mean that the corresponding bits configured for the source_address parameter must be identical.
• One-bits in this parameter mean that the corresponding bits configured for the source_address parameter must be ignored.

Important: The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

any

Specifies that the rule definition applies to all packets.

host

Specifies that the rule definition applies to a specific host as determined by its IP address.

source_host_address

The IP address of the source host to filter against expressed in IPv6 colon-separated-hexadecimal notation.

dest_host_address

The IP address of the destination host to filter against expressed in IPv6 colon-separated-hexadecimal notation.

dest_address

The IP address(es) to which the packet is to be sent.
This option is used to filter all packets to a specific IP address or a group of IP addresses. When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the dest_wildcard parameter.

**dest_wildcard**

This option is used in conjunction with the dest_address option to specify a group of addresses for which packets are to be filtered. The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the dest_address parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the dest_address parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

**icmp_type**

Specifies that all ICMP packets of a particular type are to be filtered. The type can be an integer value from 0 through 255.

**icmp_code**

Specifies that all ICMP packets of a particular code are to be filtered. The type can be an integer value from 0 through 255.

**Usage**

Define a rule definition to block ICMP packets which can be used for address resolution and possibly be a security risk. The IP redirecting allows flexible controls for pairs of individual hosts or groups by IP masking which allows the redirecting of entire subnets if necessary.

**Important:** A maximum of 16 rule definitions can be configured per ACL. Also note that “redirect” rule definitions are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

**Example**

The following command defines a rule definition that redirects packets to the charging service named chgsvc1, and ICMP packets in the uplink (to the Mobile Node) direction from the host with the IP address 198.162.100.25:

```
redirect css service chgsvc1 uplink icmp host 198.162.100.25
```

The following sets the insertion point to before the first rule definition above:

```
before redirect css service chgsvc1 uplink icmp host 198.162.100.25
```

The following command sets the insertion point after the second rule definition above:

```
after redirect css service chgsvc1 uplink icmp host 198.162.100.25
```

The following deletes the first rule definition above:
no redirect css service chgsvcl uplink icmp host 198.162.100.25
redirect css service (for uplink, by IP packets)

Used to redirect subscriber sessions based on the internet protocol packets in the uplink (to the Mobile Node) direction.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > IPv6 ACL Configuration

```
configure > context context_name > ipv6 access-list ipv6_acl_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipv6-acl)#
```

**Syntax**

```
redirect css service svc_name [ log ] uplink ip { any | host source_host_address | source_address source_wildcard } { any | host dest_host_address | dest_address dest_wildcard } [ fragment ]

after redirect css service svc_name [ log ] uplink ip { any | host source_host_address | source_address source_wildcard } { any | host dest_host_address | dest_address dest_wildcard } [ fragment ]

before redirect css service svc_name [ log ] uplink ip { any | host source_host_address | source_address source_wildcard } { any | host dest_host_address | dest_address dest_wildcard } [ fragment ]

no redirect css service svc_name [ log ] uplink ip { any | host source_host_address | source_address source_wildcard } { any | host dest_host_address | dest_address dest_wildcard } [ fragment ]
```

- **after**
  
  Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.
  
  This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

- **before**
  
  Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed.
  
  This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

---

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.
redirect css service (for uplink, by IP packets)

**Important:** If the options specified do not exactly match an existing rule definition, the insertion point does not change.

```plaintext
no
Removes the rule definition which exactly matches the options specified.
```

```plaintext
css service svc_name
The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the `show active-charging service all` command to display the names of all configured charging services.
`svc_name` must be a string of 1 through 15 characters.
```

```plaintext
uplink
Apply this rule definition only to packets in the uplink (to the Mobile Node) direction.
```

```plaintext
log
Default: packets are not logged. Indicates all packets which match the redirect are to be logged.
```

```plaintext
source_address
The IP address(es) from which the packet originated. This option is used to filter all packets from a specific IP address or a group of IP addresses. When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the `source_wildcard` parameter.
```

```plaintext
source_wildcard
This option is used in conjunction with the `source_address` option to specify a group of addresses for which packets are to be filtered. The mask must be entered as a complement:
- Zero-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be ignored.
```

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.

```plaintext
any
Specifies that the rule definition applies to all packets.
```

```plaintext
host
Specifies that the rule definition applies to a specific host as determined by its IP address.
```
IPv6 ACL Configuration Mode Commands

redirect css service (for uplink, by IP packets)

source_host_address
The IP address of the source host to filter against expressed in IPv6 colon notation.

dest_host_address
The IP address of the destination host to filter against expressed in IPv6 colon notation.

dest_address
The IP address(es) to which the packet is to be sent. This option is used to filter all packets to a specific IP address or a group of IP addresses. When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the dest_wildcard parameter.

dest_wildcard
This option is used in conjunction with the dest_address option to specify a group of addresses for which packets are to be filtered. The mask must be entered as a complement:
- Zero-bits in this parameter mean that the corresponding bits configured for the dest_address parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the dest_address parameter must be ignored.

fragment
Indicates packet redirection is to be applied to IP packet fragments only.

Usage
Block IP packets when the source and destination are of interest.

Example
The following command defines a rule definition that redirects packets to the charging service named chgsvcl, and uplink IP packets going to the host with the IP address 198.162.100.25, and fragmented packets for any destination are matched:

   redirect css service chgsvcl uplink ip host 198.162.100.25 any fragment

The following sets the insertion point to before the first rule definition above:

   redirect css service chgsvcl uplink ip host 198.162.100.25 any fragment

The following command sets the insertion point after the second rule definition above:

   after redirect css service chgsvcl uplink ip host 198.162.100.25 any fragment

The following deletes the first rule definition above:

   no redirect css service chgsvcl uplink ip host 198.162.100.25 any fragment
redirect css service (for uplink, by source IP address masking)

Used to redirect subscriber sessions based on the IP address mask sent by the source in the uplink (to the Mobile Node) direction.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > IPv6 ACL Configuration
```
configure > context context_name > ipv6 access-list ipv6_acl_name
```

Entering the above command sequence results in the following prompt:
```
[context_name]host_name(config-ipv6-acl)#
```

**Syntax**

```
redirect css service svc_name [ log ] uplink source_address source_wildcard
```

**after**
Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed. This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.

**before**
Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed. This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

**no**
Removes the rule definition which exactly matches the options specified.

**css service svc_name**
The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the `show active-charging service all` command to display the names of all configured charging services.

`svc_name` must be a string of 1 through 15 characters.

**uplink**
Apply this rule definition only to packets in the uplink (to the Mobile Node) direction.

**log**
Default: packets are not logged.
Indicates all packets which match the filter are to be logged.
source_address

The IP address(es) form which the packet originated. This option is used to filter all packets from a specific IP address or a group of IP addresses. When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the source_wildcard parameter.

source_wildcard

This option is used in conjunction with the source_address option to specify a group of addresses for which packets are to be filtered. The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the source_address parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the source_address parameter must be ignored.

Usage

Define a rule definition when any packet from the IP addresses which fall into the group of addresses matching the IP address masking. This allows the reduction of filtering rule definitions as it does not require a rule definition for each source and destination pair.

Example

The following command defines a rule definition to redirect packets to a charging service named chgsvc1:

```
redirect css service chgsvc1 uplink 1:1:1:1:1:1:1:1
```
redirect css service (for uplink, by TCP/UDP packets)

Used to redirect subscriber sessions to a charging service based on the transmission control protocol/user datagram protocol packets in the uplink (to the Mobile Node) direction.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > IPv6 ACL Configuration

```bash
configure > context context_name > ipv6 access-list ipv6_acl_name
```

Entering the above command sequence results in the following prompt:

```
[context_name] host_name(config-ipv6-acl)#
```

**Syntax**

```bash
redirect css service svc_name [ log ] uplink { tcp | udp } { { source_address source_wildcard | any | source_host_address } [ eq source_port | gt source_port | lt source_port | neq source_port | range start_source_port end_source_port ] } { { dest_address dest_wildcard | any | host dest_host_address } [ eq dest_port | gt dest_port | lt dest_port | neq dest_port | range start_dest_port end_dest_port ] }
```

- **after redirect css service svc_name [ log ] uplink { tcp | udp } { { source_address source_wildcard | any | source_host_address } [ eq source_port | gt source_port | lt source_port | neq source_port | range start_source_port end_source_port ] } { { dest_address dest_wildcard | any | host dest_host_address } [ eq dest_port | gt dest_port | lt dest_port | neq dest_port | range start_dest_port end_dest_port ] }

- **before redirect css service svc_name [ log ] uplink { tcp | udp } { { source_address source_wildcard | any | source_host_address } [ eq source_port | gt source_port | lt source_port | neq source_port | range start_source_port end_source_port ] } { { dest_address dest_wildcard | any | host dest_host_address } [ eq dest_port | gt dest_port | lt dest_port | neq dest_port | range start_dest_port end_dest_port ] }

- **no redirect css service svc_name [ log ] uplink { tcp | udp } { { source_address source_wildcard | any | source_host_address } [ eq source_port | gt source_port | lt source_port | neq source_port | range start_source_port end_source_port ] } { { dest_address dest_wildcard | any | host dest_host_address } [ eq dest_port | gt dest_port | lt dest_port | neq dest_port | range start_dest_port end_dest_port ] }

**after**

Indicates all rule definitions subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to be immediately after the rule definition which matches the exact options specified such that new rule definitions will be added, in order, after the matching rule definition.
IPv6 ACL Configuration Mode Commands

redirect css service (for uplink, by TCP/UDP packets)

before
Indicates all rule definitions subsequent to this command are to be inserted before the command identified by the exact options listed. This moves the insertion point to be immediately before the rule definition which matches the exact options specified such that new rule definitions will be added, in order, before the matching rule definition.

no
Removes the rule definition which exactly matches the options specified.

css service svc_name
The name of the active charging service to which packets are to be redirected. At the executive mode prompt, use the show active-charging service all command to display the names of all configured charging services. svc_name must be a string of 1 through 15 characters.

uplink
Apply this rule definition only to packets in the uplink (to the Mobile Node) direction.

log
Default: packets are not logged. Indicates all packets which match the redirect are to be logged.

tcp | udp
Specifies the redirect is to be applied to IP-based transmission control protocol or the user datagram protocol.

• tcp: Redirect applies to TCP packets.
• udp: Redirect applies to UDP packets.

source_address
The IP address(es) from which the packet originated. This option is used to filter all packets from a specific IP address or a group of IP addresses. When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the source_wildcard parameter.

source_wildcard
This option is used in conjunction with the source_address option to specify a group of addresses for which packets are to be filtered. The mask must be entered as a complement:

• Zero-bits in this parameter mean that the corresponding bits configured for the source_address parameter must be identical.
• One-bits in this parameter mean that the corresponding bits configured for the source_address parameter must be ignored.

any
Specifies that the rule definition applies to all packets.
**IPv6 ACL Configuration Mode Commands**

- **host**
  Specifies that the rule definition applies to a specific host as determined by its IP address.

- **source_host_address**
  The IP address of the source host to filter against expressed in IPv6 colon notation.

- **dest_host_address**
  The IP address of the destination host to filter against expressed in IPv6 colon notation.

- **eq source_port**
  Specifies a single, specific source TCP port number to be filtered. **source_port** must be configured to an integer value from 0 to 65535.

- **gt source_port**
  Specifies that all source TCP port numbers greater than the one specified are to be filtered. **source_port** must be configured to an integer value from 0 to 65535.

- **lt source_port**
  Specifies that all source TCP port numbers less than the one specified are to be filtered. **source_port** must be configured to an integer value from 0 to 65535.

- **neq source_port**
  Specifies that all source TCP port numbers not equal to the one specified are to be filtered. **source_port** must be configured to an integer value from 0 to 65535.

- **range start_source_port end_source_port**
  Specifies that all source TCP ports within a specific range are to be filtered. **start_source_port** is the initial port in the range and **end_source_port** is the final port in the range. Both **start_source_port** and **end_source_port** can be configured to an integer value from 0 to 65535.

- **dest_address**
  The IP address(es) to which the packet is to be sent. This option is used to filter all packets to a specific IP address or a group of IP addresses. When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the **dest_wildcard** parameter.

- **dest_wildcard**
  This option is used in conjunction with the **dest_address** option to specify a group of addresses for which packets are to be filtered. The mask must be entered as a complement:
  - Zero-bits in this parameter mean that the corresponding bits configured for the **dest_address** parameter must be identical.
  - One-bits in this parameter mean that the corresponding bits configured for the **dest_address** parameter must be ignored.
eq dest_port
Specifies a single, specific destination TCP port number to be filtered.
dest_port must be configured to an integer value from 0 to 65535.

gt dest_port
Specifies that all destination TCP port numbers greater than the one specified are to be filtered.
dest_port must be configured to an integer value from 0 to 65535.

lt dest_port
Specifies that all destination TCP port numbers less than the one specified are to be filtered.
dest_port must be configured to an integer value from 0 to 65535.

neq dest_port
Specifies that all destination TCP port numbers not equal to the one specified are to be filtered.
dest_port must be configured to an integer value from 0 to 65535.

range start_dest_port end_dest_port
Specifies that all destination TCP ports within a specific range are to be filtered.
start_dest_port is the initial port in the range and end_dest_port is the final port in the range.
Both start_dest_port and end_dest_port can be configured to an integer value from 0 to 65535.

Usage
Block IP packets when the source and destination are of interest but for only a limited set of ports.

Example
The following command defines a rule definition that redirects packets to the charging service named chgsvcl, and UDP packets coming from any host are matched:

   redirect css service chgsvcl uplink udp any

The following sets the insertion point to before the rule definition above:

   before redirect css service chgsvcl uplink udp any

The following command sets the insertion point after the rule definition above:

   after redirect css service chgsvcl uplink udp any

The following deletes the rule definition above:

   no redirect css service chgsvcl uplink udp any
redirect nexthop (by IP address masking)

Used to redirect subscriber sessions based on the IP address mask sent by the source to the mobile node or the network.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > IPv6 ACL Configuration

configure > context context_name > ipv6 access-list ipv6_acl_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ipv6-acl)#

**Syntax**

\[
\text{redirect nexthop } \text{nexthop_addr \{ context context_id | interface interface_name \} [ log ]}
\]

\[
\text{source_address source_wildcard}
\]

\[
\text{after redirect nexthop } \text{nexthop_addr \{ context context_id | interface interface_name \} [ log ]}
\]

\[
\text{source_address source_wildcard}
\]

\[
\text{before redirect nexthop } \text{nexthop_addr \{ context context_id | interface interface_name \} [ log ]}
\]

\[
\text{source_address source_wildcard}
\]

\[
\text{no redirect nexthop } \text{nexthop_addr \{ context context_id | interface interface_name \} [ log ]}
\]

\[
\text{source_address source_wildcard}
\]

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

\[
\text{after}
\]

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

\[
\text{before}
\]

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Removes the rule which exactly matches the options specified.</td>
</tr>
<tr>
<td><code>nexthop nexthop_addr</code></td>
<td>The IP address to which the IP packets are redirected.</td>
</tr>
<tr>
<td><code>context context_id</code></td>
<td>The context identification number of the context to which packets are redirected. At the executive mode prompt, use the <code>show context all</code> command to display context names and context IDs.</td>
</tr>
<tr>
<td><code>interface interface_name</code></td>
<td>The name of the logical interface to which the packets should be redirected. <code>interface_name</code> must be an alpha and/or numeric string from 1 to 79 characters.</td>
</tr>
<tr>
<td>log</td>
<td>Default: packets are not logged. Indicates all packets which match the redirect are to be logged.</td>
</tr>
<tr>
<td><code>source_address</code></td>
<td>The IP address(es) form which the packet originated. This option is used to filter all packets from a specific IP address or a group of IP addresses. When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the <code>source_wildcard</code> parameter.</td>
</tr>
</tbody>
</table>
| `source_wildcard` | This option is used in conjunction with the `source_address` option to specify a group of addresses for which packets are to be filtered. The mask must be entered as a complement:  
  * Zero-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be identical.  
  * One-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be ignored.  

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is **not** acceptable since the one-bits are not contiguous.  

**Usage**  
Define a rule when any packet from the IP addresses which fall into the group of addresses matching the IP address masking. This allows the reduction of redirect rules as it does not require a rule for each source and destination pair.  

**Important:** The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the Engineering Rules appendix in the System Administration Guide. Also
note that “redirect” rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example

The following command defines a rule that redirects packets to the next hop host at 192.168.10.4, the context with the context ID of 23 and the source IP and wildcard of 198.162.22.0 and 0.0.0.31:

```
redirect nexthop 192.168.10.4 context 23 198.162.22.0 0.0.0.31
```

The following sets the insertion point to before the first rule defined above:

```
before redirect nexthop 192.168.10.4 context 23 198.162.22.0 0.0.0.31
```

The following command sets the insertion point after the second rule defined above:

```
after redirect nexthop 192.168.10.4 context 23 198.162.22.0 0.0.0.31
```

The following deletes the first rule defined above:

```
no redirect nexthop 192.168.10.4 context 23 198.162.22.0 0.0.0.31
```
redirect nexthop (any)

Used to redirect subscriber sessions based on any packet received. This command is also used to set the access control list insertion point.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > IPv6 ACL Configuration
configure > context context_name > ipv6 access-list ipv6_acl_name

Entering the above command sequence results in the following prompt:

>[context_name]host_name(config-ipv6-acl)#

Syntax

redirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ] any

after redirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ] any

before redirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ] any

no redirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ] any

after
 Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

Important: If the options specified do not exactly match an existing rule, the insertion point does not change.

before
 Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

Important: If the options specified do not exactly match an existing rule, the insertion point does not change.
redirect nexthop (any)

no
Removes the rule which exactly matches the options specified.

nexthop nexthop_addr
The IP address to which the IP packets are redirected.

context context_id
The context identification number of the context to which packets are redirected. At the executive mode prompt, use the show context all command to display context names and context IDs.

interface interface_name
The name of the logical interface to which the packets should be redirected. interface_name must be an alpha and/or numeric string from 1 to 79 characters.

log
Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

any
Indicates all packets will match the redirect regardless of source and/or destination.

Usage
Define a catch all rule to place at the end of the list of rules to provide explicit handling of rules which do not fit any other criteria.

Important: It is suggested that any rule which is added to be a catch all should also have the log option specified. The logged packets may be used to determine if the current list of rules is adequate or needs modification to ensure proper security. The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the Engineering Rules appendix in the System Administration Guide. Also note that “redirect” rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example
The following command defines a rule that redirects packets to the next hop host at 192.168.10.4, the context with the context ID of 23 and any source IP:

   redirect nexthop 192.168.10.4 context 23 any

The following sets the insertion point to before the first rule defined above:

   before redirect nexthop 192.168.10.4 context 23 any

The following command sets the insertion point after the second rule defined above:

   after redirect nexthop 192.168.10.4 context 23 any

The following deletes the first rule defined above:
no redirect nexthop 192.168.10.4 context 23 any
redirect nexthop (by host IP address)

Used to redirect subscriber sessions based on the targeted host IP address sent by the source to the mobile node or the network.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > IPv6 ACL Configuration

configure > context context_name > ipv6 access-list ipv6_acl_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ipv6-acl)#

Syntax

redirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ] host source_ip_address

after redirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ] host source_ip_address

before redirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ] host source_ip_address

no redirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ] host source_ip_address

**after**

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

**before**

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.
no
Removes the rule which exactly matches the options specified.

nexthop  nexthop_addr
The IP address to which the IP packets are redirected.

context  context_id
The context identification number of the context to which packets are redirected. At the executive mode prompt, use the show context all command to display context names and context IDs.

interface  interface_name
The name of the logical interface to which the packets should be redirected. interface_name must be an alpha and/or numeric string from 1 to 79 characters.

log
Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

host
Specifies that the rule applies to a specific host as determined by its IP address.

source_host_address
The IP address of the source host to filter against expressed in IPv6 colon notation.

Usage
Define a rule when a very specific remote host is to be blocked. In simplified networks where the access controls need only block a few hosts, this command allows the rules to be very clear and concise.

Important: The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the Engineering Rules appendix in the System Administration Guide. Also note that “redirect” rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

Example
The following command defines a rule that redirects packets to the next hop host at 192.168.10.4, the context with the context ID of 23 and a host IP address of 192.168.200.11:

    redirect nexthop 192.168.10.4 context 23 host 192.168.200.11

The following sets the insertion point to before the first rule defined above:

    before redirect nexthop 192.168.10.4 context 23 host 192.168.200.11

The following command sets the insertion point after the second rule defined above:

    after redirect nexthop 192.168.10.4 context 23 host 192.168.200.11
The following deletes the first rule defined above:

```
no redirect nexthop 192.168.10.4 context 23 host 192.168.200.11
```
redirect nexthop (by source ICMP packets)

Used to redirect subscriber sessions based on the internet control message protocol packets sent by the source to the mobile node or the network.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > IPv6 ACL Configuration

configure > context context_name > ipv6 access-list ipv6_acl_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ipv6-acl)#
```

**Syntax**

```
redirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ] icmp { source_address source_wildcard | any | host source_host_address }{ dest_address dest_wildcard | any | host dest_host_address } [ icmp_type [ icmp_code ] ]

after redirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ] icmp { source_address source_wildcard | any | host source_host_address }{ dest_address dest_wildcard | any | host dest_host_address } [ icmp_type [ icmp_code ] ]

before redirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ] icmp { source_address source_wildcard | any | host source_host_address }{ dest_address dest_wildcard | any | host dest_host_address } [ icmp_type [ icmp_code ] ]

no redirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ] icmp { source_address source_wildcard | any | host source_host_address }{ dest_address dest_wildcard | any | host dest_host_address } [ icmp_type [ icmp_code ] ]
```

**after**

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

**before**

Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.
**redirect nexthop (by source ICMP packets)**

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>no</strong></td>
<td>Removes the rule which exactly matches the options specified.</td>
</tr>
<tr>
<td><strong>nexthop</strong> nexthop_addr</td>
<td>The IP address to which the IP packets are redirected.</td>
</tr>
<tr>
<td><strong>context</strong> context_id</td>
<td>The context identification number of the context to which packets are redirected. At the executive mode prompt, use the <code>show context all</code> command to display context names and context IDs.</td>
</tr>
<tr>
<td><strong>interface</strong> interface_name</td>
<td>The name of the logical interface to which the packets should be redirected. <code>interface_name</code> must be an alpha and/or numeric string from 1 to 79 characters.</td>
</tr>
<tr>
<td><strong>log</strong></td>
<td>Default: packets are not logged. Indicates all packets which match the redirect are to be logged.</td>
</tr>
<tr>
<td><strong>source_address</strong></td>
<td>The IP address(es) form which the packet originated. This option is used to filter all packets from a specific IP address or a group of IP addresses. When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the <code>source_wildcard</code> parameter.</td>
</tr>
</tbody>
</table>
| **source_wildcard**            | This option is used in conjunction with the `source_address` option to specify a group of addresses for which packets are to be filtered. The mask must be entered as a complement:  
  - Zero-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be identical.  
  - One-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be ignored. |

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>any</strong></td>
<td>Specifies that the rule applies to all packets.</td>
</tr>
<tr>
<td><strong>host</strong></td>
<td>Specifies that the rule applies to a specific host as determined by its IP address.</td>
</tr>
</tbody>
</table>
source_host_address
The IP address of the source host to filter against expressed in IPv6 colon notation.

dest_host_address
The IP address of the destination host to filter against expressed in IPv6 colon notation.

dest_address
The IP address(es) to which the packet is to be sent.
This option is used to filter all packets to a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this parameter.
The range can then be configured using the dest_wildcard parameter.

dest_wildcard
This option is used in conjunction with the dest_address option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:
- Zero-bits in this parameter mean that the corresponding bits configured for the dest_address parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the dest_address parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

icmp_type
Specifies that all ICMP packets of a particular type are to be filtered. The type can be an integer value from 0 through 255.

icmp_code
Specifies that all ICMP packets of a particular code are to be filtered. The type can be an integer value from 0 through 255.

**Usage**

Define a rule to block ICMP packets which can be used for address resolution and possible be a security risk.
The IP redirecting allows flexible controls for pairs of individual hosts or groups by IP masking which allows the redirecting of entire subnets if necessary.

**Important:** The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used.
For more information, refer to the Engineering Rules appendix in the System Administration Guide.
Also note that “redirect” rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

**Example**

The following command defines a rule that redirects packets to the next hop host at `fe80::c0a8:a04`, the context with the context ID of 23, and ICMP packets coming from the host with the IP address `2002::c6a2:64195`:
redirect nexthop fe80::c0a8:a04 context 23 icmp host 2002::c6a2:6419

The following sets the insertion point to before the first rule defined above:

before redirect nexthop fe80::c0a8:a04 context 23 icmp host 2002::c6a2:6419

The following command sets the insertion point after the second rule defined above:

after redirect nexthop fe80::c0a8:a04 context 23 icmp host 2002::c6a2:6419

The following deletes the first rule defined above:

no redirect nexthop fe80::c0a8:a04 context 23 icmp host 2002::c6a2:6419
redirect nexthop (by IP packets)

Used to redirect subscriber sessions based on the internet protocol packets sent by the source to the mobile node or the network.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > IPv6 ACL Configuration
configure > context context_name > ipv6 access-list ipv6_acl_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ipv6-acl)#

Syntax

redirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ]
ip { source_address source wildcard | any | host source_host_address } { dest_address dest wildcard | any | host dest_host_address } [ fragment ] [ protocol num ]

after
Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.
This moves the insertion point to be immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

Important: If the options specified do not exactly match an existing rule, the insertion point does not change.

before
Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

Important: If the options specified do not exactly match an existing rule, the insertion point does not change.

no
Removes the rule which exactly matches the options specified.

nexthop nexthop_addr
The IP address to which the IP packets are redirected.
**context context_id**

The context identification number of the context to which packets are redirected. At the executive mode prompt, use the `show context all` command to display context names and context IDs.

**interface interface_name**

The name of the logical interface to which the packets should be redirected. `interface_name` must be an alphanumeric string from 1 through 79 characters.

**log**

Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

**source_address**

The IP address(es) from which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the `source_wildcard` parameter.

**source_wildcard**

This option is used in conjunction with the `source_address` option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:
- Zero-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be ignored.

**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

**any**

Specifies that the rule applies to all packets.

**host**

Specifies that the rule applies to a specific host as determined by its IP address.

**source_host_address**

The IP address of the source host to filter against expressed in IPv6 colon-separated-hexadecimal notation.

**dest_host_address**

The IP address of the destination host to filter against expressed in IPv6 colon-separated-hexadecimal notation.

**dest_address**

The IP address(es) to which the packet is to be sent.
This option is used to filter all packets to a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this parameter. The range can then be configured using the `dest_wildcard` parameter.

`dest_wildcard`

This option is used in conjunction with the `dest_address` option to specify a group of addresses for which packets are to be filtered.

The mask must be entered as a complement:

- Zero-bits in this parameter mean that the corresponding bits configured for the `dest_address` parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the `dest_address` parameter must be ignored.

**Important**: The mask must contain a contiguous set of one-bits from the least significant bit (LSB).

`fragment`

Indicates packet redirection is to be applied to IP packet fragments only.

`protocol num`

Indicates that the packet filtering is to be applied to a specific protocol number. `num` can be an integer from 0 through 255.

**Usage**

Block IP packets when the source and destination are of interest.

**Important**: The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the Engineering Rules appendix in the System Administration Guide. Also note that “redirect” rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.
redirect nexthop (by TCP/UDP packets)

Used to redirect subscriber sessions based on the transmission control protocol/user datagram protocol packets sent by the source to the mobile node or the network.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > IPv6 ACL Configuration

configure > context context_name > ipv6 access-list ipv6_acl_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ipv6-acl)#

Syntax

redirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ] { tcp | udp } { { source_address source_wildcard | any | host source_host_address } [ eq source_port | gt source_port | lt source_port | neq source_port ] } { { dest_address dest_wildcard | any | host dest_host_address } [ eq dest_port | gt dest_port | lt dest_port | neq dest_port ] }

after redirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ] { tcp | udp } { { source_address source_wildcard | any | host source_host_address } [ eq source_port | gt source_port | lt source_port | neq source_port ] } { { dest_address dest_wildcard | any | host dest_host_address } [ eq dest_port | gt dest_port | lt dest_port | neq dest_port ] }

before redirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ] { tcp | udp } { { source_address source_wildcard | any | host source_host_address } [ eq source_port | gt source_port | lt source_port | neq source_port ] } { { dest_address dest_wildcard | any | host dest_host_address } [ eq dest_port | gt dest_port | lt dest_port | neq dest_port ] }

no redirect nexthop nexthop_addr { context context_id | interface interface_name } [ log ] { tcp | udp } { { source_address source_wildcard | any | host source_host_address } [ eq source_port | gt source_port | lt source_port | neq source_port ] } { { dest_address dest_wildcard | any | host dest_host_address } [ eq dest_port | gt dest_port | lt dest_port | neq dest_port ] }

after

Indicates all rules defined subsequent to this command are to be inserted after the command identified by the exact options listed.

This moves the insertion point to immediately after the rule which matches the exact options specified such that new rules will be added, in order, after the matching rule.

> Important: If the options specified do not exactly match an existing rule, the insertion point does not change.
IPv6 ACL Configuration Mode Commands

redirect next-hop (by TCP/UDP packets)

**before**
Indicates all rules defined subsequent to this command are to be inserted before the command identified by the exact options listed.
This moves the insertion point to be immediately before the rule which matches the exact options specified such that new rules will be added, in order, before the matching rule.

**Important:** If the options specified do not exactly match an existing rule, the insertion point does not change.

**no**
Removes the rule which exactly matches the options specified.

**nexthop**  
**nexthop_addr**
The IP address to which the IP packets are redirected.

**context**  
**context_id**
The context identification number of the context to which packets are redirected. At the executive mode prompt, use the `show context all` command to display context names and context IDs.

**interface**  
**interface_name**
The name of the logical interface to which the packets should be redirected. `interface_name` must be an alphanumeric string from 1 through 79 characters.

**log**
Default: packets are not logged.
Indicates all packets which match the redirect are to be logged.

**tcp** | **udp**
Specifies the redirect is to be applied to IP-based transmission control protocol or the user datagram protocol.
- **tcp**: Redirect applies to TCP packets.
- **udp**: Redirect applies to UDP packets.

**source_address**
The IP address(es) form which the packet originated.
This option is used to filter all packets from a specific IP address or a group of IP addresses.
When specifying a group of addresses, the initial address is configured using this option. The range can then be configured using the `source_wildcard` parameter.

**source_wildcard**
This option is used in conjunction with the `source_address` option to specify a group of addresses for which packets are to be filtered.
The mask must be entered as a complement:
- Zero-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be identical.
- One-bits in this parameter mean that the corresponding bits configured for the `source_address` parameter must be ignored.
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>redirect</code></td>
<td>Specifies that the rule applies to all packets.</td>
</tr>
<tr>
<td><code>host</code></td>
<td>Specifies that the rule applies to a specific host as determined by its IP address.</td>
</tr>
<tr>
<td><code>source_host_address</code></td>
<td>The IP address of the source host to filter against expressed in IPv6 colon-separated-hexadecimal notation.</td>
</tr>
<tr>
<td><code>dest_host_address</code></td>
<td>The IP address of the destination host to filter against expressed in IPv6 colon-separated-hexadecimal notation.</td>
</tr>
<tr>
<td><code>eq source_port</code></td>
<td>Specifies a single, specific source TCP port number to be filtered.</td>
</tr>
<tr>
<td><code>gt source_port</code></td>
<td>Specifies that all source TCP port numbers greater than the one specified are to be filtered.</td>
</tr>
<tr>
<td><code>lt source_port</code></td>
<td>Specifies that all source TCP port numbers less than the one specified are to be filtered.</td>
</tr>
<tr>
<td><code>neq source_port</code></td>
<td>Specifies that all source TCP port numbers not equal to the one specified are to be filtered.</td>
</tr>
<tr>
<td><code>dest_address</code></td>
<td>The IP address(es) to which the packet is to be sent.</td>
</tr>
<tr>
<td><code>dest_wildcard</code></td>
<td>This option is used in conjunction with the <code>dest_address</code> option to specify a group of addresses for which packets are to be filtered.</td>
</tr>
<tr>
<td></td>
<td>The mask must be entered as a complement:</td>
</tr>
<tr>
<td></td>
<td>• Zero-bits in this parameter mean that the corresponding bits configured for the <code>dest_address</code> parameter must be identical.</td>
</tr>
<tr>
<td></td>
<td>• One-bits in this parameter mean that the corresponding bits configured for the <code>dest_address</code> parameter must be ignored.</td>
</tr>
</tbody>
</table>
**Important:** The mask must contain a contiguous set of one-bits from the least significant bit (LSB). Therefore, allowed masks are 0, 1, 3, 7, 15, 31, 63, 127, and 255. For example, acceptable wildcards are 0.0.0.3, 0.0.0.255, and 0.0.15.255. A wildcard of 0.0.7.15 is not acceptable since the one-bits are not contiguous.

---

**eq dest_port**

Specifies a single, specific destination TCP port number to be filtered. 
`dest_port` must be configured to an integer value from 0 to 65535.

**gt dest_port**

Specifies that all destination TCP port numbers greater than the one specified are to be filtered. 
`dest_port` must be configured to an integer value from 0 to 65535.

**lt dest_port**

Specifies that all destination TCP port numbers less than the one specified are to be filtered. 
`dest_port` must be configured to an integer value from 0 to 65535.

**neq dest_port**

Specifies that all destination TCP port numbers not equal to the one specified are to be filtered. 
`dest_port` must be configured to an integer value from 0 to 65535.

---

**Usage**

Block IP packets when the source and destination are of interest but for only a limited set of ports.

---

**Important:** The maximum number of rules that can be configured per ACL varies depending on how the ACL is to be used. For more information, refer to the Engineering Rules appendix in the System Administration Guide. Also note that “redirect” rules are ignored for ACLs applied to specific subscribers or all subscribers facilitated by a specific context.

---

**Example**

The following command defines a rule that redirects packets to the next hop host at `fe80::c0a8:a04`, the context with the context ID of 23, and UDP packets coming from any host are matched:

```
redirect nexthop fe80::c0a8:a04 context 23 udp any
```

The following sets the insertion point to before the rule defined above:

```
before redirect nexthop fe80::c0a8:a04 context 23 udp any
```

The following command sets the insertion point after the rule defined above:

```
after redirect nexthop fe80::c0a8:a04 context 23 udp any
```

The following command deletes the first rule defined above:

```
no redirect nexthop fe80::c0a8:a04 context 23 udp any
```
Chapter 181
IPv6 to IPv4 Tunnel Interface Configuration Mode Commands

The IPv6 to IPv4 Tunnel Interface Configuration Mode is used to create and manage the IP interface for addresses, address resolution options, etc.

Mode

Exec > Global Configuration > Context Configuration > Tunnel Interface Configuration > IPv6 to IPv4 Tunnel Interface Configuration

configure > context context_name > interface interface_name tunnel > tunnel-mode ipv6ip

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-if-tunnel-ipv6ip)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
destination address

Configures the destination of the tunneled packets for a manual tunnel.

Product
All

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > Tunnel Interface Configuration > IPv6 to IPv4 Tunnel Interface Configuration
configure > context context_name > interface interface_name tunnel > tunnel-mode ipv6ip

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-if-tunnel-ipv6ip)#

Syntax

destination address address

no destination address

no

Removes configuration for the specified keyword.

address

Specifies the IP address of the destination device. address must be specified in IPv4 dotted decimal or IPv6 colon-separated-hexadecimal notation.

Usage

Use this command to configure the IP address of the destination end of the tunnel.

Example

The following command sets the destination address for packets on this tunneled interface to 10.2.3.4:

destination address 10.2.3.4
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

exit

**Usage**

Use this command to return to the parent configuration mode.
mode

Configures the mode of IPv6 to IPv4 tunneling. The default is set to manual mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Tunnel Interface Configuration > IPv6 to IPv4 Tunnel Interface Configuration
configure > context context_name > interface interface_name tunnel > tunnel-mode ipv6ip

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-tunnel-ipv6ip)#
```

**Syntax**

```
mode { 6to4 | manual }
```

default mode

**6to4**

Configures automatic IPv6-to-IPv4 (6to4) tunnels as specified in RFC 3056.

**manual**

Configures point-to-point manual IPv6-to-IPv4 tunnels by specifying the IPv4 address of the tunnel remote end.

**default**

Resets the mode of IPv6-to-IPv4 tunneling to manual mode.

**Usage**

There can be only one IPv6-to-IPv4 tunnel possible in a context. Once an IPv6-to-IPv4 tunnel is configured, all subsequent tunnels will be configured as manual tunnels.

**Example**

The following command configures the mode to IPv6-to-IPv4 (6to4).

```
mode 6to4
```

The following command configures the mode to 6to4.

```
mode manual
```
source

Configures the source of tunneled packets.

Product
PDSN
HA

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Tunnel Interface Configuration > IPv6 to IPv4 Tunnel Interface Configuration

configure > context context_name > interface interface_name tunnel > tunnel-mode ipv6ip

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-if-tunnel-ipv6ip)#

Syntax

source { address ip_address | interface interface_name }

no source { address | interface } 

address ip_address

Specifies the IPv4 address to use as the source address of the tunnel.

ip_address must be expressed in IPv4 dotted-decimal notation.

interface interface_name

Specifies the name of a non-tunnel IPv4 interface, whose address is used as the source address of the tunnel. interface must be an alphanumeric string of 1 through 79 characters.

no source { address | interface } 

Removes configuration for the specified keyword.

Usage

Configures the source IPv4 address of the tunnel by either specifying the IP address (host address) or by specifying another configured non-tunnel IPv4 interface. The source address must be an existing interface address before it is used. State of source address will affect the operational state of the tunnel.

Example

The following command configures the source address of the tunnel.

source address 10.2.3.4

The following command specifies the source interface as testsource1.

source interface testsource1
tos

Configures the type of service (TOS) settings of the outer IPv4 header of the tunneled packets.

**Product**

PDSN

HA

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > Tunnel Interface Configuration > IPv6 to IPv4 Tunnel Interface Configuration

```
configure > context context_name > interface interface_name tunnel > tunnel-mode ipv6ip
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-tunnel-ipv6ip)#
```

**Syntax**

```
tos { copy | value tos_value }
```

**default tos**

```
copy
```

Copies the DC octet of the IPv6 packet to the TOS octet of IPv4 packet.

```
default
```

Configures default setting for the specified keyword.

```
value tos_value
```

Configures the raw TOS value ranging from 0 to 255. The default is 0.

**Usage**

Sets the TOS parameter to be used in the tunnel transport protocol or copies the TOS value from the original IPv6 DC byte to the TOS value of the encapsulating IPv4 header.

**Example**

The following command sets the tos value to 1:

```
tos value 1
```
ttl

Configures the TTL (Time to live) value of the outer IPv4 header of the tunneled packets.

**Product**

- PDSN
- HA

**Privilege**

Security Administrator, Administrator

**Mode**

- Exec > Global Configuration > Context Configuration > Tunnel Interface Configuration > IPv6 to IPv4 Tunnel Interface Configuration

```
configure > context context_name > interface interface_name tunnel > tunnel-mode ipv6ip
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-tunnel-ipv6ip)#
```

**Syntax**

```
ttl value ttl_value
```

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Configures default setting for the specified keyword.</td>
</tr>
<tr>
<td>value ttl_value</td>
<td>ttl_value is an integer from 1 through 255. The default is 16.</td>
</tr>
</tbody>
</table>

**Usage**

Configures the TTL parameter to be used in the tunnel transport protocol.

**Example**

The following command sets the TTL value to 25.

```
ttl value 25
```
Chapter 182
ISAKMP Configuration Mode Commands

The ISAKMP Configuration Mode is used to configure Internet Security Association Key Management Protocol (ISAKMP) policies that are used to define Internet Key Exchange (IKE) security associations (SAs).

Modification(s) to an existing ISAKMP policy configuration will not take effect until the related security association has been cleared. Refer to the `clear crypto security-association` command described in the Exec Mode (A–C) Commands chapter for more information.

Mode

Exec > Global Configuration > Context Configuration > ISAKMP Configuration

`configure > context context_name > isakmp policy policy_number`

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
authentication

Configures the ISAKMP policy authentication mode.

**Product**
- PDSN
- HA
- GGSN

**Privilege**
- Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > ISAKMP Configuration

`configure > context context_name > isakmp policy policy_number`

**Syntax**

```
authentication preshared-key
[ default | no ] authentication
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default authentication</td>
<td>Restores the default setting of this parameter. This command is enabled by default.</td>
</tr>
<tr>
<td>no authentication</td>
<td>Disables the preshared key authentication mode.</td>
</tr>
<tr>
<td>preshared-key</td>
<td>Specifies that the policy will be authenticated through the use of the pre-shared key.</td>
</tr>
</tbody>
</table>

**Usage**
When the system is configured to use ISAKMP-type crypto maps for establishing IPSec tunnels, this command is used to indicate that the policy will be authenticated through the use of the pre-shared key configured in the ISAKMP crypto map.

**Example**
The following command sets policy authentication mode to use a pre-shared key:

```
authentication preshared-key
```
encryption

Configures the encryption protocol to use to protect subsequent IKE SA negotiations.

**Product**

PDSN
HA
GGSN

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > ISAKMP Configuration

`configure > context context_name > isakmp policy policy_number`

**Syntax**

```
encryption { 3des-cbc | aes-cbc-128 | aes-cbc-256 | des-cbc }
[ default | no ] encryption
```

---

**default encryption**

Restores the default setting of this parameter.

**no encryption**

Removes a previously configured encryption type.

**3des-cbc**

Specifies that the encryption protocol is Triple Data Encryption Standard (3DES) in chain block (CBC) mode.

**aes-cbc-128**

Specifies that the encryption protocol is Advanced Encryption Standard (AES) in CBC mode with a 128-bit key.

**aes-cbc-256**

Specifies that the encryption protocol is Advanced Encryption Standard (AES) in CBC mode with a 256-bit key.

**des-cbc**

Specifies that the encryption protocol is DES in CBC mode. This is the default setting.

**Usage**

Once the D-H exchange between the system and the security gateway has been successfully completed, subsequent IKE SA negotiations will be protected using the protocol specified by this command.

**Example**


The following command sets the IKE encryption method to 3des-cbc:

```
encryption 3des-cbc
```
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Use this command to return to the parent configuration mode.
**group**

Configures the Oakely group (also known as the Diffie-Hellman [D-H] group) in which the D-H exchange occurs.

**Product**

PDSN
HA
GGSN

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > ISAKMP Configuration

cfgure > context context_name > isakmp policy policy_number

**Syntax**

```
group { 1 | 2 | 5 }
[ default | no ] group
```

---

**default group**

Restores the default setting of this parameter.

---

**no group**

Removes a previously configured group.

---

{ 1 | 2 | 5 }

Default: 1

Specifies the number of the Oakley group. The following groups are allowed:

- **1**: Enables Oakley Group 1 using a 768-bit modp as defined in RFC 2409.
- **2**: Enables Oakley Group 2, using a 1024-bit modp as defined in RFC 2409.
- **5**: Enables Oakley Group 5, using a 1536-bit modp as defined in RFC 3526.

---

**Usage**

Specifies the Oakley group that determine the length of the base prime numbers that are used during the key exchange process.

**Example**

The following command sets the group to 5 which specifies 1536-bit base prime numbers:

```
group 5
```
hash

Confirms the IKE hash protocol to use during IKE SA negotiations.

Product
- PDSN
- HA
- GGSN

Privilege
- Security Administrator, Administrator

Mode
- Exec > Global Configuration > Context Configuration > ISAKMP Configuration
- configure > context context_name > isakmp policy policy_number

Syntax
hash { md5 | sha1 }
[ default | no ] hash

default
Restores the default setting of this parameter.

no
Removes a previously configured hash algorithm.

md5
Specifies that the hash protocol is Message Digest 5 truncated to 96 bits.

sha1
Specifies that the hash protocol is Secure Hash Algorithm-1 truncated to 96 bits. This is the default setting for this command.

Usage
Use this command to configure the hash algorithm used during key negotiation.

Example
Set the hash algorithm to Message-Digest 5 by entering the following command:

hash md5
**lifetime**

Configures the lifetime of the IKE Security Association (SA).

**Product**
- PDSN
- HA
- GGSN

**Privilege**
- Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > ISAKMP Configuration

```bash
configure > context context_name > isakmp policy policy_number
```

**Syntax**

```bash
lifetime seconds
```

**default lifetime**

```bash
default lifetime
```

**Usage**
Use this command to set the time that an ISAKMP SA will be valid. The lifetime is negotiated with the peer and the lowest configured lifetime duration is used.

**Example**
The following command sets the SA lifetime to 100 seconds:

```bash
lifetime 100
```
Chapter 183
IuPS Service Configuration Mode Commands

The IuPS Service configuration mode is used to define properties for the IuPS service which controls the Iu-PS interface connections to Radio Network Controllers (RNCs) of the UMTS Terrestrial Radio Access Network (UTRAN).

Mode

Exec > Global Configuration > Context Configuration > IuPS Service Configuration

configure > context context_name > iups-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx-iups-service)#

⚠️ **Important**: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
**access-protocol**

This command configures the access protocol parameters for the IuPS service.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > IuPS Service Configuration

```bash
configure > context context_name > iups-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service)#
```

**Syntax**

```bash
access-protocol sccp-network sccp_net_id

no access-protocol sccp-network
```

**Usage**

Use this command to configure access protocol parameters for the current IuPS service.

**Example**

The following command specifies that the current Iu-PS service should use SCCP 1:

```bash
access-protocol sccp-network 1
```
associate

This command associates a configured DSCP marking template with this IuPS service and associated Iu interface.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > IuPS Service Configuration

```
configure > context context_name > iups-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service)#
```

**Syntax**

```
associate dscp-template downlink dscp_template_name

no associate dscp-template downlink
```

- **no**
  - Removes a previously configured association.

- **dscp_template_name**
  - Specifies a DSCP marking template that was previously configured with the commands in the DSCP Template configuration mode.
  - `dscp_template_name` - Enter an alphanumeric string of 1 to 64 characters, including dots (.), dashes (-), and forward slashes (/), to identify a unique instance of a DSCP marking template.

**Usage**

Use this command to associate a specific DSCP marking template with this IuPS service and associated Iu interface. The DSCP template provides a mechanism for differentiated services code point (DSCP) marking of control packets and signaling messages at the SGSN’s M3UA level on the Iu interface. This DSCP marking enables the SGSN to perform classifying and managing of network traffic and to determine quality of service (QoS) for the interface to the IP network.

**Example**

The following command associates a DSCP marking template named `dscptempl1` with the Iu interface:

```
associate dscp-template downlink dscptempl1
```

The following command disassociates a previously associated DSCP marking template named `template4` with this IuPS service configuration:

```
no associate dscp-template downlink
```
blacklist-timeout-gtpu-bind-addresses

This command specifies the time period that a GTP-U bind address (loopback address) will not be used (is blacklisted) in RAB-Assignment requests after a RAB assignment request, with that GTP-U bind address, has been rejected by an RNC with the cause - Unspecified Error. This is a failure at the RNC’s GTP-U IP interface.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > IuPS Service Configuration
configure > context context_name > iups-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx-iups-service)#

Syntax

blacklist-timeout-gtpu-bind-addresses seconds

default blacklist-timeout-gtpu-bind-addresses

default
Resets the blacklist time to 60 seconds.

seconds
Number of seconds that the GTP-U bind (loopback) address will not be used in a RAB-Assignment request.
seconds: Must be an integer from 1 to 1800.

Usage
Use this command to configure the blacklist period.

Example
The following command specifies a 15 minutes (460 seconds) blacklist period.

blacklist-timeout-gtpu-bind-addresses 460
empty-cr

This command allows the operator to determine how empty Connection Request messages will be handled.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > IuPS Service Configuration

configure > context context_name > iups-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx-iups-service)#

**Syntax**

empty-cr procedure reject

[ default | no ] empty-cr procedure reject

```
default | no
```

Using either `default` or `no` with the command disables the rejection function and returns the system to the default behavior, which is to ignore receipt of the empty CRs.

**Usage**

Use this command to enable/disable the procedure for handling empty (not containing dataparameters) Connection Request (CR) messages.

This feature can be used in the following scenario: During 4G to 3G handovers, some Connection Requests from mobile subscribers might be ignored by the SGSN, even though their UE would display that the WCDMA was available. The RNC would send an SCCP Connection Request (CR) over the Iu interface to the SGSN. Normally, this message contains a RANAP message and GMM, but according to 3GPP and ITU Q.713 standards, it is permissible to send an SCCP CR without any data parameters. In such a situation, normally the SGSN would ignore these SCCP CR messages, because without these data parameters the SGSN would be unable to derive the DeMux key which is the basis for determining the Session Manager instance to be used for a subscriber. Using this feature allows the SGSN to send a Reject to the mobile subscriber when an “empty” SCCP CR is sent from their UE.

Fields have been added to the output of the following CLI show commands to track the receipt and rejection of Connect Request (CR) messages:

- `show gmm-sm statistics`
- `show gmm-sm statistics verbose`

**Example**

The following command enables the empty CR handling procedure:

```
empty-cr procedure reject
```

The following command disables the empty CR handling procedure:
default empty-cr procedure reject
end

Exits the current configuration mode and returns to the Exec mode.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Return to the Exec mode.
exit

Exits the current configuration mode and returns to the previous configuration mode, the context configuration mode.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Return to the context configuration mode.
force-authenticate consecutive-security-failure

Disable/enable authentication when the MS/UE security fails and configures the procedures and frequency for authentication

Product
SGSN

Privilege
Security Administrator, Administrator, Operator

Mode
Exec > Global Configuration > Context Configuration > IuPS Service Configuration
configure > context context_name > iups-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx-iups-service)#

Syntax

force-authenticate consecutive-security-failure { inter-sgsn-rau | local-messages count frequency | non-local-messages count frequency }

[ default | no ] force-authenticate consecutive-security-failure { inter-sgsn-rau | local-messages | non-local-messages }

default

Resets the values to defaults. Forced authentication is enabled for all the types of event procedures with the default values for determining frequency for authentication.

no

Disables the specified authentication configuration.

inter-sgsn-rau

Default: enabled
Enables/disables authentication for inter-SGSN RAU.
The SGSN does not remember previous inter-SGSN-RAU failures for a P-TMSI/RAI because the SGSN clears all contexts on the occurrence of an inter-SGSN-RAU security failure. So the next inter-SGSN-RAU can only be authenticated forcefully if it comes before the previous context is cleared. This type of forced authentication is enabled by default because this type of failure is fairly common.

local-messages count frequency

Default: 5
Enables/disables authentication for local messages (such as local RAUs, Service Requests, Detach Requests, etc). Consecutive security failures is fairly rare for local messages so the default count frequency is fairly high, 5. Setting the count frequency enables the feature and sets the number of consecutive local message security failures that must occur prior to authentication being forced.

frequency: Enter an integer from 1 to 10.
**force-authenticate consecutive-security-failure**

`non-local-messages count count`

Default: 1

Enables/disables authentication for non-local messages (such as inter-RAT RAUs and all types of attaches). Consecutive security failures for non-local messages is fairly common so the default count frequency is 1. Setting the count frequency enables the feature and sets the number of consecutive non-local message security failures that must occur prior to authentication being forced.

*frequency:* Enter an integer from 1 to 10.

**Usage**

GMM authentication is optional for UMTS. When GMM authentication is skipped, the SGSN and the MS continue to re-use the latest keys exchanged during the most recent GMM authentication procedure. This can result in the SGSN and the MS going out of sync with the CK and IK currently in use. If a mismatch occurs when the MS continues to use the correct parameters (e.g., cksn or P-TMSI signature) in the next Iu and if the SGSN skips authentication on the Iu, then, usually, the security mode will timeout or be rejected because the MS will not be able to decipher or perform an integrity check on the network messages. This scenario results in a lot of useless signaling in the network. This command allows the operator to enable a forced GMM authentication that will either resolve this type of problem or avoid it. As well, the operator can configure a frequency of authentication that best meets their needs.

**Example**

The following command enables forced authentication after every 3rd local message security failure:

```
force-authenticate consecutive-security-failure local-messages count 3
```
gtpu

This command configures parameters for the GTP user (GTP-U) dataplane.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > IuPS Service Configuration

```bash
configure > context context_name > iups-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service)#
```

**Syntax**

```bash
gtpu { bind ip_addr | echo-interval seconds | max-retransmissions number | retransmission-timeout seconds | sync-echo-with-peer }
no gtpu { bind address ip_addr | echo-interval | max-retransmissions | retransmission-timeout | sync-echo-with-peer }
default gtpu { echo-interval | max-retransmissions | retransmission-timeout | sync-echo-with-peer }

```

---

**no**

Removes the configured parameter value.

---

**default**

Sets the specified parameter to its default setting.

---

**bind address ip_addr**

This command binds the specified IP address to the Iu-PS GTP-U endpoint.

*ip_addr*: Must be an IP v4 IP address in dotted decimal notation.

---

**echo-interval seconds**

Default: 60

Configures the rate, in seconds, at which GTP-U echo packets are sent to the UTRAN over the Iu-PS interface.

*seconds*: Must be an integer from 60 through 3600.

---

**max-retransmissions number**

Default: 5

Configures the maximum number of transmission retries for GTP-U packets.

*number*: Must be an integer from 0 through 15.
retransmission-timeout seconds

Default: 5
Configures the retransmission timeout for GTPU packets in seconds.
seconds: Must be an integer from 1 through 20.

sync-echo-with-peer

This keyword is applicable to the SGSN only.
This keyword enables the SGSN to synchronize path management procedures with the peer after a GTP service restart recovery.
After GTP service recovery, the SGSN restarts the timers for GTP echo transmission, hence a drift in echo request transmission time (from the pre-recovery time) can occur causing the SGSN to be out of sync with the peer. By using this keyword, when the SGSN receives the first Echo Request (GTPC or GTPU) from the peer after the GTP service restart, in addition to replying with an ECHO Response, the SGSN transmits an ECHO Request to the peer and the SGSN restarts the timers associated with the path management procedures. This causes the path management procedure at SGSN to synchronize with the peer node.
Default: Enabled

Usage

Use this command to configure GTP-U parameters for the Iu-PS interface.

Example

The following command binds the IP address 192.168.0.10 to the Iu-PS interface for communication with the UTRAN:

```
gtpu bind address 192.168.0.10
```
inter-rnc-procedures

This command enables the processing of SRNS relocation when the source RNC is behaving as the target RNC.

**Product**

SGSN

Insert product and tag this paragraph appropriately.

**Mode**

Exec > Global Configuration > Context Configuration > IuPS Service Configuration

configure > context context_name > iups-service service_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service)#
```

**Syntax**

```
[no] inter-rnc-procedures source-rnc-as-target-rnc
```

Configures the SGSN to complete SRNS relocation when the source RNC is behaving as the target RNC. For example, in the case of a Femtocell-to-Femtocell handoff - the femtocell gateway may act both as the source and target RNC to the femtocells, although from the SGSN’s perspective it is the same RNC.

```
no
```

Disables SRNS relocation when the source RNC is behaving as the target RNC. This is the default setting.

**Usage**

Use this command to enable/disable SRNS relocation when the source RNC is behaving as the target RNC.

**Example**

Enter this command to enable SRNS relocation for those scenarios where the source RNC is behaving as the target RNC:

```
inter-rnc-procedures source-rnc-as-target-rnc
```
iu-hold-connection

Defines the type and duration of the Iu hold connection.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > IuPS Service Configuration

```
configure > context context_name > iups-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service)#
```

**Syntax**

```
iu-hold-connection [ always | requested-by-ms ] [ hold-time seconds ]
default iu-hold-connection
no iu-hold-connection
```

---

**default**

 Resets the Iu hold connection parameters to requested-by-ms and 100 second duration.

---

**no**

 Removes the configuration information for the specified Iu hold connection parameter.

---

**always**

 Specifies that there is always to be an Iu hold connection procedure.

---

**requested-by-ms**

 Specifies that there is only an Iu hold connection procedure if requested by the MS/UE. This is the default setting for Iu-hold-connection.

---

**hold-time time**

 This variable configures the interval (in seconds) that the SGSN holds the Iu connection.

 | time: must be an integer from 1 to 3600. 
 | time: must be an integer from 10 to 3600.

**Important:** It is recommended to use a minimum value of “10” seconds. If a value less than “10” seconds is used, more collisions may be observed. If the minimum value of “1” is set, after a re-load, INTRA-RAU (with unknown ptmsi, old-rai known) will be released in “1” second if the Identity Rsp does not come within “1” second.

Default is 100.
Usage
Define the amount of time the Iu connection will be held open.

Example
Instruct the SGSN to hold the Iu connection open for 120 seconds

    iu-hold-connection always hold-time 120
**Important:** This command has been deprecated and is no longer available.

**Product**
SGSN

**Mode**
Exec > Global Configuration > Context Configuration > IuPS Service Configuration

```
configure > context context_name > iups-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service)#
```
**iu-release-complete-timeout**

Configures the SGSN’s timer for waiting for an Iu Release Complete message from the RNC.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > IuPS Service Configuration

```plaintext
configure > context context_name > iups-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service)#
```

**Syntax**

```plaintext
iu-release-complete-timeout time
```

**default iu-release-complete-timeout**

- **default**
  - Resets the timer to its default setting.

- **time**
  - This variable defines the amount of time (in seconds) that the SGSN waits to receive an ‘Iu Release Complete’ message from the RNC.
  - Default: 10.
  - `time`: Must be an integer from 1 to 60.

**Usage**
Configure the number of seconds that the SGSN waits to receive the Iu Release Complete message.

**Example**

Set the SGSN to wait 20 seconds for Iu-Release-Complete:

```plaintext
iu-release-complete-timeout 20
```
loss-of-radio-coverage ranap-cause

This command sets the detection cause included in the Iu Release message. This command is unique to releases 9.0 and higher.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > IuPS Service Configuration
configure > context context_name > iups-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx-iups-service)#

**Syntax**

```
loss-or-radio-coverage ranap-cause cause_number

default loss-of-radio-coverage ranap-cause
```

**Usage**

By defining a cause code, the SGSN knows to detect the LORC state of the mobile from Iu Release messages it receives for the subscriber. This configuration also instructs the SGSN to include the defined cause code for the LORC state in the IE portion of various messages sent to the GGSN and optionally the peer SGSN. This command is one of the two commands required to enable the SGSN to work with the GGSN and, optionally the peer SGSN, to implement the Overcharging Protection feature (see the SGSN Overview in the SGSN Administration Guide for feature details. The other command needed to implement the Overcharging Protection feature is the `gtp private extension` command explained in the SGSN APN Policy Configuration Mode chapter of the Command Line Interface Reference.

**Example**

Use the following command to set the cause code to indicate that there are no radio resources available in the target cell, cause 53.

```
loss-or-radio-coverage ranap-cause 53
```
mbms

This command is in development for future use so the command and keywords that you might see are not currently supported.
network-sharing cs-ps-coordination

Enables/disables the SGSN service to perform a CS-PS coordination check.

**Important:** With the release of 15.0, both 2G and 3G MOCN functionality is license controlled and the license is required to use all previously available network sharing SGSN configuration commands. For additional information, contact your Cisco Account Representative.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > IuPS Service Configuration

configure > context context_name > iups-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx-iups-service)#

**Syntax**

```plaintext
network-sharing cs-ps-coordination [ homer | roamer ]

default network-sharing cs-ps-coordination

no network-sharing cs-ps-coordination
```

**Usage**

Use this command to facilitate the network sharing functionality. With this command, the SGSN can be instructed to perform a check to determine if CS-PS coordination is needed.

3GPP TS 25.231 section 4.2.5 describes the functionality of the SGSN to handle CS-PS (circuit-switching/packet-switching) coordination for attached networks not having a Gs-interface. In compliance with the standard, the SGSN rejects an Attach in a MOCN configuration with cause 'CS-PS coordination
required', after learning the IMSI, to facilitate the RNC choosing the same operator for both CS and PS domains.

**Example**

Use the following syntax to disable the CS-PS coordination check:

```
no network-sharing cs-ps-coordination
```

Use the following command to enable the CS-PS coordination check only for UEs from outside the home network:

```
no network-sharing cs-ps-coordination roamer
```
network-sharing failure-code

Configure the reject cause code to included in network-sharing Reject messages.

Important: With the release of 15.0, both 2G and 3G MOCN functionality is now license controlled and the license is required to use all previously available network sharing SGSN configuration commands. For additional information, contact your Cisco Account Representative.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > IuPS Service Configuration
configure > context context_name > iups-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx-iups-service)#

Syntax

network-sharing failure failure_code

default network-sharing failure

default

Resets the SGSN service to use the default cause code,14 (GPRS services not allowed in this PLMN).

failure_code

Enter one of the GMM failure cause codes listed below (from section 10.5.5.14 of the 3GPP TS 124.008 v7.2.0 R7):

- 2 - IMSI unknown in HLR
- 3 - Illegal MS
- 6 - Illegal ME
- 7 - GPRS services not allowed
- 8 - GPRS services and non-GPRS services not allowed
- 9 - MSID cannot be derived by the network
- 10 - Implicitly detached
- 11 - PLMN not allowed
- 12 - Location Area not allowed
- 13 - Roaming not allowed in this location area
- 14 - GPRS services not allowed in this PLMN
- 15 - No Suitable Cells In Location Area
• 16 - MSC temporarily not reachable
• 17 - Network failure
• 20 - MAC failure
• 21 - Synch failure
• 22 - Congestion
• 23 - GSM authentication unacceptable
• 40 - No PDP context activated
• 48 to 63 - retry upon entry into a new cell
• 95 - Semantically incorrect message
• 96 - Invalid mandatory information
• 97 - Message type non-existent or not implemented
• 98 - Message type not compatible with state
• 99 - Information element non-existent or not implemented
• 100 - Conditional IE error
• 101 - Message not compatible with the protocol state
• 111 - Protocol error, unspecified

Usage

Use this command to determine which failure code will be included in Reject messages sent by the SGSN when there is a network-sharing failure.

Example

Use the following syntax to indicate that roaming is not allowed (# 13) as the cause for the network-sharing failure:

```
network-sharing failure 13
```
network-sharing non-shared

This command allows non-shared area access when network-sharing is enabled.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > IuPS Service Configuration

```
configure > context context_name > iups-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service)#
```

**Syntax**

```
network-sharing non-shared

[ default | no ] network-sharing non-shared
```

```
default

Resets the default to disable non-shared access.
```

**Usage**
When non-shared area access is enabled, the SGSN sends the selected-plmn value in Attach/RAU accept if LAI is having one of the selected-plmn and "selected-plmn" or "Redirect-attempt flag" IEs are not included in the request message.

**Example**
Disable non-shared area access if it has already been configured:

```
no network-sharing non-shared
```
plmn

Configures the PLMN (public land mobile network) related parameters for the IuPS service. This command is applicable to releases 8.1 and higher.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > IuPS Service Configuration

configure > context context_name > iups-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx-iups-service)#

Syntax

plmn id mcc mcc_num mnc mnc_num [ network-sharing common-plmn mcc mcc_num mnc mnc_num [ plmn-list mcc mcc_num mnc mnc_num [ mcc mcc_num mnc mnc_num+ ] ] ]

no plmn id

no

Removes the PLMN ID from the configuration.

id

Creates a PLMN configuration instance based on the PLMN ID (comprised of the MCC and MNC). In accordance with TS 25.413, the SGSN supports up to 32 PLMN configurations for shared networks.

mcc mcc_num

Specifies the mobile country code (MCC) portion of the PLMN’s identifier.

mcc_num: The PLMN MCC identifier and can be configured to any integer value between 100 and 999.

mnc mnc_num

Specifies the mobile network code (MNC) portion of the PLMN’s identifier.

mnc_num: The PLMN MNC identifier and can be configured to any 2-digit or 3-digit value between 00 and 999.

network-sharing common-plmn mcc mcc_num mnc mnc_num

When network sharing is employed, this set of keywords is required to define the PLMN Id of the common PLMN. The common PLMN is usually not the same as the local PLMN.

Important: With the release of 15.0, both 2G and 3G MOCN functionality is now license controlled and the license is required to use all previously available network sharing SGSN configuration commands. For additional information, contact your Cisco Account Representative.
**plmn-list mcc mcc_num mnc mnc_num**

When network sharing is employed and more than two PLMNs are available, then use the `plmn-list` keyword to begin a list of all additional PLMNs.

---

**Usage**

Use this command to configure the PLMN associated with the SGSN. There can only be one PLMN associated with an SGSN unless one of the following features is enabled and configured: network sharing or multiple PLMN.

For network sharing, use of the `network-sharing` keywords make it possible to identify more than one PLMN. Including the PLMN identified initially. None have precedence. They are all treated equally but they must each be unique. In a MOCN configuration, the PLMN list will not be used as there would only be one local PLMN.

For multiple PLMN support, the SGSN can support up to 8 Iu-PS configurations for PLMNs. These Iu-PS service configurations must be associated with the SGSN via the `ran-protocol` command in the SGSN Service configuration mode.

**Example**

Use the following command to identify a PLMN by the MCC 313 and MNC 23 and instruct the SGSN to perform network sharing with a single common PLMN identified by MCC 404 and MNC 123:

```
plmn id mcc 313 mnc 23 network-sharing common-plmn mcc 404 mnc 123
```
rab-assignment-response-timeout

Configures the RAB assignment timer.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > IuPS Service Configuration

Syntax

rab-assignment-response-timeout time

default rab-assignment-response-timeout

default
Resets the timer to its default setting.

time
This variable configures the amount of time (in seconds) that the SGSN waits to receive a RAB assignment from the RNC.
time: must be an integer from 1 to 60.
Default: 8.

Usage
This command defines time the SGSN waits for the completion of the RAB assignment procedure.

Example
Change the timer setting to 11 seconds.

rab-assignment-response-timeout 11
radio-network-controller

This command creates an instance of an RNC configuration to associate with the IuPS service for the SGSN. This command is only available in release 8.0; use the rnc command for releases 8.1 and higher.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > IuPS Service Configuration

configure > context context_name > iups-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx-iups-service)#

Syntax

radio-network-controller id rnc_id mcc mcc_num mnc mnc_num

no radio-network-controller id rnc_id mcc mcc_num mnc mnc_num

no

Removes the configuration information for the specified RNC.

id rnc_id

Define the instance number of the RNC configuration.

rnc_id: Must be an integer from 0 to 4095.

mcc mcc_num

Specifies the mobile country code (MCC).

mcc_num: Must be an integer between 100 and 999.

mnc mnc_num

Specifies the mobile network code (MNC).

mnc_num: Must be an integer between 00 and 999.

Usage

Use this command to configure information for the IuPS service to use to contact specific RNCs. This command also provides access to the RNC configuration mode.

Example

The following command creates or accesses RNC configuration instance #1 with MCC of 131 and MNC of 22:

radio-network-controller id 1 mcc 131 mnc 22
relocation.alloc.timeout

This command defines the amount of time the SGSN waits for a Relocation Request message.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > IuPS Service Configuration
configure > context context_name > iups-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx-iups-service)#

Syntax

relocation.alloc.timeout  timeout_value

default relocation.alloc.timeout

<table>
<thead>
<tr>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resets the configuration to a 5 second wait time.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>timeout_value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time in seconds that the SGSN waits to receive a Relocation Request message.</td>
</tr>
<tr>
<td>timeout_value: Must be an integer from 1 to 60.</td>
</tr>
<tr>
<td>Default: 5 seconds.</td>
</tr>
</tbody>
</table>

Usage

Use this command to configure the number of seconds the SGSN will wait for a Relocation Request message to be received. This timeout needs to be set with sufficient time so that SRNS procedure aborts can be avoided if the peer fails to respond in a timely fashion in the case of a hard handoff.

Example

The following command sets the wait time to 10 seconds.

relocation.alloc.timeout 10
relocation-complete-timeout

This command specifies the maximum time for the SGSN to wait for a Relocation Completion from the core network.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > IuPS Service Configuration

```
configure > context context_name > iups-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service)#
```

**Syntax**

```
relocation-complete-timeout timeout_value
```

```
default relocation-complete-timeout
```

```
default
  Resets the configuration to a 5 second wait time.
```

```
timeout_value
  Time in seconds that the SGSN waits for relocation to be completed.
  timeout_value: Must be an integer from 1 to 60.
  Default: 5 seconds.
```

**Usage**

Use this command to configure the number of seconds the SGSN will wait for a relocation to be completed. This timeout needs to be set with sufficient time so that SRNS procedure aborts can be avoided if the peer fails to respond in a timely fashion in the case of a hard handoff.

**Example**

The following command sets the wait time for 10 seconds.

```
relocation-complete-timeout 10
```
reset

Defines the configuration specific to the RESET procedure.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > IuPS Service Configuration

```
configure > context context_name > iups-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service)#
```

**Syntax**

```
reset { ack-timeout time | guard-timeout time | max-retransmissions retries | sgsn-initiated }
```

```
default reset { ack-timeout | guard-timeout | max-retransmissions | sgsn-initiated }
```

```
no reset sgsn-initiated
```

---

**default**

Returns to the default settings for the Reset procedure.

**no**

Removes the SGSN-initiated reset procedure from the configuration.

**ack-timeout** *time*

Configures the interval (in seconds) for which the SGSN waits for RESET-ACK from the RNC.

*time* must be an integer from 5 to 60.
Default: 20.

**guard-timeout**

Configures the interval (in seconds) after which the SGSN sends RESET-ACK to the RNC.

*time* must be an integer from 5 to 60.
Default: 10

**max-retransmissions**

Configures maximum retries for RESET message.

*retries* must be an integer from 0 to 2.
Default: 1.

**sgsn-initiated**

Enables SGSN initiated RESET procedure.
Default: disabled.

Usage

Configures the parameters that determine a RESET.

Example

Use the following to have the SGSN initiate the RESET procedure:

```
reset sgsn-initiated
```
**rnc**

This command creates or accesses an instance of an RNC (radio network controller) configuration.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > IuPS Service Configuration

configure > context context_name > iups-service service_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service)#
```

**Syntax**

- **rnc id rnc_id**
- **no rnc id rnc_id**

**Usage**

Use this command to configure information for the IuPS service to use to contact specific RNCs. This command also provides access to the RNC configuration mode.

**Example**

The following command creates an RNC configuration instance 3442:

```
rnc id 3442
```
security-mode-complete-timeout

This command configures the security mode timer.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > IuPS Service Configuration

`configure > context context_name > iups-service service_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service)#
```

**Syntax**

```
security-mode-complete-timeout time

default security-mode-complete-timeout
```

- **default**

  Resets the timer configuration to the default settings.

- **time**

  Configures the interval (in seconds) the SGSN waits for the security mode from the MS to complete.
  
  *time* must be an integer from 1 to 60.
  
  Default is 5

**Usage**

Use this command to configure the timer that determines how long the SGSN waits for a Security Mode Complete message from the MS (mobile station).

**Example**

Instruct the SGSN to wait 7 seconds:

```
security-mode-complete-timeout 7
```
service-request-follow-on

Instructs the SGSN not to release an Iu immediately.

Product
SGSN

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > IuPS Service Configuration
configure > context context_name > iups-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx-iups-service)#

Syntax

[ default | no ] service-request-follow-on

---

**default**

Resets the configuration to the default, this function is enabled.

---

**no**

Disables this function so that Iu is released without waiting for the Iu-Hold-Timer to expire.

---

Usage

For an Iu established as the result of a Service Request (signaling), the SGSN, by default, waits for the Iu-Hold-Timer to expire.

Use this command with the ‘no’ prefix to disable this function.

Use this command with the ‘default’ prefix or without any prefix if the configuration was modified previously with by no service-request-follow-on.

Example

Disable this function to wait for the Iu-Hold-Timer to expire:

no service-request-follow-on

Enable this function if it was previously disabled:

service-request-follow-on
srns-context-response-timeout

This command configures the SGSN context response timer.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > IuPS Service Configuration

configure > context context_name > iups-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx-iups-service)#

Syntax

srns-context-response-timeout time

default srns-context-response-timeout

<table>
<thead>
<tr>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resets the timer configuration to the default setting.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configures the interval (in seconds) for which the SGSN waits for an SRNS Context Request message.</td>
</tr>
</tbody>
</table>

| time must be an integer from 1 to 60. |
| Default: 5. |

Usage

Configures the time to wait before the SGSN sends a response to the SRNS Context-Request message.

Example

Configure the SGSN to wait 7 seconds for an SRNS Context-Request response:

srns-context-response-timeout 7
tigoc-timeout

This command configures the TigOc interval.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > IuPS Service Configuration

configure > context context_name > iups-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx-iups-service)#

Syntax

tigoc-timeout time
default tigoc-timeout

default

Resets the timer configuration to the default setting.

time

This command sets the time in seconds.

time: Must be an integer from 1 to 60.
Default: 5.

Usage

Define the amount of time that the SGSN ignores any overload messages for TigOc interval after receiving one overload message from the RNC.

Example

Use the following command to change the default TigOc interval to 4 seconds:

tigoc-timeout 4
tintc-timeout

This command configures the TinTc interval..

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > IuPS Service Configuration

configure > context context_name > iups-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx-iups-service)#

Syntax

tintc-timeout time

default tintc-timeout

default

Resets the timer configuration to the default setting.

time

Set the number of seconds to wait.

time: Must be an integer from 1 to 60.
Default: 30.

Usage

Define 4 as the number of seconds that the SGSN waits before decrementing (by one) the traffic level of the RNC.

Example

tintc-timeout 4
Chapter 184
LAC Service Configuration Mode Commands

The LAC Service Configuration Mode is used to create and manage L2TP services within contexts on the system. L2TP Access Concentrator (LAC) services facilitate tunneling to peer L2TP Network Servers (LNSs).

Mode

Exec > Global Configuration > Context Configuration > LAC Service Configuration

configure > context context_name > lac-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-lac-service)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
allow

This command configure the system to allow different attributes in the LAC Hostname Attribute Value Pair (AVP) and Called-Number AVP for L2TP messages exchanged between LAC and LNS.

Product
GGSN
PDSN
P-GW
SAEGW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > LAC Service Configuration
configure > context context_name > lac-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-lac-service)#

Syntax

allow { aaa-assigned-hostname | called-number value apn | calling-number value imsi }

default allow { aaa-assigned-hostname | called-number value apn }

no allow { aaa-assigned-hostname | called-number value apn | calling-number }

no

Disable the configured attribute and returns to the behavior that uses the LAC-Service name as the HostName AVP.

aaa-assigned-hostname

When enabled if AAA assigns a valid Tunnel-Client-Auth-ID attribute for the tunnel, it is used as the HostName AVP in the L2TP tunnel setup message.
This keyword works in conjunction with the local-hostname hostname keyword applied via the tunnel l2tp command in APN Configuration mode.
When Tunnel parameters are not received from the RADIUS Server, Tunnel parameters configured in an APN are considered for the LNS peer selection. When APN configuration is selected, the local-hostname configured with the tunnel l2tp command in the APN for the LNS peer will be used as an LAC Hostname.

called-number value apn

Configures the system to send the APN name in the Called-Number AVP as a part of ICRQ message sent to the LNS. If this keyword is not configured, Called-Number AVP will not be included in ICRQ message sent to the LNS.
allow calling-number value imsi  

Configures the system to allow the IMSI to be used as Calling-Number as a part of ICRQ message sent to the LNS. If this keyword is not configured, then MSISDN will be used as Calling-Number.

**Important:** This is a customer-specific keyword available for PDSN. Please contact your local Cisco sales representative for more information.

**Usage**

Use this command to configure the attribute for the HostName AVP for L2TP messages exchanged between LAC and LNS. LAC Hostname will be different for the subscribers corresponding to the different corporate APNs. In the absence of a AAA assigned HostName, the LAC-Service name is used as HostName. By default the LAC-Service name is used as the HostName AVP.

**Example**

The following command enables the use of the value of Tunnel-Client-Auth-ID attribute for the HostName AVP:

```
allow aaa-assigned-hostname
```

Use the following command to reset the behavior so that the LAC-Service uses the LAC-Service name as the HostName AVP:

```
no allow aaa-assigned-hostname
```
bind

This command assigns a local end point address to the LAC service in the current context.

Product
GGSN
PDSN
P-GW
SAEGW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > LAC Service Configuration
configure > context context_name > lac-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-lac-service)#

Syntax
bind ip_address [ max-subscribers ]
no bind ip_address

Usage
Use this command to bind a local end point IP address to the LAC service.

Example
The following command binds the local end point IP address 10.10.10.100 to the LAC service in the current context:

    bind 10.10.10.100

The following command removes the binding of the local end point to the LAC service:

    no bind
**data sequence-number**

Enables data sequence numbering for sessions that use the current LAC service. Data sequence numbering is enabled by default.

**Product**
- GGSN
- PDSN
- P-GW
- SAEGW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > LAC Service Configuration

`configure > context context_name > lac-service service_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-lac-service)#
```

**Syntax**

```
[ no ] data sequence-number
```

- **no**
  Disables data sequence numbering for sessions.

**Usage**

An L2TP data packet header has an optional data sequence numbers field. The data sequence number may be used to ensure ordered delivery of data packets. This command is used to re-enable or disable the use of the data sequence numbers for data packets.

**Example**

Use the following command to disable the use of data sequence numbering:

```
no data sequence-number
```

Use the following command to re-enable data sequence numbering:

```
data sequence-number
```
**default**

This command sets the specified LAC service parameter to its default value or setting.

**Product**

- GGSN
- PDSN
- P-GW
- SAEGW

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > LAC Service Configuration

```
configure > context context_name > lac-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-lac-service)#
```

**Syntax**

```
default { data sequence-number | hide-attributes | keepalive-interval | load-balancing | local-receive-window | max-retransmission | max-session-per-tunnel | max-tunnel-challenge-length | max-tunnels | proxy-lcp-authentication | retransmission-timeout-first | retransmission-timeout-max | trap all | tunnel-authentication }
```

---

**data sequence-number**

Enables data sequence numbering for sessions.

**hide-attributes**

Disables hiding attributes in control messages sent from the LAC to the LNS.

**keepalive-interval**

Sets the interval for send L2TP Hello keepalive if there is no control or data transactions to the default value of 60 seconds.

**load-balancing**

Sets the load balancing algorithm to be used when many LNS peers have been configured to the default of round robin.

**local-receive-window**

Sets the window size to be used for the local side for the reliable control transport to the default of 16.

**max-retransmission**

Sets the maximum number of retransmissions to the default of 5.
max-session-per-tunnel
Sets the maximum number of sessions per tunnel at any point in time to the default of 512.

max-tunnel-challenge-length
Sets the maximum length of the tunnel challenge to the default of 16 bytes.

max-tunnels
Sets the maximum number of tunnels for this service to the default of 32000.

proxy-lcp-authentication
Sets sending of proxy LCP authentication parameters to the LNS to the default state of enabled.

retransmission-timeout-first
Sets the first retransmit interval to the default of 1 second.

retransmission-timeout-max
Sets the maximum retransmit interval to the default of 8 seconds.

tunnel-authentication
Sets tunnel authentication to the default state of enabled.

Usage
Use the default command to set LAC service parameters to their default states.

Example
Use the following command to set the keep alive interval to the default value of 60 seconds:

    default
    keepalive-interval

Use the following command to set the maximum number of sessions per tunnel to the default value of 512:

    default max-session-per-tunnel
**end**

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
end

**Usage**
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Use this command to return to the parent configuration mode.
hide-attributes

Enables hiding certain attributes (such as proxy-auth-name and proxy-auth-rsp) in control messages sent from the LAC to the LNS. The LAC hides such attributes only if tunnel authentication is enabled between the LAC and the LNS.

**Product**
- GGSN
- PDSN
- P-GW
- SAEGW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > LAC Service Configuration

```
configure > context context_name > lac-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-lac-service)#
```

**Syntax**
```
[ no ] hide-attributes
```  

```
no
```

Disable hiding attributes.

**Usage**
Use this command to hide certain attributes from control messages when tunnel authentication is enabled between the LAC and the LNS.

**Example**
The following command enables hiding attributes:

```
hide-attributes
```
keepalive-interval

This command specifies the amount of time to wait before sending a Hello keep alive message.

Product
GGSN
PDSN
P-GW
SAEGW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > LAC Service Configuration
configure > context context_name > lac-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-lac-service)#

Usage
Use this command to set the amount of time to wait before sending a Hello keep alive message or disable the generation of Hello keep alive messages completely. A keepalive mechanism is employed by L2TP in order to differentiate tunnel outages from extended periods of no control or data activity on a tunnel. This is accomplished by injecting Hello control messages after a specified period of time has elapsed since the last data or control message was received on a tunnel. As for any other control message, if the Hello message is not reliably delivered then the tunnel is declared down and is reset. The transport reset mechanism along with the injection of Hello messages ensures that a connectivity failure between the LNS and the LAC is detected at both ends of a tunnel.

Example
Use the following command to set the Hello keepalive message interval to 120 seconds:

    keepalive-interval 120

Use the following command to disable the generation of Hello keepalive messages:

    no keepalive-interval
no keepalive-interval
load-balancing

Configures how LNSs are selected for this LAC service.

Product
GGSN
PDSN
P-GW
SAEGW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > LAC Service Configuration
configure > context context_name > lac-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-lac-service)#

Syntax

load-balancing { balanced | prioritized | random }

<table>
<thead>
<tr>
<th>balanced</th>
</tr>
</thead>
<tbody>
<tr>
<td>LNS selection is made without regard to prioritization, but in a sequential order that balances the load across the total number of LNS nodes available.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>prioritized</th>
</tr>
</thead>
<tbody>
<tr>
<td>LNS selection is made based on the priority assigned in the Tunnel-Preference attribute. An example of this method is three LNS nodes, with preferences of 1, 2, and 3 respectively. In this example, the RADIUS server always tries the tunnel with a preference of 1 before using any of the other LNS nodes.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>random</th>
</tr>
</thead>
</table>
| Default: Enabled
LNS selection is random in order, wherein the RADIUS server does not use the Tunnel-Preference attribute in determining which LNS to select. |

Usage
Use this command to configure the load-balancing algorithm that defines how the LNS node is selected by the LAC when there are multiple peer LNSs configured in the LAC service.

Example
The following command sets the LAC service to connect to LNSs in a sequential order;

load-balancing balanced

The following command sets the LAC service to connect to LNSs according to the priority assigned through the Tunnel-Preference attribute:
load-balancing prioritized
local-receive-window

Specifies the number of control messages the remote peer LNS can send before waiting for an acknowledgement.

Product
GGSN
PDSN
P-GW
SAEGW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > LAC Service Configuration

configure > context context_name > lac-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-lac-service)#

Syntax

local-receive-window integer

integer
Default: 4
Specifies the number of control messages to send before waiting for an acknowledgement. The number can be configured to an integer from 1 to 256.

Usage
Use this command to set the size of the control message receive window being offered to the remote peer LNS. The remote peer LNS may send the specified number of control messages before it must wait for an acknowledgment.

Example
The following command sets the local receive window to 10 control messages:

local-receive-window 10
max-retransmission

Sets the maximum number of retransmissions of a control message to a peer before the tunnel and all sessions within it are cleared.

**Product**
- GGSN
- PDSN
- P-GW
- SAEGW

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration > Context Configuration > LAC Service Configuration

```
configure > context context_name > lac-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name] host_name(config-lac-service)#
```

**Syntax**

```
max-retransmission integer
```

- **integer**
  - Default: 5
  - Specifies the maximum number of retransmissions of a control message to a peer. This value must be an integer from 1 through 10.

**Usage**

Each tunnel maintains a queue of control messages to be transmitted to its peer. After a period of time passes without acknowledgement, a message is retransmitted. Each subsequent retransmission of a message employs an exponential backoff interval. For example; if the first retransmission occurs after 1 second, the next retransmission occurs after 2 seconds has elapsed, then the next after 4 seconds. If no peer response is detected after the number of retransmissions set by this command, the tunnel and all sessions within are cleared.

Use this command to set the maximum number of retransmissions that the LAC service sends before closing the tunnel and all sessions within it.

**Example**

The following command sets the maximum number of retransmissions of a control message to a peer to 7:

```
max-retransmissions 7
```
max-session-per-tunnel

Sets the maximum number of sessions that can be facilitated by a single a tunnel at any time.

**Product**
- GGSN
- PDSN
- P-GW
- SAEGW

**Privilege**
- Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > LAC Service Configuration
configure > context context_name > lac-service service_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-lac-service)#
```

**Syntax**

```
max-sessions-per-tunnel integer
```

<table>
<thead>
<tr>
<th>integer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default: 512</td>
</tr>
<tr>
<td>The maximum number of sessions expressed as an integer from 1 through 65535.</td>
</tr>
</tbody>
</table>

**Usage**
Use this command to set the maximum number of sessions you want to allow in a tunnel.

**Example**
The following command sets the maximum number of sessions in a tunnel to 5000:

```
max-sessions-per-tunnel 5000
```
max-tunnel-challenge-length

Sets the maximum length of the tunnel challenge in bytes. The challenge is used for tunnel authentication purposes during tunnel creation.

**Product**

GGSN
PDSN
P-GW
SAEGW

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > LAC Service Configuration

```bash
configure > context context_name > lac-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name] host_name(config-lac-service)#
```

**Syntax**

```
max-tunnel-challenge-length bytes
```

- `bytes`

  Default: 16

  Specifies the maximum length (in bytes of the tunnel challenge. This must be an integer from 4 through 32.

**Usage**

Use this command to set the maximum length (in bytes) for the tunnel challenge that is used during tunnel creation.

**Example**

The following command sets the maximum length of the tunnel challenge to 32 bytes:

```
max-tunnel-challenge-length 32
```
max-tunnels

The maximum number of tunnels that the current LAC service can support.

**Product**
- GGSN
- PDSN
- P-GW
- SAEGW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > LAC Service Configuration

```config
configure > context context_name > lac-service service_name
```

Entering the above command sequence results in the following prompt:

```config
[context_name]host_name(config-lac-service)>
```

**Syntax**

```
max-tunnels integer
```

integer
Default: 32000
The maximum number of tunnels expressed as an integer from 1 through 32000.

**Usage**
Use this command to set the maximum number tunnels that this LAC service can support at any on time.

**Example**
Use the following command to set the maximum number of tunnels for the current LAC service to 20000:

```
max-tunnels 20000
```
peer-lns

Adds a peer LNS address for the current LAC service. Up to eight peer LNSs can be configured for each LAC service.

**Product**

GGSN  
PDSN  
P-GW  
SAEGW

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > LAC Service Configuration  
`configure > context context_name > lac-service service_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-lac-service)#
```

**Syntax**

```
peer-lns ip_address [ encrypted ] secret secret [ crypto-map map_name { [ encrypted ] isakmp-secret secret } ] [ description text ] [ preference integer ]
```

```
no peer-lns ip_address
```

**Description**

```
no peer-lns ip_address
```

Deletes the peer LNS at the IP address specified by `ip_address`. **ip_address** must be entered in IPv4 dotted-decimal notation.

```
ip_address
```

The IP address of the peer LNS for the current LAC service. **ip_address** must be entered in IPv4 dotted-decimal notation.

```
[ encrypted ] secret secret
```

Designates the secret which is shared between the current LAC service and the peer LNS. **secret** must be an alphanumeric string of 1 through 256 characters that is case sensitive.

**encrypted secret secret**: Specifies that encryption should be used when communicating the secret with the peer LNS.

```
crypto-map map_name { [ encrypted ] isakmp-secret secret }
```

**map_name** is the name of a crypto map that has been configured in the current context. **map_name** must be an alphanumeric string of 1 through 127 characters that is case sensitive.

**isakmp-secret secret**: The pre-shared key for IKE. **secret** must be an alphanumeric string of 1 through 127 characters that is case sensitive.

**encrypted isakmp-secret secret**: The pre-shared key for IKE. Encryption must be used when sending the key. **secret** must be an alphanumeric string of 1 through 127 characters.
description text

Specifies the descriptive text to use to describe the specified peer LNS. text must be an alphanumeric string of 0 through 79 characters.

preference integer

This sets the priority of the peer LNS if multiple peer LNSs are configured. integer must be an integer from 1 through 128.

Usage

Use this command to add a peer LNS address for the current LAC service.

Example

The following command adds a peer LNS to the current LAC service with the IP address of 10.10.10.100, sets encryption on, specifies the shared secret to be 1b34nnf5d, and sets the preference to 3:

```
peer-lns 10.10.10.100 encrypted secret 1b34nnf5d preference 3
```

The following command removes the peer LNS with the IP address of 10.10.10.200 for the current LAC service:

```
no peer-lns 10.10.10.200
```
proxy-lcp-authentication

Enables and disables the sending of proxy LCP authentication parameters to the LNS.

**Product**
- GGSN
- PDSN
- P-GW
- SAEGW

**Privilege**
- Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > LAC Service Configuration
configure > context context_name > lac-service service_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-lac-service)#
```

**Syntax**

```
[ no ] proxy-lcp-authentication
```

- **no**
  - Disables the sending of proxy LCP authentication parameters to the LNS.

- **proxy-lcp-authentication**
  - Default: Enabled
  - Enables the sending of proxy LCP authentication parameters to the LNS.

**Usage**

Use this feature in situations where the peer LNS does not understand the proxy LCP Auth AVPs that the system sends and does not do an LCP renegotiation and tears down the call.

**Example**

Use the following command to disable the sending of proxy LCP authentication parameters to the LNS:

```
no proxy-lcp-authentication
```

Use the following command to re-enable the sending of proxy LCP authentication parameters to the LNS:

```
proxy-lcp-authentication
```
retransmission-timeout-first

Each tunnel maintains a queue of control messages to transmit to its peer. After a period of time passes without acknowledgement, a message is retransmitted. This command sets the initial timeout for retransmission of control messages.

Product
- GGSN
- PDSN
- P-GW
- SAEGW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > LAC Service Configuration
configure > context context_name > lac-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-lac-service)#

Syntax

retransmission-timeout-first integer

integer
Default: 1
The amount of time to wait (in seconds) before sending the first control message retransmission. This must be an integer from 1 through 100.

Usage
Use this command to set the initial timeout before retransmitting control messages to the peer.

Example
The following command sets the initial retransmission timeout to 3 seconds:

retransmission-timeout-first 3
retransmission-timeout-max

Configures maximum amount of time between two retransmission of control messages.

**Product**
- GGSN
- PDSN
- P-GW
- SAEGW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > LAC Service Configuration

```
configure > context context_name > lac-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-lac-service)#
```

**Syntax**

```
retransmission-timeout-max integer
```

- `integer`
- Default: 8
- `integer` is the maximum time (in seconds) to wait before retransmitting control messages expressed as an integer from 1 through 100.

**Usage**

Use this command to set the maximum amount of time that can elapse before retransmitting control messages.

Each tunnel maintains a queue of control messages to transmit to its peer. After a period of time passes without acknowledgement, a message is retransmitted. Each subsequent retransmission of a message employs an exponential backoff interval.

**Example**

The following command sets the maximum retransmission time-out to 10 seconds:

```
retransmission-timeout-max 10
```
**single-port-mode**

This command enables/disables the L2TP LAC service always to use standard L2TP port 1701 as source port for all L2TP control and data packets originated from LAC node.

**Product**

GGSN
PDSN
P-GW
SAEGW

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > LAC Service Configuration

`configure > context context_name > lac-service service_name`

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-lac-service)#`

**Syntax**

```
[ default | no ] single-port-mode
```

- **default**
  
  Default: Enabled
  
  Sets this command to its default state of disabled. By default single source port configuration for L2TP LAC packets is disabled.

- **no**
  
  Disables the configured single source port configuration from this LAC service.

**Usage**

Use this command to enable or disable the single port mode for L2TP LAC service.

If this feature is enabled, then L2TP LAC service will always use standard L2TP port 1701 as source port for all L2TP control/data packets originated from LAC (instead of the default scheme in which each L2TPMgr uses a dynamic source port). L2TPMgr instance 1 will handle all L2TP calls for the service.

⚠️ **Caution:** Changing this configuration, while the service is already running, will cause restart of the service.

**Example**

The following command enables the LAC service to use port 1701 as source port for all L2TP control and data packets:

```
single-port-mode
```
snoop framed-ip-address

When enabled, this feature allows the LAC to detect IP Control Protocol (IPCP) packets exchanged between the mobile node and the LNS and extract the framed-ip-address assigned to the mobile node. The address will be reported in accounting start/stop messages and displayed for subscriber sessions.

Product
GGSN
PDSN
P-GW
SAEGW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > LAC Service Configuration

configure > context context_name > lac-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-lac-service)#

Syntax

[ default | no ] snoop framed-ip-address

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Disabled.</td>
</tr>
<tr>
<td>no</td>
<td>Disables the feature. Accounting start/stop will occur before the PPP session is established and the framed IP address field will be reported as 0.0.0.0.</td>
</tr>
</tbody>
</table>

Usage

This feature is available to address simple IP roaming scenarios. If this feature is enabled, the Accounting Start will be sent only after the framed-ip-address is detected. If the framed-ip-address is not detected within 16 seconds, an Accounting Start will be sent for the session with the 0.0.0.0 address. If the session is disconnected during the detection attempt, Accounting Start/Stop will be sent for the session. If the session renegotiates IPCP, an Accounting Stop will be generated with a framed-ip-address from the old session, and an Accounting Start will be generated with an IP address for the new session. IPv6 address detection is not supported.

**Important:** When this feature is enabled and the show subscribers all command is invoked, the framed-IP-address is displayed for the PDSN Simple IP subscriber in the output display.
trap

This command generates SNMP traps.

**Product**
- GGSN
- PDSN
- P-GW
- SAEGW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > LAC Service Configuration

```bash
configure > context context_name > lac-service service_name
```

Entering the above command sequence results in the following prompt:

```bash
[context_name]host_name(config-lac-service)#
```

**Syntax**

```
[ no ] trap all
```

- `no`

Disables SNMP traps.

**Usage**

Use this command to enable/disable all supported SNMP traps.

**Example**

To enable all supported SNMP traps, enter the following command:

```
trap all
```
tunnel selection-key

Enables the creation of tunnels between an L2TP service and an LNS server on the basis of a key received from AAA server.

**Product**
- GGSN
- P-GW
- SAEGW

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration > Context Configuration > LAC Service Configuration
  - `configure > context context_name > lac-service service_name`
  - Entering the above command sequence results in the following prompt:
    
    `[context_name]host_name(config-lac-service)#`

**Syntax**

```
tunnel selection-key { none | tunnel-client-auth-id | tunnel-server-auth-id }
```

**default tunnel selection-key**

```
default
```

**default**

Disables the creation of tunnel between LAC service and LNS based on a key value received from AAA server.

```
none
```

**none**

Default: Enabled

This keyword disables the creation of multiple tunnels between a pair of LAC service and LNS server. LAC will not make use of the key to choose a tunnel with LNS in this setup.

```
tunnel-client-auth-id
```

**tunnel-client-auth-id**

Default: Disabled

This keyword enables the creation of tunnels between LAC service and an LNS server on the basis of domain attribute “Tunnel-Client-Auth-ID” value received from AAA server.

```
tunnel-server-auth-id
```

**tunnel-server-auth-id**

Default: Disabled

This keyword enables the creation of tunnels between LAC service and an LNS server on the basis of domain attribute “Tunnel-Server-Auth-ID” value received from AAA server.

**Usage**

Use this command to enable or disable the creation of additional L2TP tunnels between LAC service and LNS server on the basis of “Tunnel-Client-Auth-ID” or “Tunnel-Server-Auth-ID” attribute value received
from AAA Server in Access-Accept message. This value of attribute is treated as a key for tunnel selection and creation.

When the LAC needs to establish a new L2TP session, it first checks for an existing L2TP tunnel with the peer LNS based on the value of the key configured. If no such tunnel exists for the key, it will create a new tunnel with the LNS.

The default configuration has the selection-key as none. Hence, LAC will not make use of key to choose a tunnel with LNS in default setup.

The maximum number of sessions, as configured via the max-sessions-per-tunnel command, is applicable for each tunnel created through this command. By default, each tunnel supports 512 sessions.

If the LAC service needs to establish a new tunnel for a new L2TP session with LNS and the tunnel create request fails because maximum tunnel creation limit is reached, LAC will try other LNS addresses received from AAA server in Access-Accept message for the APN/subscriber. If all available peer-LNS are exhausted, LAC service will reject the call.

**Example**

The following command enables the use of “Tunnel-Server-Auth-ID” attribute value received from AAA Server in Access-Accept message as a key for tunnel selection and creation:

```
tunnel selection-key tunnel-server-auth-id
```
**tunnel-authentication**

Enables tunnel authentication. When tunnel authentication is enabled, a configured shared secret is used to ensure that the LAC service is communicating with an authorized peer LNS. The shared secret is configured by the `peer-lns` command in the LAC Service Configuration mode, the `tunnel l2tp` command in the Subscriber Configuration mode, or the **Tunnel-Password** attribute in the subscribers RADIUS profile.

**Product**
- GGSN
- PDSN
- P-GW
- SAEGW

**Privilege**
- Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > LAC Service Configuration
configure > context context_name > lac-service service_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-lac-service)#
```

**Syntax**

```
[ no ] tunnel-authentication
```

**Usage**

Disable or enable the usage of secrets to authenticate a peer LNS when setting up a tunnel.

**Example**

To disable tunnel authentication, use the following command:

```
no tunnel-authentication
```

To re-enable tunnel authentication, use the following command:

```
tunnel-authentication
```
Chapter 185
Line Configuration Mode Commands

The Line Configuration Mode is used to manage the terminal line characteristics for output formatting.

Mode

Exec > Global Configuration > Line Configuration
configure > line

Entering the above command sequence results in the following prompt:

[local]host_name(config-line)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
default

Restores the default length or width for the output to the display terminal.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Line Configuration
configure > line
Entering the above command sequence results in the following prompt:

[local]host_name(config-line)#

Syntax

default { length | width }

length | width
length: restores the default value for the number of rows (length) of the output for display.
width: restores the default value for the number of columns (width) of the output for display as the number of characters.

Usage
Reset the output display properties if they had been changed during a session.

Example

default length
default width
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

end

Usage
Use this command to return to the Exec mode.
**exit**

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Use this command to return to the parent configuration mode.
length

Configures the output for the display's length (number of rows).

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Line Configuration

configure > line

Entering the above command sequence results in the following prompt:

[local] host_name(config-line) #

Syntax

length number

number

Specifies the number of rows (lines) of output that can be displayed at one time for the display (output) terminal. number must be 0 or an integer from 5 through 512, where the special value 0 implies an infinite number of rows.

Usage

Set the current session's display terminal has different display characteristics than the defaults. The special infinite value (0) is typically used when logging the output of a session from a remote machine since this will result in no pagination of output.

Example

The following commands set the length of the display to infinite and 33, respectively.

length 0

length 33
**width**

Configures the output for the displays width (number of columns/characters wide).

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Line Configuration

```
configure > line
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-line)#
```

**Syntax**

```
width number
```

*number*

Specifies the number of columns (characters) of output that can be displayed at one time for the display (output) terminal. *number* must be an integer from 5 through 512.

**Usage**

Set the current session’s display terminal has different display characteristics than the defaults.

**Example**

```
width 160
```
Chapter 186
Link Configuration Mode Commands

The Link configuration mode defines the MTP3 link parameters for a specific link in a linkset of an SS7 routing domain instance.

**Mode**

Exec > Global Configuration > SS7 Routing Domain Configuration > Linkset Configuration > Link Configuration

configure > ss7-routing-domain domain_id variant var_type > linkset id linkset_id > link id link_id

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ss7-rd-linkset-linkset_id-link-link_id)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
arbitration

This command configures link arbitration.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > SS7 Routing Domain Configuration > Linkset Configuration > Link Configuration

configure > ss7-routing-domain domain_id variant var_type > linkset id linkset_id > link id link_id

Entering the above command sequence results in the following prompt:

[local]host_name(config-ss7-rd-linkset-linkset_id-link-link_id)#

Syntax

arbitration { active | passive }

no arbitration

Syntax Table

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>arbitration { active</td>
<td>passive }</td>
</tr>
<tr>
<td>no arbitration</td>
<td>Removes the arbitration configuration for the link.</td>
</tr>
</tbody>
</table>

Usage

The SSCOP initiates the transmission of PDUs.

Example

arbitration active
end

Exits the current configuration mode and returns to the Exec mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

end

**Usage**

Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Use this command to return to the parent configuration mode.
mtp2-aerm-emergency-threshold

Configure the alignment error rate monitor (AERM) emergency threshold value. This command is only available for a lowspeed-narrowband link-type.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > SS7 Routing Domain Configuration > Linkset Configuration > Link Configuration

configure > ss7-routing-domain domain_id variant var_type > linkset id linkset_id > link id link_id

Entering the above command sequence results in the following prompt:

[local]host_name(config-ss7-rd-linkset-linkset_id-link-link_id)#

**Syntax**

mtp2-aerm-emergency-threshold value

default mtp2-aerm-emergency-threshold

<table>
<thead>
<tr>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resets the parameter to the default value of 1.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>value</th>
</tr>
</thead>
<tbody>
<tr>
<td>value: Enter an integer from 1 to 50. Default: 1.</td>
</tr>
</tbody>
</table>

**Usage**
This command sets the emergency threshold for the MTP2 alignment error rate monitor.

**Example**
Set the emergency AERM threshold to 17:

mtp2-aerm-emergency-threshold 17
mtp2-aerm-normal-threshold

Configure the alignment error rate monitor (AERM) normal threshold value. This command is only available for a lowspeed-narrowband link-type.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > SS7 Routing Domain Configuration > Linkset Configuration > Link Configuration configure > ss7-routing-domain domain_id variant var_type > linkset id linkset_id > link id link_id

Entering the above command sequence results in the following prompt:

[local]host_name(config-ss7-rd-linkset-linkset_id-link-link_id)#

Syntax

mtp2-aerm-normal-threshold value

default mtp2-aerm-normal-threshold

default

 Resets the parameter to the default value of 4.

value

value: Enter an integer from 4 to 100. Default: 4.

Usage

This command sets the normal threshold for the MTP2 alignment error rate monitor.

Example

Set the normal AERM threshold to 55:

mtp2-aerm-normal-threshold 55
mtp2-eim-decrement

Configure the errored interval monitor (EIM) emergency decrement value. This command is only available for a highspeed-narrowband link-type.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > SS7 Routing Domain Configuration > Linkset Configuration > Link Configuration

configure > ss7-routing-domain domain_id variant var_type > linkset id linkset_id > link id link_id

Entering the above command sequence results in the following prompt:

[local]host_name(config-ss7-rd-linkset-linkset_id-link-link_id)#

Syntax

mtp2-eim-decrement value

default mtp2-eim-decrement

default

Resets the parameter to the default value of 11.

value

value: Enter an integer from 1 to 63. Default: 11.

Usage

This command sets the emergency decrement value for the EIM.

Example

Reset the EIM emergency decrement to 1:

default mtp2-eim-decrement
mtp2-eim-increment

Configure the errored interval monitor (EIM) emergency increment value. This command is only available for a highspeed-narrowband link-type.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > SS7 Routing Domain Configuration > Linkset Configuration > Link Configuration
configure > ss7-routing-domain domain_id variant var_type > linkset id linkset_id > link id link_id

Entering the above command sequence results in the following prompt:

[local]host_name(config-ss7-rd-linkset-linkset_id-link-link_id)#

Syntax

mtp2-eim-increment value

default mtp2-eim-increment

default
Resets the parameter to the default value of 198.

value

value: Enter an integer from 1 to 1023. Default: 198.

Usage

This command sets the emergency increment value for the EIM.

Example

Set the EIM emergency increment to 2:

mtp2-eim-increment 2
mtp2-eim-threshold

Configure the errored interval monitor (EIM) emergency threshold value. This command is only available for a highspeed-narrowband link-type.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > SS7 Routing Domain Configuration > Linkset Configuration > Link Configuration
configure > ss7-routing-domain domain_id variant var_type > linkset id linkset_id > link id link_id

Entering the above command sequence results in the following prompt:

[local]host_name(config-ss7-rd-linkset-linkset_id-link-link_id)#

Syntax

mtp2-eim-threshold value

default mtp2-eim-threshold

default

Resets the parameter to the default value of 794.

value

value: Enter an integer from 1 to 65535. Default: 794.

Usage

This command sets the emergency threshold value for the EIM.

Example

Set the EIM emergency threshold to 154:

mtp2-eim-threshold 154
mtp2-error-correction

Configure the error correction method to be used. This command is only available for lowspeed or highspeed narrowband link-types.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > SS7 Routing Domain Configuration > Linkset Configuration > Link Configuration
configure > ss7-routing-domain domain_id variant var_type > linkset id linkset_id > link id link_id

Entering the above command sequence results in the following prompt:

[local]host_name(config-ss7-rd-linkset-linkset_id-link-link_id)#

Syntax

mtp2-error-correction { basic | preventive-cyclic-retransmission }

default mtp2-error-correction

default
Resets the parameter to the default value.

basic
Basic error correction (BEC) is a positive / negative acknowledgement method that uses backwards retransmission. This method is best for links with less than 30 ms one-way propagation delays.

preventive-cyclic-retransmission
PCR is recommended for links with 125 ms, or higher, propagation delays.

Usage
Set the method of MTP2 layer error correct to be used on the link.

Example
Set error correction for a link with 15 ms propagation delay:

mtp2-error-correction basic
mtp2-Issu-len

This command sets the length of the link status signal unit (LSSU) which carries link status information used to manage link alignment and indicate the status of the signaling points to each other. This command is only available for lowspeed or highspeed narrowband link-types.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > SS7 Routing Domain Configuration > Linkset Configuration > Link Configuration

configure > ss7-routing-domain  domain_id  variant  var_type  > linkset id  linkset_id  > link id  link_id

Entering the above command sequence results in the following prompt:

[local]host_name(config-ss7-rd-linkset-linkset_id-link-link_id)#

Syntax

mtp2-Issu-len  #_octets

default mtp2-Issu-len

default

Using this keyword with the command resets the length to the default of 1 octet.

#_octets

Sets the number of octets for the length of the LSSU.

#_octets: Must be either 1 or 2.

Usage

Use this command to define the maximum amount of link status information that is to be shared between signaling points.

Example

You can use the following command to set the LSSU length to 2 octets - the maximum length:

mtp2-Issu-len  2
**mtp2-max-outstand-frames**

This command sets the maximum number of outstanding packets to be sent by the link manager (linkmgr) - applicable for both high speed (HSL) and low speed (LSL) narrowband links.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > SS7 Routing Domain Configuration > Linkset Configuration > Link Configuration

```bash
configure > ss7-routing-domain domain_id variant var_type > linkset id linkset_id > link id link_id
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ss7-rd-linkset-linkset_id-link-link_id)#
```

**Syntax**

```
 mtp2-max-outstand-frames #_bytes
 default mtp2-max-outstand-frames
```

- **default**
  
  Using this keyword with the command resets number of packets to the default of 7 bytes.

- **#_bytes**
  
  Sets the maximum number of packets sent by the linkmgr that can be allowed to be outstanding.
  
  #_bytes: Must be an integer from 5 to 10.

**Usage**

The linkmgr (MTP2) sends data at a higher rate, than the narrowband (NB) E1 link speed, when in congestion and performing retransmission. This can lead to more congestion leading to more time taken for the link to come out of congestion. If using a value of 10 during congestion, then linkmgr pumps data at a rate higher than 2.5 mbps. To avoid this problem, a lower value is usually considered optimal. This configuration holds good for both HSL and LSL.

**Example**

Use the following command to reset the default number of outstanding packets sent by the LinkMgr:

```
 default mtp2-max-outstand-frames
```

Set the maximum number of outstanding packets the linkmgr can send to 6:

```
 mtp2-max-outstand-frames 6
```
mtp2-suerm-threshold

Configure the signal unit error rate monitor (SUERM) threshold. This command is only available for lowspeed-narrowband link-types.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > SS7 Routing Domain Configuration > Linkset Configuration > Link Configuration
configure > ss7-routing-domain domain_id variant var_type > linkset id linkset_id > link id link_id

Entering the above command sequence results in the following prompt:

[local]host_name(config-ss7-rd-linkset-linkset_id-link-link_id)#

Syntax

mtp2-suerm-threshold value

default mtp2-suerm-threshold

default

Resets the parameter to the default value.

value

Defines the threshold for number of bad frames
value: Enter an integer from 64 to 1023. Default is 64.

Usage
Sets the threshold for link monitoring of bad frames.

Example
Set a new link monitoring bad frames (SEURM) threshold of 256:

mtp2-suerm-threshold 256
**mtp3-discard-priority**

Configure MTP3 message discard priority.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > SS7 Routing Domain Configuration > Linkset Configuration > Link Configuration

`configure > ss7-routing-domain domain_id variant var_type > linkset id linkset_id > link id link_id`

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-ss7-rd-linkset-linkset_id-link-link_id)#
```

**Syntax**

```plaintext
mtp3-discard-priority priority

default mtp3-discard-priority

default

Resets the priority to the default value.

priority

priority: must be an integer between 0 and 3.
Default is 0.
```

**Usage**
Use this command to manage MTP3 messaging.

**Example**

```plaintext
mtp3-discard-priority 2
```
mtp3-max-slt-try

Configure maximum number of times to retry SLT (signaling link test).

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > SS7 Routing Domain Configuration > Linkset Configuration > Link Configuration

```bash
configure > ss7-routing-domain domain_id variant var_type > linkset id linkset_id > link id link_id
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ss7-rd-linkset-linkset_id-link-link_id)#
```

**Syntax**

```
mtp3-max-slt-try retries

default mtp3-max-slt-try
```

**default mtp3-max-slt-try**

```
default
Resets the number of retries to the default value.
```

```
retries
retries: must be an integer between 1 to 65535.
Default is 10.
```

**Usage**
Use this command to troubleshoot MTP3 link mismatch.

**Example**

```
mtp3-max-slt-try 35
```
mtp3-msg-priority

Configures the priority for sending MTP3 management messages.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > SS7 Routing Domain Configuration > Linkset Configuration > Link Configuration

configure > ss7-routing-domain domain_id variant var_type > linkset id linkset_id > link id link_id

Entering the above command sequence results in the following prompt:

[local]host_name(config-ss7-rd-linkset-linkset_id-link-link_id)#

Syntax

mtp3-msg-priority priority

default mtp3-msg-priority

---------------------
default

Resets the number of priority to the default value.

priority

priority: must be an integer from 0 to 3.
Default: 0

Usage

Use this command to set the priority for sending MTP3 management messages.

Example

Use the following to set the message priority to 3:

mtp3-msg-priority 3
mtp3-msg-size

Configures the size of messages from layer 3 to layer 2.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > SS7 Routing Domain Configuration > Linkset Configuration > Link Configuration
configure > ss7-routing-domain domain_id variant var_type > linkset id linkset_id > link id link_id

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ss7-rd-linkset-linkset_id-link-link_id)#
```

**Syntax**

```
mtp3-msg-size size

default mtp3-msg-size
```

**default**

Resets the size to the default value which is 4096 (for q.2140) or 272 (for MTP2)

**size**

- **size:** must be an integer from 1 to 272 for high-speed or low-speed narrowband SS7 links.
- **size:** must be an integer from 1 to 4096 for ATM broadband links.

**Usage**

Use this command to set the maximum message size, in bytes.

**Example**

Use this command to set the MTP3 message size to 4096 bytes:

```
mtp3-msg-size 4096
```
mtp3-p1-qlen

Configure the size for the MTP3 p1 queue length.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > SS7 Routing Domain Configuration > Linkset Configuration > Link Configuration
configure > ss7-routing-domain domain_id variant var_type > linkset id linkset_id > link id link_id

Entering the above command sequence results in the following prompt:
[local]host_name(config-ss7-rd-linkset-linkset_id-link-link_id)#

Syntax

mtp3-p1-qlen size

default mtp3-p1-qlen

default

Resets the number of size of the priority 1 queue to the default value.

size

size: integer from 1 to 65535. Size should be less than MTP3 p2 qlen and p3 qlen.
Default: 1024

Usage

Use this command to configure the queue length threshold for raising the congestion priority to level 1.

Example

Use this command to set the queue length priority to 128:

mtp3-p1-qlen 128
**mtp3-p2-qlen**

Configure the size of the priority 2 queue.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > SS7 Routing Domain Configuration > Linkset Configuration > Link Configuration  
configure > ss7-routing-domain domain_id variant var_type > linkset id linkset_id > link id link_id  

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ss7-rd-linkset-linkset_id-link-link_id)#
```

**Syntax**

```
mtp3-p2-qlen size

default mtp3-p2-qlen
```

**default mtp3-p2-qlen**

```
default

Resets the number of size of the priority 2 queue to the default value.

size

size: integer from 1 to 65535. Size should be less than MTP3 p3 qlen and greater than p1 qlen.  
Default: 1024
```

**Usage**

Use this command to configure the queue length threshold for raising the congestion priority to level 2.

**Example**

Use this command to set the queue length threshold to 256:

```
mtp3-p2-qlen 256
```
mtp3-p3-qlen

Configure the size of the priority 3 queue.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > SS7 Routing Domain Configuration > Linkset Configuration > Link Configuration

```
configure > ss7-routing-domain domain_id variant var_type > linkset id linkset_id > link id link_id
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ss7-rd-linkset-linkset_id-link-link_id)#
```

**Syntax**

```
mtp3-p3-qlen size
```

**default mtp3-p3-qlen**

- **default**
  Resets the number of size of the priority 3 queue to the default value.

- **size**
  
  *size:* integer from 1 to 65535. Size should be greater than MTP3 p1 qlen and p2 qlen .
  Default: 1024

**Usage**

Use this command to configure the queue length threshold for raising the congestion priority to level 3.

**Example**

```
mtp3-p3-qlen 1024
```
mtp3-test-pattern

Configures the character string for the test message.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > SS7 Routing Domain Configuration > Linkset Configuration > Link Configuration

configure > ss7-routing-domain domain_id variant var_type > linkset id linkset_id > link id link_id

Entering the above command sequence results in the following prompt:

[local]host_name(config-ss7-rd-linkset-linkset_id-link-link_id)#

Syntax

mtp3-test-pattern pattern

default mtp3-test-pattern

default

Resets the pattern to the default value.

pattern

pattern: 1 to 15 alphanumeric characters.
Default: SGSN-ORIGINATED

Usage

Use this command to define a test pattern string for the signalling link test match (SLTM).

Example

mtp3-test-pattern TEST1-HomeOffice
priority

Configures the MTP3 Link Priority.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > SS7 Routing Domain Configuration > Linkset Configuration > Link Configuration

configure > ss7-routing-domain domain_id variant var_type > linkset id linkset_id > link id link_id

Entering the above command sequence results in the following prompt:

[local]host_name(config-ss7-rd-linkset-linkset_id-link-link_id)#

Syntax

priority pri_value

no priority

no

Removes the priority configuration.

pri_value

pri_value: 0 represents highest priority and 15 represents the lowest priority.

Usage

Use this command to configure the link priority within the MTP3 link set.

Example

priority 2
signaling-link-code

Configures the signaling link code (SLC).

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > SS7 Routing Domain Configuration > Linkset Configuration > Link Configuration

configure > ss7-routing-domain *domain_id* variant *var_type* > linkset id *linkset_id* > link id *link_id*

Entering the above command sequence results in the following prompt:

[local]host_name(config-ss7-rd-linkset-linkset_id-link-link_id)#

**Syntax**

```
signaling-link-code code

no signaling-link-code
```

**Usage**

Removes the SLC configuration.

```
code

code: integer from 0 to 15.
```

**Example**

Use this command to uniquely identify the signaling link to be used for MTP3 management messages.

```
signaling-link-code 4
```
**sscf-nni-n1**

Configures the SSCF NNI N1. This command is only available for ATM-broadband link-types.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > SS7 Routing Domain Configuration > Linkset Configuration > Link Configuration

```
configure > ss7-routing-domain domain_id variant var_type > linkset id linkset_id > link id link_id
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-ss7-rd-linkset-linkset_id-link-link_id)#
```

**Syntax**

```
sscf-nni-n1 value

no scsf-nni-n1
```

**Default**
Removes the scsf-nni-n1 configuration.

**Value**

```
value

value: integer from 1 to 65535.
Default: 1000
```

**Usage**
Use this command to identify the network-to-node interface (NNI) between the MTP3 and SSCOP layers.

**Example**

```
sscf-nni-n1 4064
```
**sscop-max-cc**

Configure the maximum value for the SSCOP connection control (CC) state variable. This command is only available for ATM-broadband link-types.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > SS7 Routing Domain Configuration > Linkset Configuration > Link Configuration
configure > ss7-routing-domain domain_id variant var_type > linkset id linkset_id > link id link_id

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ss7-rd-linkset-linkset_id-link-link_id)#
```

**Syntax**

```
sscop-max-cc value

no sscop-max-cc
```

**Usage**
Use this command as part of the configuration responsible for managing the SSCOP connection. This command sets the number of times retries.

**Example**

```
sscop-max-cc 256
```
**sscop-max-pd**

Configures the maximum acceptable value for the SSCOP state variable VT(PD). This command is only available for ATM-broadband link-types.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > SS7 Routing Domain Configuration > Linkset Configuration > Link Configuration

```
configure > ss7-routing-domain  domain_id  variant  var_type  > linkset_id  linkset_id  > link_id  link_id
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ss7-rd-linkset-linkset_id-link-link_id)#
```

**Syntax**

```
sscop-max-pd  value

no sscop-max-pd
```

- **default**
  - Removes the sscop-max-pd configuration.

- **value**
  - value: integer from 1 to 65535.
  - Default: 500

**Usage**

Use this command to define the maximum number of data PDUs transmitted between POLL PDUs.

**Example**

```
sscop-max-pd  2500
```
**sscop-max-stat**

Configures the maximum number of elements included in a status PDU. This command is only available for ATM-broadband link-types.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > SS7 Routing Domain Configuration > Linkset Configuration > Link Configuration

```
configure > ss7-routing-domain domain_id variant var_type > linkset id linkset_id > link id link_id
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ss7-rd-linkset-linkset_id-link-link_id)#
```

**Syntax**

```
sscop-max-stat value

no sscop-max-stat
```

**default**

Removes the sscop-max-stat configuration.

**value**

*value*: integer from 3 to 65535. This parameter should be an odd integer greater than or equal to 3. Default: 67

**Usage**

Received in response to a POLL PDU, the STAT PDU includes information about the number of SD PDUs that have been received.

**Example**

```
sscop-max-stat 56000
```
**timeout**

This command enables configuration of an array of signaling and flow control timers - for MTP, SSCF, and SSCOP.

**Product**  
SGSN

**Privilege**  
Security Administrator, Administrator

**Mode**  
Exec > Global Configuration > SS7 Routing Domain Configuration > Linkset Configuration > Link Configuration

```bash
configure > ss7-routing-domain domain_id variant var_type > linkset id linkset_id > link id link_id
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-ss7-rd-linkset-linkset_id-link-link_id)#
```

**Syntax**

```bash
[ no ] timeout timer timer_value
```

- **no**  
  Adding **no** to the **timeout** command removes the timer configuration.

- **timer timer_value**  
  Select the timer and enter a value from the range.
  For timers having different ranges for highspeed and lows speed links or for different variants, the appropriate ranges will be displayed based on the link-type configured.

**Important:** Currently, the China variant uses ITU values.

<table>
<thead>
<tr>
<th>Timer</th>
<th>Link Type &amp; Variant</th>
<th>Range of Times Granularity = 100ms</th>
<th>Default Time</th>
</tr>
</thead>
</table>
| **mtp2-tmr-t1**
Alignment ready timer | Highspeed; ITU       | 160..3500 (16 - 350 seconds) | 3000 (300 seconds)  |
|               | Lowspeed; ITU       | 120 - 500 (12 - 50 seconds) | 400 (40 seconds)  |
|               | Highspeed; ANSI     | 160 - 3500 (16 to 350 seconds) | 1700 (170 seconds) |
|               | Lowspeed; ANSI      | 120 - 500 (12 - 50 seconds) | 130 (13 seconds)  |
| **mtp2-tmr-t2**
Not aligned timer | Highspeed; ITU       | 50 - 1500 (5 - 150 seconds) | 50 (5 seconds)    |
<p>|               | Lowspeed; ITU       | 50 - 150 (5 - 15 seconds) | 50 (5 seconds)    |</p>
<table>
<thead>
<tr>
<th>Timer</th>
<th>Link Type &amp; Variant</th>
<th>Range of Times Granularity = 100ms</th>
<th>Default Time</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Highspeed; ANSI</td>
<td>50 - 1500 (5 - 150 seconds)</td>
<td>230 (23 seconds)</td>
</tr>
<tr>
<td></td>
<td>Lowspeed; ANSI</td>
<td>50 - 150 (5 - 15 seconds)</td>
<td>115 (11.5 seconds)</td>
</tr>
<tr>
<td><strong>mtp2-tmr-t3</strong></td>
<td>Highspeed/Lowspeed; ITU</td>
<td>10 - 140 (1 - 14 seconds)</td>
<td>15 (1.5 seconds)</td>
</tr>
<tr>
<td>Aligned timer</td>
<td>Highspeed/Lowspeed; ITU</td>
<td>10 - 140 (1 - 14 seconds)</td>
<td>115 (11.5 seconds)</td>
</tr>
<tr>
<td><strong>mtp2-tmr-t4e</strong></td>
<td>Highspeed; ITU</td>
<td>4 - 60 (400 milliseconds - 6 seconds)</td>
<td>5 (500 milliseconds)</td>
</tr>
<tr>
<td>Emergency proving period timer</td>
<td>Lowspeed; ITU</td>
<td>4 - 6 (400 - 600 milliseconds)</td>
<td>5 (500 milliseconds)</td>
</tr>
<tr>
<td></td>
<td>Highspeed; ANSI</td>
<td>4 - 60 (400 milliseconds - 6 seconds)</td>
<td>50 (5 seconds)</td>
</tr>
<tr>
<td></td>
<td>Lowspeed; ANSI</td>
<td>4 - 6 (400 - 600 milliseconds)</td>
<td>6 (600 milliseconds)</td>
</tr>
<tr>
<td><strong>mtp2-tmr-t4n</strong></td>
<td>Highspeed; ITU</td>
<td>30 - 700 (3 to 70 seconds)</td>
<td>3 (30 seconds)</td>
</tr>
<tr>
<td>Normal proving period timer</td>
<td>Lowspeed; ITU</td>
<td>20 - 95 (2 - 9.5 seconds)</td>
<td>82 (8.2 seconds)</td>
</tr>
<tr>
<td>Once set this timer can be reset but it can not be disabled.</td>
<td>Highspeed; ANSI</td>
<td>30 - 700 (3 to 70 seconds)</td>
<td>3 (30 seconds)</td>
</tr>
<tr>
<td></td>
<td>Lowspeed; ANSI</td>
<td>20 - 95 (2 - 9.5 seconds)</td>
<td>23 (2.3 seconds)</td>
</tr>
<tr>
<td><strong>mtp2-tmr-t5</strong></td>
<td>Highspeed/Lowspeed ITU/ANSI</td>
<td>1 - 2 (100 - 200 milliseconds)</td>
<td>1 (100 milliseconds)</td>
</tr>
<tr>
<td>Sending status indication busy (SIB) timer</td>
<td>Highspeed/Lowspeed ITU/ANSI</td>
<td>10 - 60 (1 to 6 seconds)</td>
<td>30 (3 seconds)</td>
</tr>
<tr>
<td><strong>mtp2-tmr-t6</strong></td>
<td>Highspeed/Lowspeed ITU/ANSI</td>
<td>5 - 20 (500 milliseconds - 2 seconds)</td>
<td>10 (1 second)</td>
</tr>
<tr>
<td>Remote congestion timer</td>
<td>Highspeed/Lowspeed ITU/ANSI</td>
<td>1 - 2 (100 - 200 milliseconds)</td>
<td>1 (100 milliseconds)</td>
</tr>
<tr>
<td><strong>mtp2-tmr-t7</strong></td>
<td>Highspeed/Lowspeed ITU/ANSI</td>
<td>5 - 12 (500 - 1200 milliseconds)</td>
<td>5 (500 milliseconds)</td>
</tr>
<tr>
<td>Excessive delay of acknowledgement timer</td>
<td>Highspeed/Lowspeed ITU/ANSI</td>
<td>5 - 12 (500 - 1200 milliseconds)</td>
<td>5 (500 milliseconds)</td>
</tr>
<tr>
<td><strong>mtp3-tmr-t1</strong></td>
<td>Highspeed/Lowspeed ITU/ANSI</td>
<td>5 - 12 (500 - 1200 milliseconds)</td>
<td>5 (500 milliseconds)</td>
</tr>
<tr>
<td>Timer</td>
<td>Link Type &amp; Variant</td>
<td>Range of Times</td>
<td>Default Time</td>
</tr>
<tr>
<td>-----------------------</td>
<td>--------------------</td>
<td>----------------</td>
<td>-------------------</td>
</tr>
<tr>
<td><strong>mtp3-tmr-t12</strong></td>
<td>Highspeed/Lowspeed</td>
<td>8 - 15 (800 - 1500 milliseconds)</td>
<td>8 (800 milliseconds)</td>
</tr>
<tr>
<td>Waiting for uninhibit acknowledgement timer</td>
<td>ITU/ANSI</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>mtp3-tmr-t13</strong></td>
<td>Highspeed/Lowspeed</td>
<td>8 - 15 (800 - 1500 milliseconds)</td>
<td>8 (800 milliseconds)</td>
</tr>
<tr>
<td>Waiting for force uninhibit timer</td>
<td>ITU/ANSI</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>mtp3-tmr-t14</strong></td>
<td>Highspeed/Lowspeed</td>
<td>20 - 30 (2000 - 3000 milliseconds)</td>
<td>20 (2000 milliseconds)</td>
</tr>
<tr>
<td>Waiting for inhibition acknowledgement timer</td>
<td>ITU/ANSI</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>mtp3-tmr-t17</strong></td>
<td>Highspeed/Lowspeed</td>
<td>8 - 15 (800 - 1500 milliseconds)</td>
<td>8 (800 milliseconds)</td>
</tr>
<tr>
<td>Delay to avoid oscillation of initial alignment failure and link restart</td>
<td>ITU/ANSI</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>mtp3-tmr-t2</strong></td>
<td>Highspeed/Lowspeed</td>
<td>7 - 20 (700 - 2000 milliseconds)</td>
<td>7 (700 milliseconds)</td>
</tr>
<tr>
<td>Waiting for changeover acknowledgement</td>
<td>ITU/ANSI</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>mtp3-tmr-t22</strong></td>
<td>Highspeed/Lowspeed</td>
<td>1800 - 3000 (180 - 300 seconds)</td>
<td>1800 (180 seconds)</td>
</tr>
<tr>
<td>Local inhibit test timer</td>
<td>ITU/ANSI</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>mtp3-tmr-t23</strong></td>
<td>Highspeed/Lowspeed</td>
<td>1800 - 3000 (180 - 300 seconds)</td>
<td>1800 (180 seconds)</td>
</tr>
<tr>
<td>Remote inhibit test timer</td>
<td>ITU/ANSI</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>mtp3-tmr-t24</strong></td>
<td>Highspeed/Lowspeed</td>
<td>5 - 15 (500 - 1500 milliseconds)</td>
<td>5 (500 milliseconds)</td>
</tr>
<tr>
<td>Stabilising timer after removal of local processor outage, used in LPO latching to RPO (national option)</td>
<td>ITU/ANSI</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>mtp3-tmr-t3</strong></td>
<td>Highspeed/Lowspeed</td>
<td>5 - 12 (500 - 1200 milliseconds)</td>
<td>5 (500 milliseconds)</td>
</tr>
<tr>
<td>Time controlled diversion-delay to avoid missequencing on changeback</td>
<td>ITU/ANSI</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>mtp3-tmr-t31</strong></td>
<td>Highspeed/Lowspeed</td>
<td>50 - 100 (5 to 10 seconds)</td>
<td>50 (5 seconds)</td>
</tr>
<tr>
<td>BSN requested timer</td>
<td>ITU/ANSI</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>mtp3-tmr-t32</strong></td>
<td>Highspeed/Lowspeed</td>
<td>40 - 120 (4 - 12 seconds)</td>
<td>100 (10 seconds)</td>
</tr>
<tr>
<td>SLT timer</td>
<td>ITU/ANSI</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>mtp3-tmr-t33</strong></td>
<td>Highspeed/Lowspeed</td>
<td>50 - 100 (5 to 10 seconds)</td>
<td>50 (5 seconds)</td>
</tr>
<tr>
<td>Connecting timer</td>
<td>ITU/ANSI</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>mtp3-tmr-t34</strong></td>
<td>Highspeed/Lowspeed</td>
<td>300 - 900 (30 to 90 seconds)</td>
<td>600 (60 seconds)</td>
</tr>
<tr>
<td>Periodic signalling link test timer</td>
<td>ITU/ANSI</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>mtp3-tmr-t4</strong></td>
<td>Highspeed/Lowspeed</td>
<td>5 - 12 (500 to 1200 milliseconds)</td>
<td>5 (500 milliseconds)</td>
</tr>
<tr>
<td>Waiting for changeback acknowledgement (first attempt)</td>
<td>ITU/ANSI</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>mtp3-tmr-t5</strong></td>
<td>Highspeed/Lowspeed</td>
<td>5 - 12 (500 to 1200 milliseconds)</td>
<td>5 (500 milliseconds)</td>
</tr>
<tr>
<td>Waiting for changeback acknowledgement (second attempt)</td>
<td>ITU/ANSI</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>mtp3-tmr-t7</strong></td>
<td>Highspeed/Lowspeed</td>
<td>10 - 20 (1000 - 2000 milliseconds)</td>
<td>10 (1000 milliseconds)</td>
</tr>
<tr>
<td>Waiting for signalling data link connection acknowledgement</td>
<td>ITU/ANSI</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Timer</td>
<td>Link type &amp; Variant</td>
<td>Range of Times</td>
<td>Default Time</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------</td>
<td>-----------------------------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>sscf-nni-tmr-t1</td>
<td>ATM Broadband</td>
<td>1 - 65535 (10 - 655350 milliseconds)</td>
<td>500 (5 seconds)</td>
</tr>
<tr>
<td></td>
<td>ITU/ANSI</td>
<td>Granularity = 10 ms</td>
<td></td>
</tr>
<tr>
<td>sscf-nni-tmr-t2</td>
<td>ATM Broadband</td>
<td>1 - 65535 (10 - 655350 milliseconds)</td>
<td>3000 (30 seconds)</td>
</tr>
<tr>
<td></td>
<td>ITU/ANSI</td>
<td>Granularity = 10 ms</td>
<td></td>
</tr>
<tr>
<td>sscf-nni-tmr-t3</td>
<td>ATM Broadband</td>
<td>1 - 65535 (10 - 655350 milliseconds)</td>
<td>1 (10 milliseconds)</td>
</tr>
<tr>
<td></td>
<td>ITU/ANSI</td>
<td>Granularity = 10 ms</td>
<td></td>
</tr>
<tr>
<td>scop-tmr-cc</td>
<td>ATM Broadband</td>
<td>1 - 65535 (100 - 6553500 milliseconds)</td>
<td>2 (200 milliseconds)</td>
</tr>
<tr>
<td></td>
<td>ITU/ANSI</td>
<td>Granularity = 100 ms</td>
<td></td>
</tr>
<tr>
<td>scop-tmr-idle</td>
<td>ATM Broadband</td>
<td>1 - 65535 (100 - 6553500 milliseconds)</td>
<td>1 (100 milliseconds)</td>
</tr>
<tr>
<td></td>
<td>ITU/ANSI</td>
<td>Granularity = 100 ms</td>
<td></td>
</tr>
<tr>
<td>scop-tmr-keep-alive</td>
<td>ATM Broadband</td>
<td>1 - 65535 (100 - 6553500 milliseconds)</td>
<td>1 (100 milliseconds)</td>
</tr>
<tr>
<td></td>
<td>ITU/ANSI</td>
<td>Granularity = 100 ms</td>
<td></td>
</tr>
<tr>
<td>scop-tmr-no-rsp</td>
<td>ATM Broadband</td>
<td>1 - 65535 (100 - 6553500 milliseconds)</td>
<td>15 (1.5 seconds)</td>
</tr>
<tr>
<td></td>
<td>ITU/ANSI</td>
<td>Granularity = 100 ms</td>
<td></td>
</tr>
<tr>
<td>scop-tmr-poll</td>
<td>ATM Broadband</td>
<td>1 - 65535 (100 - 6553500 milliseconds)</td>
<td>1 (100 milliseconds)</td>
</tr>
<tr>
<td></td>
<td>ITU/ANSI</td>
<td>Granularity = 100 ms</td>
<td></td>
</tr>
</tbody>
</table>

**Usage**

For a single link and specified link-type (highspeed or lowspeed), this command sets the timer values listed above. The SS7 variant is determined when the SS7 routing domain is first defined from the Global Configuration mode.

Repeat the `timeout` command (one timer and value per entry) as needed to configure all required timers.

**Important:** Currently, the China variant uses the same timers, values, and defaults as the ITU variant.

**Example**

```
timeout timer timer_value
```
Chapter 187
Linkset Configuration Mode Commands

The Linkset configuration mode defines the MTP3 linkset parameters for a specific SS7 routing domain instance.

Mode

Exec > Global Configuration > SS7 Routing Domain Configuration > Linkset Configuration

configure > ss7-routing-domain domain_id variant var_type > linkset id linkset_id

Entering the above command sequence results in the following prompt:

[local]host_name(config-ss7-rd-linkset-linkset_id)#

⚠️ Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
adjacent-point-code

This command defines the point-code for the adjacent (next) network element in the SS7 network.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > SS7 Routing Domain Configuration > Linkset Configuration

```
configure > ss7-routing-domain domain_id variant var_type > linkset id linkset_id
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ss7-rd-linkset-linkset_id)#
```

**Syntax**

```
adjacent-point-code point-code

no adjacent-point-code
```

**point-code**

Point-code is an SS7 address for an element in the SS7 network. Point-codes must be defined in dotted-decimal format in a string of 1 to 11 digits. Format options include:

- 0.0.1 to 7.255.7 for point-code in the ITU range.
- 0.0.1 to 255.255.255 for point-code in the ANSI range.
- 0.0.1 to 15.31.255 for point-code in the TTC range.
- A string of 1 to 11 digits in dotted-decimal to represent a point-code in a different range.

**no**

Removes the adjacent-point-code configuration for this linkset in the SS7 routing domain

**Important:** Removing the linkset configuration will result in the termination of all of the links within the linkset.

**Usage**

Use this command to define the point-code for the adjacent element in the SS7 network.

**Example**

```
adjacent-point-code 6.202.7
```
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Use this command to return to the parent configuration mode.
link

This command creates an MTP3 link configuration for the SS7 linkset and enters the Link configuration mode.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > SS7 Routing Domain Configuration > Linkset Configuration

configure > ss7-routing-domain domain_id variant var_type > linkset id linkset_id

Entering the above command sequence results in the following prompt:

[local]host_name(config-ss7-rd-linkset-linkset_id)#

Syntax

link id id [ link-type [ atm-broadband | highspeed-narrowband | lowspeed-narrowband ]

no link id id

no
Disables the specified link configuration.

**Important:** Removing the link configuration will result in the termination of traffic on the specified link.

#_octets
Sets the number of octets for the length of the LSSU.

id
This number uniquely identifies the link in the linkset.
id: an integer between 1 and 16.

**link-type**
Identifies the signalling type for this link; options include:

- ATM broadband -- ATM AAL5 over an optical line card (OLC2)
- high speed-narrowband -- 64 kbps over a channelized optical line card (CLC2)
- low speed-narrowband -- 4.8 kbps over a channelized optical line card (CLC2)

**Important:** Be default link-type is ATM-broadband. To support narrowband SS7, one of the other options must be set.
**Usage**

Access the Link configuration mode to configure the parameters for the link.

**Example**

Access configuration for link 4:

```
link id 4
```
**self-point-code**

This command defines the SS7 network point-code to identify this SGSN.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > SS7 Routing Domain Configuration > Linkset Configuration

```
configure > ss7-routing-domain domain_id variant var_type > linkset id linkset_id
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ss7-rd-linkset-linkset_id)#
```

**Syntax**

```
self-point-code point-code
no self-point-code
```

- **point-code**
  
  Point-code is an SS7 address for an element in the SS7 network. Point-codes must be defined in dotted-decimal format in a string of 1 to 11 digits. Format options include:
  
  - 0.0.1 to 7.255.7 for point-code in the ITU range.
  - 0.0.1 to 255.255.255 for point-code in the ANSI range.
  - 0.0.1 to 15.31.255 for point-code in the TTC range.
  - a string of 1 to 11 digits in dotted-decimal to represent a point-code in a different range.

- **no**

  Removes the self-point-code configuration for this linkset in the SS7 routing domain.

**Important:** Removing the self-point-code will result in the termination of all traffic on this link.

**Usage**

Use this command to define the SS7 point-code to identify this system.

**Example**

```
self-point-code 6.192.7
```
Chapter 188
LMA Service Configuration Mode Commands

The LMA Service Configuration Mode is used to create and manage the Local Mobility Anchor configuration supporting Proxy Mobile IP on a PDN Gateway in an eHRPD and E-UTRAN/EPC network.

Mode

Exec > Global Configuration > Context Configuration > LMA Service Configuration

configure > context context_name > lma-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-lma-service)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
aaa accounting

Enables the LMA to send AAA accounting information for subscriber sessions.

Product
P-GW
SAEGW

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > LMA Service Configuration

configure > context context_name > lma-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-lma-service)#

Syntax

[ default | no ] aaa accounting

- default
  Sets the command to the default condition of enabled.

- no
  Disables the ability of the LMA to send AAA accounting information.

Usage

Use this command to enable the LMA service to send all accounting data (start, stop, and interim) to the configured AAA servers.

Important: In order for this command to function properly, AAA accounting must be enabled for the context in which the LMA service is configured using the `aaa accounting subscriber radius` command.

Example

The following command disables aaa accounting for the LMA service:

`no aaa accounting`
bind address

Binds the LMA service to a logical IP interface serving as the S2a (HSGW) or S5/S8 (S-GW) interface and specifies the maximum number of subscribers that can access this service over the configured interface.

**Product**
- P-GW
- SAEGW

**Privilege**
- Administrator

**Mode**
- Exec > Global Configuration > Context Configuration > LMA Service Configuration

configure > context context_name > lma-service service_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-lma-service)#
```

**Syntax**

```
bind address ipv6_address [ ipv4-address ipv4_address ] [ max-subscribers num ]
```

**no bind address**

- **no**
  - Removes the interface binding from this service.

- **address ipv6_address**
  - Specifies the IPv6 address of the interface configured as the S2a or S5/S8 interface. `ipv6_address` is specified in colon separated notation.

- **ipv4-address ipv4_address**
  - Specifies optional IPv4 HA/P-GW address to support DSMIP6 session using IPv4 transport. `ipv4_address` must be entered as a standard IPv4 address in dotted decimal notation.

- **max-subscribers num**
  - Default: 3000000
  - Specifies the maximum number of subscribers that can access this service on this interface. `num` must be configured to an integer between 0 and 3,000,000.

**Important:** The maximum number of subscribers supported is dependant on the license key installed and the number of active PSCs in the system. A fully loaded system with 13 active PSCs can support 3,000,000 total subscribers. Refer to the license key command and the Usage section (below) for additional information.
bind address

Usage

Associate the LMA service to a specific logical IP address. The logical IP address or interface takes on the characteristics of an S2a or S5/S8 interface that provides the session connectivity to an HSGW (S2a) or S-GW (S5/S8). Only one interface can be bound to a service. The interface should be configured prior to issuing this command.

This command also sets a limit as to the number of simultaneous subscribers sessions that can be facilitated by the service/interface at any given time.

When configuring the **max-subscribers** option, be sure to consider the following:

- The total number of S2a or S5/S8 interfaces you will configure
- The total number of subscriber sessions that all of the configured interfaces may handle during peak busy hours
- An average bandwidth per session multiplied by the total number of sessions
- The type of physical port (10/100Base-T or 1000Base-Tx) that these interfaces will be bound to

Taking these factors into account and distributing your subscriber session across all available interfaces will allow you to configure your interfaces to optimally handle sessions without degraded performance.

Example

The following command would bind the logical IP interface with the address of 4551:0db8:85a3:08d3:3319:8a2e:0370:1344 to the LMA service and specifies that a maximum of 300,000 simultaneous subscriber sessions can be facilitated by the interface/service at any given time:

```
bind address 4551:0db8:85a3:08d3:3319:8a2e:0370:1344 max-subscribers 300000
```
end

Exits the current mode and returns to the Exec Mode.

**Product**
All

**Privilege**
Administrator

**Syntax**

**Usage**
Change the mode back to the Exec mode.
exit

Exits the current mode and returns to the previous mode.

**Product**
- All

**Privilege**
- Administrator

**Syntax**

```plaintext
exit
```

**Usage**

Return to the previous mode.
heartbeat

Configures the PMIPv6 heartbeat message interval, retransmission timeout, and max retransmission for the LMA Service.

Product
P-GW

Privilege
Administrator

Syntax

```
heartbeat { interval seconds | retransmission { max number | timeout seconds } }

default heartbeat { interval | retransmission { max | timeout } }

no heartbeat
```

- **no**

Disables the PMIPv6 heartbeat functionality. The P-GW starts sending heartbeat request to peers when the heartbeat interval is configured.

- **default**

Resets the specified parameter to the system default value.

- **interval seconds**

The interval in seconds at which heartbeat messages are sent.

Seconds is an integer from 30 through 3600.

Default: 60

- **retransmission max number**

The maximum number of heartbeat retransmissions allowed.

Number is an integer from 1 through 15.

Default: 3

- **retransmission timeout seconds**

The timeout in seconds for heartbeat retransmissions.

Seconds is an integer from 1 through 20.

Default: 3

Usage

Proxy Mobile IPv6 (PMIPv6) is a network-based mobility management protocol to provide mobility without requiring the participation of the mobile node in any PMIPv6 mobility related signaling. The Local Mobility Anchor (LMA) service sets up tunnels dynamically to manage mobility for a mobile node.

This command provides configuration of heartbeat messages between the LMA and MAG services to know the reachability of the peers, to detect failures, quickly inform peers in the event of a recovery from node failures, and allow a peer to take appropriate action.
Example

The following command enables PMIPv6 heartbeat messaging to known LMA service peers and sets the heartbeat interval to 160 seconds.

```
    heartbeat interval 160
```
mobility-option-type-value

Changes the mobility option type value used in mobility messages.

Product
P-GW
SAEGW

Privilege
Administrator

Syntax

mobility-option-type-value { custom1 | custom2 | standard }

default mobility-option-type-value

default
Sets the command to the default value of custom1.

custom1
( Default ) Non-standard type values used before they were defined by IANA.

custom2
Standard type values, as defined by IANA, and some customer-specific message formats.

standard
Standard type values as defined by IANA. In addition, standard option uses type values defined in RFC 5844 for HoA options for PMIPv6 PBU/PBA/revocation message.

Usage
Use this command to change the mobility option type value used in mobility messages.

Example

The following command changes the mobility option type value to standard:

    mobility-option-type-value standard
refresh-advice-option

Configures inclusion of a refresh advice option in the binding acknowledgement message sent by the LMA.

**Product**
P-GW
SAEGW

**Privilege**
Administrator

**Syntax**

```
[ default | no ] refresh-advice-option
```

- **default**
  Returns the command setting to the default setting of disabled.

- **no**
  Disables the inclusion of the refresh advice option in the binding acknowledgement message sent by the LMA

**Usage**

Use this command to enable the LMA to include this option in a binding acknowledgment sent to the requesting MAG. The option provides a “hint” to the MAG of when it should refresh the binding. As defined in RFC 3775 “Mobility Support in IPv6”, the binding refresh advice option can only be present in the binding acknowledgement sent from the mobile node’s home agent in reply to a registration request. A refresh interval parameter determines the amount of time until the mobile node must send a new registration to the home agent to avoid de-registration and loss of session.

**Important:** Refer to the refresh-interval-percent and reg-lifetime commands for a complete understanding of registration (binding) lifetimes and refresh intervals.
**refresh-interval-percent**

Configures percentage of the granted registration lifetime to be used in the refresh interval mobility option in a binding acknowledgement message sent by the LMA service.

**Product**

P-GW

SAEGW

**Privilege**

Administrator

**Syntax**

```
refresh-interval-percent number
```

```
default refresh-interval-percent
```

```
default
```

Resets the command value to the default setting of 75.

```
number
```

Default: 75

Sets the percent value for session lifetimes for this service.

`number` must be an integer value from 1 to 99.

**Usage**

Use this command to configure the amount of the granted registration lifetime to be used in the refresh interval mobility option in the binding acknowledgement message sent by the LMA service to the requesting MAG.

Refreshing a binding or registration is based on the granted registration lifetime. Since a refresh request must be within the granted range of a registration lifetime, this command provides a method of setting the interval of when a refresh request is sent.

As described in RFC 3775 “Mobility Support in IPv6”, if a binding refresh advice option is present in the binding acknowledgement, the refresh interval field in the option must be a value less than the binding lifetime (also returned in the binding acknowledgement). The mobile node then should attempt to refresh its registration at the shorter refresh interval. The home agent will still honor the registration for the lifetime period, even if the mobile node does not refresh its registration within the refresh period.

**Important**: Refer to the refresh-advice-option and reg-lifetime commands for a complete understanding of registration (binding) lifetimes and refresh intervals.

**Example**

The following command sets the refresh interval percent to 90:

```
refresh-interval-percent 90
```
reg-lifetime

Configures the Mobile IPv6 session registration lifetime for this service.

Product
- P-GW
- SAEGW

Privilege
Administrator

Syntax

```
reg-lifetime seconds

default reg-lifetime
```

- **default**
  Resets the command value to the default setting of 600.

- **seconds**
  Default: 600
  Sets the time value for session lifetimes for this service.
  `seconds` must be an integer value from 1 to 262140.

Usage

Use this command to limit PMIPv6 lifetime on this service. If the PBU contains a lifetime shorter than what is specified, it is granted. If the lifetime is longer, then HA service will limit the granted lifetime to the configured value.

**Important:** Refer to the refresh-interval-percent and refresh-advice-option commands for a complete understanding of registration (binding) lifetimes and refresh intervals.

Example

The following command sets the registration lifetime for Mobile IPv6 sessions using this service to 1200 seconds (20 minutes):

```
reg-lifetime 1200
```
revocation

Enables the MIP revocation feature and configures revocation parameters.

**Product**
P-GW
SAEGW

**Privilege**
Administrator

**Syntax**

```
revocation { enable | max-retransmission number | retransmission-timeout msecs }
```

```
default revocation { enable | max-retransmission | retransmission-timeout }
```

```
no revocation enable
```

---

**default**

Resets the keyword to its default value.

---

**no**

Disables revocation for this service.

---

**enable**

Default: disabled

Enables the MIP registration revocation feature for the LMA service. When enabled, if revocation is negotiated with a MAG and a MIP binding is terminated, the LMA can send a Revocation message to the MAG. This feature is disabled by default.

---

**max-retransmission number**

Default: 3

The maximum number of retransmissions of a Revocation message before the revocation fails. *number* must be an integer value from 0 through 10.

---

**retransmission-timeout msecs**

Default: 3000

The number of milliseconds to wait for a Revocation Acknowledgement from the MAG before retransmitting the Revocation message. *msecs* must be an integer value from 500 through 10000.

---

**Usage**

Use this command to enable or disable the MIP revocation feature on the LMA or to change settings for this feature.

---

**Example**

The following command sets the maximum number of retries for a Revocation message to 6:

```
revocation max-retransmission 6
```
The following command sets the timeout between retransmissions to 10:

```plaintext
revocation retransmission-timeout 10
```
sequence-number-validate

Configures sequence number validation of the received MIPv6 control packets by the LMA service according to RFC 3775.

Product
P-GW
SAEGW

Privilege
Administrator

Syntax

[ default | no ] sequence-number-validate

- **default**
  Resets the command value to the default setting of enabled.

- **no**
  Disables the feature.

Usage

Use this command to configure the sequence number validation of the received MIPv6 control packets (PBUs) by the LMA service. This feature validates MIPv6 control packets and insures that any incoming packets with a sequence number prior to the last number received is consider invalid.

If this service has no cache entry of the home address included in the PBU, it will accept any sequence value in the initial PBU from the mobile node.
setup-timeout

The maximum amount of time allowed for session setup.

Product
P-GW
SAEGW

Privilege
Administrator

Syntax

```
setup-timeout seconds
```

```
default setup-timeout
```

```
default
Reset the command value to the default setting of 60.
```

```
seconds
Default: 60 seconds
The maximum amount of time, in seconds, to allow for setup of a session in this service. seconds must be an integer value from 1 through 100000.
```

Usage

Use this command to set the maximum amount of time allowed for setting up a session.

Example

The following command sets the maximum time allowed for setting up a session to 5 minutes (300 seconds):

```
setup-timeout 300
```
**signalling-packets**

Enables the DSCP marking feature for IP headers carrying outgoing signalling packets.

**Product**
P-GW
SAEGW

**Privilege**
Administrator

**Syntax**

```
signalling-packets ip-header-dscp value

{ default | no } signalling-packets ip-header-dscp
```

- **default**
  Restores the specified parameter to its default setting of 0x0.

- **no**
  Disables the specified functionality.

- **ip-header-dscp value**
  Used to configure the QoS Differentiated Services Code Point (DSCP) marking for IP header encapsulation. 
  *value*: Represents the DSCP setting. It represents the first six most-significant bits of the ToS field. It can be configured to any hex value from 0x0 through 0x3F. Default is 0x0.

**Usage**

Use this command to enable or disable the DSCP marking feature for IP headers carrying outgoing signalling packets. DSCP marking is disabled by default.

**Example**

The following command configures the HSGW service to support DSCP marking for IP headers carrying outgoing signalling packets:

```
signalling-packets ip-header-dscp 0x21
```
simul-bindings

Specifies the maximum number of “care-of” addresses that can simultaneously be bound for the same user as identified by NAI and Home address.

Product
P-GW
SAEGW

Privilege
Administrator

Syntax

simul-bindings number

default simul-bindings

default

Resets the command value to the default setting of 1.

number

Default: 1
Configures maximum number of “care of” addresses that can be simultaneously bound for the same user as identified by their NAI and home address. \textit{number} must be an integer value between 1 and 3.

Usage
Per RFC 5213 (and 3775), the LMA service creates a binding record known as a binding cache entry (BCE) for each subscriber session it is facilitating. Each BCE is associated with a care-of address. As the mobile node roams, it is possible that the session will be associated with a new care of address. Typically, the LMA service will delete an old binding and create a new one when the information in the registration request changes. However, the mobile node could request that the LMA maintains previously stored BCEs. This command allows you to configure the maximum number of BCEs that can be stored per subscriber if more than one is requested.

Example
The following command configures the service to support up to 2 addresses per subscriber:

\texttt{simul-bindings 2}
standalone

Configures the LMA service to start in standalone mode.

**Product**
P-GW
SAEGW

**Privilege**
Administrator

**Syntax**

```
[ default | no ] standalone
```

- **default**
  Resets the command value to the default setting.

- **no**
  Disables the feature.

**Usage**

Use this command to start the LMA service in standalone mode.
**timestamp-option-validation**

Configures validation of timestamp option in binding update messages. By default, timestamp option is mandatory.

**Product**
- P-GW
- SAEGW

**Privilege**
Administrator

**Syntax**

```
[ default | no ] timestamp-option-validation
```

- **default**
  Resets the command value to the default setting of enabled.

- **no**
  Disables the feature.

**Usage**

Use this command to configure timestamp validation in binding update messages.
timestamp-replay-protection

Designates timestamp replay protection scheme as per RFC 4285.

**Product**
P-GW
SAEGW

**Privilege**
Administrator

**Syntax**

```
timestamp-replay-protection tolerance seconds
{ default | no } timestamp-replay-protection tolerance
```

<table>
<thead>
<tr>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resets the command value to the default setting of 7.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>no</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disables the timestamp replay protection feature.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>tolerance seconds</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default: 7</td>
</tr>
<tr>
<td>Defines the acceptable difference in timing (between timestamps) before rejecting packet, in seconds.</td>
</tr>
<tr>
<td>seconds must be an integer value between 0 and 65535.</td>
</tr>
</tbody>
</table>

**Usage**

Use this command to define the acceptable difference in timing (between timestamps) before rejecting packet.

**Example**

The following command sets the acceptable difference for timestamps to 10 seconds:

```
timestamp-replay-protection tolerance 10
```
Chapter 189
LNS Service Configuration Mode Commands

The LNS Service Configuration Mode is used to create and manage L2TP services within contexts on the system. L2TP Network Server (LNS) services facilitate tunneling with peer L2TP Access Concentrators (LACs).

Mode

Exec > Global Configuration > Context Configuration > LNS Service Configuration

configure > context context_name > lns-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ns-service)#

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
aaa accounting

Enables the sending of authentication, authorization, and accounting (AAA) accounting information by the LNS.

Product
PDSN
GGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > LNS Service Configuration
configure > context context_name > lns-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-lns-service)#

Syntax

aaa accounting [ roaming ]

[ no ] aaa accounting

no
Disables this option.

roaming

Enables the sending of AAA accounting information by the LNS only for roaming subscribers.

Usage
Use this command to enable the sending of AAA accounting information by the LNS. By default this is enabled.

Example

The following command enables the sending of AAA accounting information by the LNS:

    aaa accounting
**authentication**

Configures the type of subscriber authentication for PPP sessions terminated at the current LNS.

**Product**
- PDSN
- GGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > LNS Service Configuration

```
configure > context context_name > lns-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-lns-service)#
```

**Syntax**

```
authentication { [ allow-noauth ] [ chap chap_priority ] [ mschap mschap_priority ] [ pap pap_priority ] } | msid-auth }
```

---

**allow-noauth**

Default: Disabled

Configures the LNS to allow PPP sessions access even though they have not been authenticated. This command issued by itself causes the LNS not to attempt authentication for any PPP sessions.

When the `allow-noauth` option is used in conjunction with commands specifying other authentication protocols and priorities to use, then if attempts to use those protocols fail, the system treats the `allow-noauth` option as the lowest priority.

If no authentication is allowed, the system constructs an Network Access Identifier (NAI) to provide accounting records for the PPP session.

---

**chap chap_priority**

Default: 1

Configures the LNS to attempt to use Challenge Handshake Authentication Protocol (CHAP) to authenticate the PPP session.

A `chap_priority` must be specified in conjunction with this option. Priorities specify which authentication protocol should be attempted first, second, third and so on.

`chap_priority` must be an integer from 1 through 1000. The lower the integer, the higher the preference. CHAP is enabled by default as the highest preference.

---

**mschap mschap_priority**

Default: Disabled

Configures the LNS to attempt to use the Microsoft Challenge Handshake Authentication Protocol (MSCHAP) to authenticate the PPP session.

A `mschap_priority` must be specified in conjunction with this option. Priorities specify which authentication protocol should be attempted first, second, third and so on.

`mschap_priority` must be an integer from 1 through 1000. The lower the integer, the higher the preference.
**pap pap_priority**

Default: 2

This option configures the LNS to attempt to use the Password Authentication Protocol (PAP) to authenticate the PPP session. A *pap_priority* must be specified in conjunction with this option. Priorities specify which authentication protocol should be attempted first, second, third and so on. *pap_priority* must be an integer from 1 through 1000. The lower the integer, the higher the preference. PAP is enabled by default as the second highest preference.

**msid-auth**

Default: Disabled

This option configures the LNS to attempt to authenticate the PPP session based on the Mobile Station Identity (MSID).

**Usage**

Use to specify how the LNS service should handle authentication and what protocols to use. The flexibility is given to configure this option to accommodate the fact that not every mobile will implement the same authentication protocols.

By default LNS authentication options are set as follows:
- *allow-noauth* disabled
- *chap* enabled with a priority of 1
- *mschap* disabled
- *msid-auth* disabled
- *pap* enabled with a priority of 2

**Important:** At least one of the keywords must be used to complete the command.

**Example**

The following command configures the LNS service to allow no authentication for PPP sessions and would perform accounting using the default NAI-construct of *username*@*domain*:

```
authentication allow-noauth
```

The following command configures the system to attempt authentication first using CHAP, then MSCHAP, and finally PAP. If the allow-noauth command was also issued, when all attempts to authenticate the subscriber using these protocols failed, then the subscriber would be allowed access:

```
authentication chap 1 mschap 2 pap 3
```
avp map called-number apn

This command maps an incoming Attribute Value Pair (AVP) to a GGSN Access Point Name (APN) for authentication and authorization of the call.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > LNS Service Configuration

```
configure > context context_name > lns-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ins-service)#
```

**Syntax**

```
[ default | no ] avp map called-number apn
```

- **default**
  Disables mapping.

- **no**
  Disables mapping.

**Usage**
For LNS calls received through a LAC, the ICRQ message includes an APN name in the Called Number AVP. This mapping function enables a GGSN system to provide RADIUS authentication/authorization via a defined APN in place of an LNS configuration. If the mapped APN has not been defined within the GGSN configuration then the call will be rejected.

**Example**
Enter the following command to enable mapping:

```
   avp map called-number apn
```

Enter the following command to disable mapping:

```
   no avp map called-number apn
```
bind

This command assigns the IP address of an interface in the current context to the LNS service.

Product

- PDSN
- GGSN

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > Context Configuration > LNS Service Configuration
configure > context context_name > lns-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-lns-service)#

Syntax

bind ip_address [ max-subscribers max_value ]
no bind ip_address

no

Unassign, or unbind, the local end point to the LNS service.

ip_address

Specifies the IP address of an interface in the current context. This must be a valid IP address entered using IPV4 dotted-decimal notation.

max-subscribers max_value

Default: 10000
Specifies the maximum number of subscribers that can be connected to this service at any time. max_value must be an integer from 1 through 2500000.

Usage

Use this command to bind the IP address of an interface in the current context to the LNS service.

Example

The following command binds the current context interface IP address 192.168.100.10 to the current LNS service:

bind 192.168.100.10

The following command removes the binding of the IP address from the LNS service:

no bind
data sequence-number

Enables data sequence numbering for sessions that use the current LNS service. Data sequence numbering is enabled by default.

**Product**
PDSN
GGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > LNS Service Configuration

```
configure > context context_name > lns-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-lns-service)#
```

**Syntax**

```
[ no ] data sequence-number
```

- **no**

  Disables data sequence numbering for sessions.

**Usage**

An L2TP data packet header has an optional data sequence numbers field. The data sequence number may be used to ensure ordered delivery of data packets. This command is used to re-enable or disable the use of the data sequence numbers for data packets.

**Example**

Use the following command to disable the use of data sequence numbering:

```
no data sequence-number
```

Use the following command to re-enable data sequence numbering:

```
data sequence-number
```
**default**

This command sets the specified LAC service parameter to its default value or setting.

**Product**
- PDSN
- GGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > LNS Service Configuration

```
configure > context context_name > lns-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-lns-service)#
```

**Syntax**

```
default { authentication | data sequence-number | ip source-violation | keepalive-interval | load-balancing | local-receive-window | max-retransmission | max-session-per-tunnel | max-tunnel-challenge-length | max-tunnels | proxy-lcp-authentication | retransmission-timeout-first | retransmission-timeout-max | setup-timeout| single-port-mode | subscriber| trap all tunnel-authentication}
```

---

**authentication**

Sets the authentication parameters for PPP sessions to the following defaults:
- allow-noauth disabled
- chap enabled with a priority of 1
- mschap disabled
- msid-auth disabled
- pap enabled with a priority of 2

---

**data sequence-number**

Enables data sequence numbering for sessions.

---

**ip source-violation**

Sets the IP source violation parameters to the following defaults:
- drop-limit 10
- period 120 seconds
- reneg-limit 5

---

**keepalive-interval**

Sets the interval for send L2TP Hello keepalive if there is no control or data transactions to the default value of 60 seconds.
**local-receive-window**
Sets the window size to be used for the local side for the reliable control transport to the default of 4.

**max-retransmission**
Sets the maximum number of retransmissions to the default of 5.

**max-session-per-tunnel**
Sets the maximum number of sessions per tunnel at any point in time to the default of 65535.

**max-tunnel-challenge-length**
Sets the maximum length of the tunnel challenge to the default of 16 bytes.

**max-tunnels**
Sets the maximum number of tunnels for this service to the default of 32000.

**proxy-lcp-authentication**
Sets sending of proxy LCP authentication parameters to the LNS to the default state of enabled.

**retransmission-timeout-first**
Sets the first retransmit interval to the default of 1 second.

**retransmission-timeout-max**
Sets the maximum retransmit interval to the default of 8 seconds.

**setup-timeout**
Sets the maximum time allowed for session setup to the default of 60 seconds.

**single-port-mode**
Disables assignment of only port 1107 for incoming tunnels and allows dynamic assignment of ports.

**subscriber**
Sets the name of the default subscriber configuration to use.

**tunnel-authentication**
Sets tunnel authentication to the default state of enabled.

**trap all**
Generates all supported SNMP traps.

**tunnel-switching**
Sets the ability of the LNS to create subsequent tunnels to the default of enabled.
Usage

Use the default command to set LAC service parameters to their default states.

Example

Use the following command to set the keepalive interval to the default value of 60 seconds:

```
default keepalive-interval
```

Use the following command to set the maximum number of sessions per tunnel to the default value of 512:

```
default max-session-per-tunnel
```
end

Exits the current configuration mode and returns to the Exec mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

`end`

**Usage**

Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Use this command to return to the parent configuration mode.
**ip source-violation**

This command configures settings related to IP source-violation detection.

**Product**
- PDSN
- GGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > LNS Service Configuration
configure > context context_name > lns-service service_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-lns-service)#
```

**Syntax**

```
ip source-violation { clear-on-valid-packet | drop-limit num | period secs | reneg-limit num }
no ip source-violation clear-on-valid-packet
```

---

**clear-on-valid-packet**
Default: disabled
Configures the service to reset the reneg-limit and drop-limit counters after receipt of a properly addressed packet.

**drop-limit num**
Default: 10
Sets the number of allowed source violations within a detection period before forcing a call disconnect. If `num` is not specified, the value is set to the default. `num` can be an integer from 1 through 1000000.

**period secs**
Default: 120
The length of time (in seconds) for a source violation detection period to last. drop-limit and reneg-limit counters are decremented each time this value is reached.

The counters are decremented in this manner: reneg-limit counter is reduced by one (1) each time the period value is reached until the counter is zero (0); drop-limit counter is halved each time the period value is reached until the counter is zero (0). If `secs` is not specified, the value is set to the default. `secs` can be an integer from 1 through 1000000.

**reneg-limit num**
Default: 5
Sets the number of allowed source violations within a detection period before forcing a PPP renegotiation. If `num` is not specified, the value is set to the default.
**Usage**

This function allows the operator to configure a network to prevent problems such as when a user gets handed back and forth between two PDSNs a number of times during a handoff scenario. When a subscriber packet is received with a source address violation, the system increments both the IP source-violation reneg-limit and drop-limit counters and starts the timer for the IP-source violation period. Every subsequent packet received with a bad source address during the IP-source violation period causes the reneg-limit and drop-limit counters to increment.

For example, if reneg-limit is set to 5, the system allows five packets with a bad source address (source violations), but on the fifth packet, it re-negotiates PPP. If the drop-limit is set to 10, the above process of receiving five source violations and renegotiating PPP occurs only once. After the second 5-source violation, the call is dropped. The period timer continues to count throughout this process.

If at any time before the call is dropped, the configured source-violation period is exceeded, the counters for drop-limit is decremented by half and reneg-limit is decremented by 1. See period definition above.

**Example**

To set the maximum number of source violations before dropping a call to 100, enter the following command:

```
ip source-violation drop-limit 100
```
**keepalive-interval**

This command specifies the amount of time to wait before sending a Hello keepalive message.

**Product**
- PDSN
- GGSN

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration > Context Configuration > LNS Service Configuration

```
configure > context context_name > ins-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ins-service)#
```

**Syntax**

```
keepalive-interval seconds

no keepalive-interval
```

- **no**
  - Disables the generation of Hello keepalive messages on the tunnel.

- **seconds**
  - Default: 60
  - Specifies the number of seconds to wait before sending a Hello keepalive message as an integer from 30 through 2147483648.

**Usage**

Use this command to set the amount of time to wait before sending a Hello keepalive message or disable the generation of Hello keepalive messages completely. A keepalive mechanism is employed by L2TP in order to differentiate tunnel outages from extended periods of no control or data activity on a tunnel. This is accomplished by injecting Hello control messages after a specified period of time has elapsed since the last data or control message was received on a tunnel. As for any other control message, if the Hello message is not reliably delivered then the tunnel is declared down and is reset. The transport reset mechanism along with the injection of Hello messages ensures that a connectivity failure between the LNS and the LAC is detected at both ends of a tunnel.

**Example**

Use the following command to set the Hello keepalive message interval to 120 seconds:

```
keepalive-interval 120
```

Use the following command to disable the generation of Hello keepalive messages:

```
no keepalive-interval
```
local-receive-window

Specifies the number of control messages the remote peer LAC can send before waiting for an acknowledgement.

**Product**
- PDSN
- GGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > LNS Service Configuration

```bash
configure > context context_name > lns-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-lns-service)#
```

**Syntax**

```bash
local-receive-window integer
```

- **integer**
  - Default: 4
  - Specifies the number of control messages to send before waiting for an acknowledgement as an integer from 1 through 256.

**Usage**

Use this command to set the size of the control message receive window being offered to the remote peer LAC. The remote peer LAC may send the specified number of control messages before it must wait for an acknowledgment.

**Example**

The following command sets the local receive window to 10 control messages:

```bash
local-receive-window 10
```
max-retransmission

Sets the maximum number of retransmissions of a control message to a peer before the tunnel and all sessions within it are cleared.

Product
- PDSN
- GGSN

Privilege
- Security Administrator, Administrator

Mode
- Exec > Global Configuration > Context Configuration > LNS Service Configuration
- configure > context context_name > lns-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-lns-service)#

Syntax

```
max-retransmission integer
```

- `integer`

  Default: 5
  Specifies the maximum number of retransmissions of a control message to a peer as an integer from 1 through 10.

Usage

Each tunnel maintains a queue of control messages to be transmitted to its peer. After a period of time passes without acknowledgement, a message is retransmitted. Each subsequent retransmission of a message employs an exponential backoff interval. For example; if the first retransmission occurs after 1 second, the next retransmission occurs after 2 seconds has elapsed, then the next after 4 seconds. If no peer response is detected after the number of retransmissions set by this command, the tunnel and all sessions within are cleared.

Use this command to set the maximum number of retransmissions that the LAC service sends before closing the tunnel and all sessions within it.

Example

The following command sets the maximum number of retransmissions of a control message to a peer to 7:

```
max-retransmissions 7
```
max-session-per-tunnel

Sets the maximum number of sessions that can be facilitated by a single tunnel at any time.

**Product**
PDSN
GGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > LNS Service Configuration

```
configure > context context_name > lns-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-lns-service)#
```

**Syntax**

```
max-sessions-per-tunnel integer
```

integer
Default: 512
Specifies the maximum number of sessions as an integer from 1 through 65535.

**Usage**
Use this command to set the maximum number of sessions you want to allow in a tunnel.

**Example**
The following command sets the maximum number of sessions in a tunnel to 5000:

```
max-sessions-per-tunnel 5000
```
**max-tunnel-challenge-length**

Sets the maximum length of the tunnel challenge in bytes. The challenge is used for authentication purposes during tunnel creation.

**Product**
- PDSN
- GGSN

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration > Context Configuration > LNS Service Configuration

```
configure > context context_name > lns-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-lns-service)#
```

**Syntax**

```
max-tunnel-challenge-length bytes
```

- `bytes` - Specifies the number of bytes to set the maximum length of the tunnel challenge as an integer from 4 through 32.

  - Default: 16

**Usage**

Use this command to set the maximum length, in bytes, for the tunnel challenge that is used during tunnel creation.

**Example**

The following command sets the maximum length of the tunnel challenge to 32 bytes:

```
max-tunnel-challenge-length 32
```
max-tunnels

The maximum number of tunnels that the current LNS service can support.

**Product**
- PDSN
- GGSN

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration > Context Configuration > LNS Service Configuration
- `configure > context context_name > lns-service service_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-lns-service)#
```

**Syntax**

```
max-tunnels integer
```

- `integer`
  - Default: 32000
  - Specifies the maximum number of tunnels as an integer from 1 through 32000.

**Usage**

Use this command to set the maximum number tunnels that this LNS service can support at any one time.

**Example**

Use the following command to set the maximum number of tunnels for the current LNS service to 20000:

```
max-tunnels 20000
```
nai-construction domain

Designates the alias domain name to use for Network Access Identifier (NAI) construction.

Product

PDSN
GGSN

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > Context Configuration > LNS Service Configuration
configure > context context_name > lns-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-lns-service)#

Syntax

nai-construction domain domain_name { @ | % | - | \ | # | / }

no nai-construction domain

no

Deletes the NAI construction domain alias.

domain_name { @ | % | - | \ | # | / }

Specifies the desired domain name alias followed immediately by a separator from the valid list. domain_name must be an alphanumeric string of from 1 through 79 characters.

Usage

Use this command to specify the domain alias and separator to use for NAI construction. The specified domain name must be followed by a valid separator (@ | % | - | \ | # | /).

Example

To specify a domain alias of mydomain@ with a separator of @, enter the following command:

    nai-construction domain mydomain@

To delete the current setting for the NAI construction domain alias, enter the following command:

    no nai-construction domain
newcall

Configures new call related behavior.

Product

PDSN
GGSN

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > Context Configuration > LNS Service Configuration

configure > context context_name > lns-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-lns-service)#

Syntax

newcall duplicate-subscriber-requested-address { accept | reject }

default newcall duplicate-subscriber-requested-address

---

default

Sets or restores default value assigned for specified parameter

duplicate-subscriber-requested-address

Configures how duplicate sessions with same address request are handled.

Example

The following command configures new call with duplicate address request to accept:

```
newcall duplicate-subscriber-requested-address accept
```
peer-lac

Adds a peer LAC address for the current LNS service. Up to eight peer LACs can be configured for each LNS service.

**Product**
PDSN
GGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > LNS Service Configuration

`configure > context context_name > lns-service service_name`

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-Ins-service)#`

**Syntax**

```
peer-lac { ip_address | ip_address/mask } [ encrypted ] secret secret [ description text ]
```

**no peer-lac ip_address**

```
no peer-lac ip_address
```

Deletes the peer LAC IP address specified by `ip_address`. `ip_address` must be entered using IPv4 dotted-decimal notation.

**ip_address**

The IP address of a specific peer LAC for the current LNS service. `ip_address` must be entered using IPv4 dotted-decimal notation.

**ip_address/mask**

A network prefix and mask enabling communication with a group of peer LACs. `ip_address` is the network prefix expressed in IPv4 dotted-decimal notation. `mask` is the number of bits that defines the prefix.

**encrypted**

Specifies the encrypted shared key between the LAC and the LNS service. This keyword is intended only for use by the system while saving configuration scripts. The system displays the encrypted keyword in the configuration file as a flag that the variable following the secret keyword is the encrypted version of the plain text secret. Only the encrypted secret is saved as part of the configuration file.

**secret secret**

Designates the secret which is shared between the current LNS service and the peer LAC. `secret` must be an alphanumeric string of 1 through 127 characters that is case-sensitive.
**description text**

Specifies the descriptive text to use to describe the specified peer LAC. text must be an alphanumeric string of 0 through 79 characters.

**Usage**

Use this command to add a peer LAC address for the current LNS service. Specific peer LACs can be configured by specifying their individual IP addresses. In addition, to simplify configuration, communication with a group of peer LACs can be enabled by specifying a network prefix and a mask.

**Example**

The following command adds a peer LAC to the current LNS service with the IP address of 10.10.10.100, and specifies the shared secret to be 1b34nnf5d:

```
peer-lac 10.10.10.100 secret 1b34nnf5d
```

The following command enables communication with up to 16 peer LACs on the 192.168.1.0 network each having a secret of abc123:

```
peer-lac 92.168.1.0/28 secret abc123
```

The following command removes the peer LAC with the IP address of 10.10.10.200 for the current LNS service:

```
no peer-lac 10.10.10.200
```
proxy-lcp-authentication

Enables/disables proxy LCP authentication.

Product
- PDSN
- GGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > LNS Service Configuration

configure > context context_name > lns-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-lns-service)#

Syntax

[ no ] proxy-lcp-authentication

no
Disables the processing of proxy LCP authentication parameters from the LAC.

proxy-lcp-authentication
Default: Enabled
Enables the processing proxy LCP authentication parameters from the LAC.

Usage
When enabled, if proxy LCP authentication parameters are received from the LAC and are acceptable, the LNS resumes the PPP session from the authentication phase and goes to the IPCP phase.
When disabled, PPP is always started from the LCP phase, ignoring and discarding any proxy LCP authentication parameters received from the LAC. Disable this feature in situations where accept proxy LCP Auth AVPs that the peer LAC sends should not be expected.

Example
Use the following command to disable the processing of proxy LCP authentication parameters from the LAC:

    no proxy-lcp-authentication

Use the following command to re-enable the processing of proxy LCP authentication parameters from the LAC:

    proxy-lcp-authentication
retransmission-timeout-first

Configures the initial timeout for the retransmission of control messages to the peer LAC.

**Product**
- PDSN
- GGSN

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration > Context Configuration > LNS Service Configuration
- configure > context context_name > lns-service service_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-lns-service)#
```

**Syntax**

```
retransmission-timeout-first integer
```

- `integer`
  
Default: 1

Specifies the amount of time (in seconds) to wait before sending the first control message retransmission. This value is an integer from 1 through 100.

**Usage**

Each tunnel maintains a queue of control messages to transmit to its peer. After a period of time passes without acknowledgement, a message is retransmitted.

**Example**

The following command sets the initial retransmission timeout to 3 seconds:

```
retransmission-timeout-first 3
```
retransmission-timeout-max

Configures the maximum amount of time that can elapse before retransmitting control messages to the peer LAC.

Product
- PDSN
- GGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > LNS Service Configuration
configure > context context_name > lns-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ins-service)#

Syntax

retransmission-timeout-max integer

integer
Default: 8
Specifies the maximum time (in seconds) to wait before retransmitting control messages. If this limit is reached, the tunnel, and all sessions within it, is cleared. This value is an integer from 1 through 100.

Usage
Each tunnel maintains a queue of control messages to transmit to its peer. After a period of time passes without acknowledgement, a message is retransmitted. Each subsequent retransmission of a message employs an exponential backoff interval. For example; if the first retransmission occurs after 1 second, the next retransmission occurs after 2 seconds has elapsed, then the next after 4 seconds. This continues until the limit set by this command is reached. If this limit is reached, the tunnel, the tunnel, and all sessions within it, is cleared.

Example
Use the following command to set the maximum retransmission time-out to 10 seconds:

retransmission-timeout-max 10
setup-timeout

Configures the maximum amount of time, in seconds, allowed for session setup.

**Product**
- PDSN
- GGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > LNS Service Configuration

```
configure > context context_name > lns-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-lns-service)#
```

**Syntax**

```
setup-timeout seconds
```

- `seconds`

Default: 60
- Specifies the maximum time (in seconds) to wait for the setup of a session. `seconds` must be an integer from 1 through 100000.

**Usage**

This command controls the amount of time allowed for tunnel establishment with a peer LAC. If this timer is exceeded the tunnel setup is aborted.

**Example**

The following command configures a maximum setup time of 120 seconds:

```
setup-timeout 120
```
single-port-mode

When enabled, this command sets the LNS to use only the default local UDP port (port 1701) for the life of a tunnel.

Product
PDSN
GGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > LNS Service Configuration

Syntax

[ default | no ] single-port-mode

no
Disable single port mode

Usage
Use this command to control the L2TP LNS tunnel local UDP port assignment mode. If single-port-mode is enabled, the LNS-service uses the standard UDP port (port 1701) for the life of the incoming tunnel. Otherwise, it assigns a new local UDP port number for a tunnel when it responds to a tunnel create request received on the standard port number. This is done for load distributing the tunnel processing between multiple tasks within the system to increase the capacity and performance. Even though all L2TP LACs are required to support such dynamic port assignments during tunnel establishments, there exist some LACs that do not support port assignment other than port 1701. This single-port-mode feature can be enabled to support such LAC peers. This configuration must be applied for the LNS-Service before the bind command is executed.

Example

The following command enables single port mode for the current LNS service:

    single-port-mode
**trap**

This command generates SNMP traps.

**Product**

PDSN

GGSN

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > LNS Service Configuration

```
configure > context context_name > lns-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-lns-service)#
```

**Syntax**

```
[ no ] trap all
```

no

Disables SNMP traps.

**Usage**

Use this command to enable/disable all supported SNMP traps.

**Example**

To enable all supported SNMP traps, enter the following command;

```
trap all
```
tunnel-authentication

Enables/disables L2TP tunnel authentication for the LNS service.

Product
PDSN
GGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > LNS Service Configuration

configure > context context_name > lns-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-lns-service)#

Syntax

[ no ] tunnel-authentication

no

Disables tunnel authentication
Tunnel authentication is enabled by default.

Usage
When tunnel authentication is enabled, a configured shared secret is used to ensure that the LNS service is communicating with an authorized peer LAC. The shared secret is configured by the peer-lac command, the tunnel l2tp command in the Subscriber Configuration mode, or the Tunnel-Password attribute in the subscribers RADIUS profile.

Example
To disable tunnel authentication, use the following command:

    no tunnel-authentication

To re-enable tunnel authentication, use the following command:

    tunnel-authentication
tunnel-switching

Enables or disables the LNS service from creating tunnels to another LAC for an existing tunnel.

**Product**
- PDSN
- GGSN

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration > Context Configuration > LNS Service Configuration
- `configure > context context_name > lns-service service_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ns-service)#
```

**Syntax**

```
[ no ] tunnel-switching
```

- `no`
  - Disable tunnel switching.
  - Tunnel switching is enabled by default.

**Usage**

Tunnel switching is when the LNS has a tunnel connected to a LAC and creates a tunnel to a different LAC and routes the data from the original LAC through the new tunnel to the other LAC.

**Example**

To disable tunnel switching in the LNS, enter the following command;

```
no tunnel-switching
```
Chapter 190
Local Policy Actiondef Configuration Mode Commands

The Local Policy Actiondef Configuration Mode is used to define the action definitions to be used for local QoS policies.

Mode

Exec > Global Configuration > Local Policy Service Configuration > Local Policy Actiondef Configuration

configure > local-policy-service service_name > actiondef actiondef_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-local-policy-actiondef)#

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
**action**

This command configures the action priority for an actiondef.

**Product**

P-GW  
SAEGW  

**Privilege**

Security Administrator, Administrator  

**Mode**

Exec > Global Configuration > Local Policy Service Configuration > Local Policy Actiondef Configuration  
configure > local-policy-service service_name > actiondef actiondef_name  

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-local-policy-actiondef)＃
```

**Syntax**

```
action priority priority action_name arguments
no action priority priority
```

---

### priority  priority

Specifies a priority for the specified action.  
**priority** must be a unique integer from 1 to 2048.

```
action_name arguments
```

The following actions are supported. **arguments** specify a set of parameters to be used when invoking the action.

- **activate-ambr uplink bandwidth downlink bandwidth**
  
  Sets the aggregated maximum bit rate (AMBR) for the APN.  
  Configures uplink and downlink bandwidth. **bandwidth** must be an integer from 1 to 1000000000.

- **activate-flow-detection { initiation | termination } ruledef ruledef_name**
  
  Detects a flow and takes action.  
  **initiation ruledef**: Checks for flow initiation and adds a rule definition.  
  **termination ruledef**: Checks for flow termination and adds a rule definition.  
  **ruledef_name** must be an existing ruledef.

- **activate-policy-group**
  
  This keyword is not supported in this release.

- **activate-rule name rule_name**
  
  Activates a rule within ECS rulebase for a subscriber.  
  **rule_name** must be an existing rule within this local QoS policy service expressed as an alphanumeric string of 1 through 63 characters.
• activate-rulebase name rulebase_name
  Associates the session with a specific rulebase.
  rulebase_name must be an existing rulebase within this local QoS policy service expressed as an alphanumeric string of 1 through 63 characters.

• allow-requested-qos
  Allow a specific UE initiated QoS request.

• allow-session
  Allows the session to continue.

• create-bearer qci value arp value uplink-mbr mbr_rate downlink-mbr mbr_rate [ uplink-gbr gbr_rate ] downlink-gbr gbr_rate
  Creates a bearer with a specific QCI and BANDWIDTH.
  qci value must be an integer from 1 through 254.
  arp value must be an integer from 1 through 15 (StarOS v12.1 and earlier) or 1 through 127 (StarOS v12.2 and later).
  uplink-mbr: Uplink maximum bitrate. mbr_rate must be an integer from 1 through 1000000000.
  downlink-mbr: Downlink maximum bitrate. mbr_rate must be an integer from 1 through 1000000000.
  uplink-gbr: Uplink guaranteed bitrate. gbr_rate must be an integer from 1 through 1000000000.
  downlink-gbr: Downlink guaranteed bitrate. gbr_rate must be an integer from 1 through 1000000000.

• deactivate-ambr
  Removes AMBR control for the specific session.

• deactivate-flow-detection { initiation | termination } ruledef ruledef_name
  Deactivates detection of flow and takes action.
  initiation ruledef: Checks for flow initiation and adds a rule definition.
  termination ruledef: Checks for flow termination and adds a rule definition.
  ruledef_name must be an existing ruledef.

• deactivate-policy-group
  This keyword is not supported in this release.

• deactivate-rule name rule_name
  Deactivates a rule within ECS.
  rule_name must be an existing rule within this local QoS policy service expressed as an alphanumeric string of 1 through 63 characters.

• deactivate-rulebase name rulebase_name
  Disassociates the rulebase from a session.
  rulebase_name must be an existing rulebase within this local QoS policy service expressed as an alphanumeric string of 1 through 63 characters.

• default-qos qci value arp value
  Sets the default QoS parameters for the session
**Local Policy Actiondef Configuration Mode Commands**

qci  value must be an integer from 1 through 254.

arp  value must be an integer from 1 through 15 (StarOS v12.1 and earlier) or 1 through 127 (StarOS v12.2 and later).

*delete-bearer qci  value  arp  value*

Deletes a bearer.

qci  value must be an integer from 1 through 254.

arp  value must be an integer from 1 through 15 (StarOS v12.1 and earlier) or 1 through 127 (StarOS v12.2 and later).

*reconnect-to-server*

Reconnects to the PCRF server to handle fallback scenario. That is, when the session falls back to local policy, this action specifies to retry connecting to the PCRF server.

*reject-requested-qos*

Rejects UE QoS resource request.

*retry-count  value*

Retry action. This applies to start-timer/activate-rule/activate-ruledef.

value must be an integer from 0 through 65535.

*start-timer  name  duration  value  retry-count  value*

Starts a named timer. On expiry of this timer, the local policy engine is contacted to initiate the appropriate action, such as termination of a session.

duration  value: Enter a timer duration from 0 through 28800 seconds. A value of 0 can be used to leave the local policy until the subscriber disconnects. Default timer value is 14400 (seconds).

retry-count specifies the maximum number of times the server will be retried before terminating the call.

retry-count  value must be an integer from 0 through 65535. Default retry count is 3.

*stop-timer  name*

Stops the designated timer.

*terminate-session*

Terminates the session.

no action priority  priority

Deletes the specified action.

**Usage**

Use this command to enable the setting of parameters to be used when invoking actions. Actions are a series of operations that are triggered by activated rules.

This command can be entered multiple times to configure multiple actions for an actiondef. The actions are examined in priority order until a match is found and the corresponding action is applied.

**Example**

The following command creates an action to allow a session to continue with priority set to 125:

```
action priority 125 allow-session
```
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Use this command to return to the parent configuration mode.
Chapter 191
Local Policy Eventbase Configuration Mode Commands

The Local Policy Eventbase Configuration Mode is used to configure the events to be used for local QoS policies.

Mode

Exec > Global Configuration > Local Policy Service Configuration > Local Policy Eventbase Configuration
configure > local-policy-service service_name > eventbase eventbase_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-local-policy-eventbase)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
**exit**

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**
Use this command to return to the parent configuration mode.
rule

This command enables the setting of event rules. An event is something that occurs in the system which would trigger a set of actions to take place, such as new-call or rat-change.

Product
P-GW
SAEGW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Local Policy Service Configuration > Local Policy Eventbase Configuration
configure > local-policy-service service_name > eventbase eventbase_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-local-policy-eventbase)#

Syntax

```
rule priority priority [ event list_of_events ] ruledef ruledef_name actiondef actiondef_name [ continue ]

no rule priority priority
```

<table>
<thead>
<tr>
<th>priority priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies a priority for the specified rule.</td>
</tr>
<tr>
<td>priority must be unique and an integer from 1 to 2048.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>event list_of_events</th>
</tr>
</thead>
<tbody>
<tr>
<td>The event is defined by any of the following events. Upon triggering the event, the rules specified in the eventbase are executed.</td>
</tr>
<tr>
<td>•default-qos-change: The event is triggered as a result of a default QoS change.</td>
</tr>
<tr>
<td>•fallback: This event is triggered as a result of fallback from PCRF.</td>
</tr>
<tr>
<td>•location-change: The event is triggered as a result of any change relating to location.</td>
</tr>
<tr>
<td>•new-call: This event is initiated when a new call is established.</td>
</tr>
<tr>
<td>•out-of-credit: This event is initiated on out of OCS credit.</td>
</tr>
<tr>
<td>•realloc-of-credit: This event is initiated on OCS reallocation of credit.</td>
</tr>
<tr>
<td>•request-qos: This event is initiated as the result of UE requested QoS.</td>
</tr>
<tr>
<td>•service-flow: The event is triggered as a result of a new service flow being detected for the subscriber.</td>
</tr>
<tr>
<td>•timer-expiry: The event is triggered as a result of the expiry of Local Policy Timer.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ruledef ruledef_name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Associates the rule with a specific ruledef.</td>
</tr>
</tbody>
</table>
ruledef_name must be an existing ruledef within this local QoS policy service.

actiondef actiondef_name
Associates the rule with a specific actiondef. actiondef_name must be an existing actiondef within this local QoS policy service expressed as an alphanumeric string of 1 through 63 characters.

continue
Subsequent rules are also matched; otherwise, rule evaluation is terminated on first match.

no rule priority priority
Deletes the specified rule.

Usage
Use this command to create, configure, or delete event rules. The rules are executed in priority order, and if the rule is matched the action specified in the actiondef is executed. If an event qualifier is associated with a rule, the rule is matched only for that specific event. If a qualifier of continue is present at the end of the rule, the subsequent rules are also matched; otherwise, rule evaluation is terminated on first match. This command can be entered multiple times to configure multiple rules for an eventbase.

Important: A maximum 256 rules are suggested in an eventbase for performance reasons.

Example
The following command creates a rule with priority set to 2 and associated with ruledef rule5 and actiondef action7:

   rule priority 2 ruledef rule5 actiondef action7
Chapter 192
Local Policy Ruledef Configuration Mode Commands

The Local Policy Ruledef Configuration Mode is used to configure the rule definitions to be used for local QoS policies.

Mode
Exec > Global Configuration > Local Policy Service Configuration > Local Policy Ruledef Configuration
configure > local-policy-service service_name > ruledef ruledef_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-local-policy-ruledef)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
**condition**

This command is used to configure the conditions which trigger the ruledef event.

**Product**
- P-GW
- SAEGW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Local Policy Service Configuration > Local Policy Ruledef Configuration

```bash
configure local-policy-service service_name ruledef ruledef_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-local-policy-ruledef)#
```

**Syntax**

```bash
condition priority priority \{ variable \{ eq | ge | gt | le | lt | match | ne | nomatch \} regex | string_value | int_value | set \}

no condition priority priority
```

**priority priority**

Specifies a priority for the specified condition.

**variable**

The following variables are supported:

- **apn**
  The APN associated with the current session expressed as an alphanumeric string of 1 through 63 characters.

- **arp**
  The APN associated with the current session expressed as an integer from 1 through 15.

- **bandwidth**
  Total bandwidth associated with the QCI and ARP value associated with the request, expressed as an integer from 0 through 1000000000.

- **bsid**
  Base Station Identifier associated with the subscriber as expressed as an alphanumeric string of 1 through 63 characters.

- **cause-code**
  Failure Cause Code associated with the subscriber as expressed as an alphanumeric string of 1 through 63 characters.

- **cgi**
Cell Global Identification associated with the subscriber as expressed as an alphanumeric string of 1 through 63 characters.

**Important:** This variable is available only in 15.0 and earlier releases. In 16.0 and later releases, it is deprecated.

- **date**
  Date value to match. <Clock in format YYYYY-MM-DD>

- **day-of-month**
  The day of the month to match the rule to, expressed as an integer from 1 through 31.

- **day-of-week**
  Sunday...Saturday, expressed as an integer from 1 to 7.

- **ecgi**
  E-UTRAN Cell Global Identification associated with the subscriber as expressed as an alphanumeric string of 1 through 63 characters.

**Important:** This variable is available only in 15.0 and earlier releases. In 16.0 and later releases, it is deprecated.

- **imeisv**
  IMEISV of the user equipment expressed as an alphanumeric string of 1 through 63 characters.

- **imsi**
  IMSI associated with the subscriber expressed as an alphanumeric string of 1 through 63 characters.

- **meid**
  MEID associated with the subscriber expressed as an alphanumeric string of 1 through 63 characters.

- **month-of-year**
  Jan, Feb....Dec, expressed as an integer from 1 through 12.

- **msisdn**
  MSISDN associated with the session expressed as an alphanumeric string of 1 through 63 characters.

- **nai**
  NAI associated with the session expressed as an alphanumeric string of 1 through 63 characters.

- **pdn-type**
  Type of PDNs associated with the same APN.
  - **IPV4**: IPv4 PDN Type
  - **IPV4V6**: IPv4v6 PDN Type
  - **IPV6**: IPv6 PDN Type

- **qci**
  QCI associated with the current event expressed as an integer from 1 through 254.

- **radio-access-technology**
Radio access technology associated with the subscriber:

- **cdma-lxrtt**: CDMA 1X RTT radio access technology
- **cdma-evdo**: CDMA-EVDO radio access technology
- **cdma-evdo-reva**: CDMA EVDO REVA radio access technology
- **cdma-other**: Other CDMA radio access technologies
- **ehrpdp**: EHRPD radio access technology
- **eutan**: EUTRAN radio access technology
- **gan**: GAN radio access technology
- **gprs-geran**: GPRS GERAN radio access technology
- **gprs-other**: Other GPRS radio access technology
- **hsapa**: HSPA radio access technology
- **unknown**: Unknown radio access technology
- **wcdma-utran**: WCDMA UTRAN radio access technology
- **wimax**: WiMax radio access technology
- **wireless-lan**: Wireless LAN radio access technology

- **rai**
  
  Routing Area Identification associated with the subscriber as expressed as an alphanumeric string of 1 through 63 characters.

- **sai**
  
  Serving Area Identification associated with the subscriber as expressed as an alphanumeric string of 1 through 63 characters.

**Important**: This variable is available only in 15.0 and earlier releases. In 16.0 and later releases, it is deprecated.

- **serving-node-address**
  
  IP address associated with the current node serving the subscriber entered using IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

- **serving-plmn**
  
  PLMN associated with the current node serving the subscriber expressed as an alphanumeric string of 1 through 63 characters.

- **tai**
  
  Tracking Area Identification associated with the subscriber as expressed as an alphanumeric string of 1 through 63 characters.

**Important**: This variable is available only in 15.0 and earlier releases. In 16.0 and later releases, it is deprecated.

- **time-of-day**
  
  Time associated with the change. <Clock in format HH:mm:ss or HH:mm>
**timer**

Timer name as expressed as an alphanumeric string of 1 through 63 characters.

---

**Important:** This variable is available only in 15.0 and earlier releases. In 16.0 and later releases, it is deprecated.

---

```
| eq | ge | gt | le | lt | match | ne | nomatch |
---|----|----|----|----|-------|----|---------|

**eq:** Operation equal to

**ge:** Operation greater than or equal to

**gt:** Operation greater than

**le:** Operation less than or equal to

**lt:** Operation less than

**match:** Operation match

**ne:** Operation not equal to

**nomatch:** Operation nomatch
```

---

```
no condition priority priority
```

Deletes the specified condition.

---

**Usage**

Use this command to configure the conditions which trigger the ruledef event. A ruledef represents a set of matching conditions. This command can be entered multiple times to configure multiple conditions for a ruledef. The conditions are examined in priority order until a match is found and the corresponding condition is applied.

---

**Example**

The following command creates a condition with priority set to 5 and configured match apn myapn*:

```
condition priority 5 apn match myapn*
```
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

exit

**Usage**
Use this command to return to the parent configuration mode.
The Local Policy Service Configuration Mode is used to configure the local QoS policy for one or more services.

**Important:** A maximum of 16 local QoS policy services are supported.

**Mode**

Exec > Global Configuration > Local Policy Service Configuration

```bash
configure > local-policy-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-local-policy-service)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
actiondef

This command enables creating, configuring, or deleting action definitions for an event.

**Product**

P-GW
SAEGW

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Local Policy Service Configuration

```
configure > local-policy-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-local-policy-service)#
```

**Syntax**

```
actiondef actiondef_name [ -noconfirm ]

no actiondef actiondef_name
```

---

**no**

Deletes the specified actiondef from the local QoS policy service.

```
actiondef_name
```

Specifies name of the actiondef.

*actiondef_name* must be unique within the service expressed as an alphanumeric string of 1 through 63 characters. If the named actiondef does not exist, it is created, and the CLI mode changes to the Local Policy Actiondef Configuration Mode wherein the actiondef can be configured. If the named actiondef already exists, the CLI mode changes to the Local Policy Actiondef Configuration Mode for that actiondef.

---

**-noconfirm**

Specifies that the command must execute without prompting for confirmation.

---

**Usage**

Use this command to create, configure, or delete an actiondef. The actiondef configuration is used to configure the action definitions for an event. The event ruledef will have one or more rules and associated action(s).

This command can be entered multiple times to specify multiple actiondefs.

---

**Important:** A maximum of 256 actiondefs are suggested in a local QoS policy service for performance reasons. An actiondef can be referenced by multiple eventbases.
Entering this command results in the following prompt:

```
[context_name]hostname(config-local-policy-actiondef)#
```

Local Policy Actiondef Configuration Mode commands are defined in the *Local Policy Actiondef Configuration Mode Commands* chapter.

**Example**

The following command creates an actiondef named `actiondef1` and enters the Local Policy Actiondef Configuration Mode:

```
actiondef actiondef1
```
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
```
end
```

**Usage**
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Use this command to return to the parent configuration mode.
eventbase

This command enables creating, configuring, or deleting an eventbase.

**Product**

P-GW
SAEGW

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Local Policy Service Configuration
configure > local-policy-service service_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-local-policy-service)#
```

**Syntax**

```
eventbase eventbase_name [ -noconfirm ]
no eventbase eventbase_name
```

-no

Deletes the specified eventbase from the local QoS policy service.

```
eventbase_name
```

Specifies name of the eventbase.

`eventbase_name` must be unique within the service expressed as an alphanumeric string of 1 through 63 characters.

**Important:** Currently, only one eventbase is supported, and it must be named “default”.

If the named eventbase does not exist, it is created, and the CLI mode changes to the Local Policy Eventbase Configuration Mode wherein the eventbase can be configured.

If the named eventbase already exists, the CLI mode changes to the Local Policy Eventbase Configuration Mode for that eventbase.

-noconfirm

Specifies that the command must execute without prompting for confirmation.

**Usage**

Use this command to create, configure, or delete an eventbase.

Entering this command results in the following prompt:

```
[context_name]host_name(config-local-policy-eventbase)#
```
Local Policy Eventbase Configuration Mode commands are defined in the *Local Policy Eventbase Configuration Mode Commands* chapter.

**Example**

The following command creates an eventbase named *default* and enters the Local Policy Eventbase Configuration Mode:

```
eventbase default
```
**ruledef**

This command enables creating, configuring, or deleting a rule definition.

**Product**

P-GW
SAEGW

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Local Policy Service Configuration

`configure > local-policy-service service_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-local-policy-service)#
```

**Syntax**

```
ruledef  ruledef_name  [  -noconfirm  ]

no  ruledef  ruledef_name
```

- **no**
  
  Deletes the specified ruledef from the local QoS policy service.

  ```
  ruledef_name
  ```

  Specifies name of the ruledef.

  `ruledef_name` must be unique within the service expressed as an alphanumeric string of 1 through 63 characters.

  If the named ruledef does not exist, it is created, and the CLI mode changes to the Local Policy Ruledef Configuration Mode wherein the ruledef can be configured.

  If the named ruledef already exists, the CLI mode changes to the Local Policy Ruledef Configuration Mode for that ruledef.

  ```
  -noconfirm
  ```

  Specifies that the command must execute without prompting for confirmation.

**Usage**

Use this command to create, configure, or delete a ruledef. A ruledef represents a set of matching conditions. This command can be entered multiple times to specify multiple ruledefs.

**Important:** A maximum 256 ruledefs are suggested in a local QoS policy service for performance reasons.

Entering this command results in the following prompt:

```
[context_name]host_name(config-local-policy-ruledef)#
```
Local Policy Ruledef Configuration Mode commands are defined in the *Local Policy Ruledef Configuration Mode Commands* chapter.

**Example**

The following command creates a ruledef named `rule5` and enters the Local Policy Ruledef Configuration Mode:

```
ruledef rule5
```
Chapter 194
Location Service Configuration Mode Commands

The Location Service Configuration Mode is used to manage Location Services (LCS). Using LCS, the system (MME or SGSN) can collect and use or share location (geographical position) information for connected UEs in support of a variety of location services.

Mode

Exec > Global Configuration > Context Configuration > Location Service Configuration

configure > context context_name > location-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-location-service)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
associate

Associates or disassociates supportive interfaces or services with this location service instance.

Product
MME
SGSN

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > Location Service Configuration
configure > context context_name > location-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-location-service)#

Syntax

associate { diameter { dictionary standard | endpoint } | map-service map_svc_name }
default associate diameter dictionary
no associate { diameter endpoint | map-service }

---

default
Returns the command to its default value of ‘standard’.

---

no
Disassociates a previously associated interface or service with this location service.

---

diameter dictionary standard
Associates a Diameter dictionary with this location service. The standard dictionary contains definitions per the 3GPP definition.

diameter endpoint endpoint_name
Specifies the Diameter endpoint for this location service, which includes the hostname, peer configuration, and other Diameter base configuration.

---

map-service map_svc_name
Associates a Mobile Application Part (MAP) service with this location service. This keyword is applicable for SGSN only.

map_sv_svc_name specifies the name for a pre-configured MAP service to associate with this location service.
Usage
Use this command to specify the Diameter dictionary and endpoint to be used for this location service, or associate supportive services with this location service.
The location service provides SLg (MME) interface support or Lg (SGSN) interface support via the Diameter protocol between the MME or SGSN and the GLMC.

Example
The following command associates a pre-configured Diameter endpoint named test12 to this location service:

```
associate diameter endpoint test12
```
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
end

**Usage**
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```bash
exit
```

Usage
Use this command to return to the parent configuration mode.
timeout

Configures the timers used to control various location service procedures.

Product
SGSN

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > Location Service Configuration

configure > context context_name > location-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-location-service)#

Syntax

[ default ] timeout { area-event-invoke-timer aietimer_seconds | lcsn lcns_seconds | periodic-event-invoke-timer peitimer_seconds | ue-available-guard-timer ueagtimer_seconds

default

Resets the specified timer to the default value.

area-event-invoke-timer aietimer_seconds

This timer, set in seconds, is used to guard the area event invoke procedure.

aietimer_seconds is an integer from 10 through 20. Default is 15.

lcsn lcns_seconds

Sets the NAS location service notification timer defining how long the SGSN will wait (in seconds) before aborting the Location Service Request, and release all resources allocated for the transaction.

lcns_seconds is an integer from 10 through 20. Default is 15.

periodic-event-invoke-timer peitimer_seconds

This timer, set in seconds, is used to guard the period location invoke procedure.

peitimer_seconds is an integer from 10 to 20. Default is 15.

ue-available-guard-timer ueagtimer_seconds

This timer, set in seconds, is used to guard the packet-switched deferred location request (UE available event) procedures.

ueagtimer_seconds is an integer from 10 to 600. Default is 600.

Usage
Use this command to set the amount of time the SGSN waits to perform various location service procedures.

Example
The following command can be used to set the time the SGSN will wait, for example 12 seconds, before aborting the Location Service Request:

```
timeout lcns 12
```

The following command can be used to set the timeout for the UE available guard timer to 460 seconds:

```
timeout ue-available-guard-timer 460
```
Chapter 195
Logical eNode Configuration Mode Commands

The Logical eNodeB configuration option enables the configuration of one or more logical eNodeBs within the HeNB-GW. The Logical eNodeB configuration can be used to support load balancing within a pool of TAI.

Mode

Exec > Global Configuration > Context Configuration > HENBGW-NETWORK Service Configuration > Logical eNodeB Configuration

configure > context context_name > henbgw-network-service service_name > logical-enb
  global-enb-id plmn-id mcc mcc_id mnc mnc_id { home-enb-id henb_id | macro-enb-id menb_id }

Entering the above command sequence results in the following prompt:

[context_name]host_name(logical-enb)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
associate mme-pool

Associates a previously configured MME pool to this logical eNodeB. An MME pool must be configured in LTE Policy Configuration mode before using this configuration.

Product
HeNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > HENBGW-NETWORK Service Configuration > Logical eNodeB Configuration

```bash
configure > context context_name > hnbgw-network-service service_name > logical-enb global-enb-id plmn_id mcc mcc_id mnc mnc_id { home-enb-id henb_id | macro-enb-id menb_id }
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(logical-enb)#
```

Syntax

```bash
associate mme-pool pool_name

no associate mme-pool
```

`no`
Removes the associated MME pool from this logical eNodeB configuration.

`pool_name`
Identifies the name of the pre-configured MME pool to associate with this logical eNodeB. `pool_name` is an alphanumeric string of 1 through 63 characters.

Usage

Use this command to bind/associate a pre-configured MME pool to the this logical eNodeB. The MME pool can be configured in LTE Policy configuration mode. The associate configuration is used to establish associations with other helper services in general. Each logical eNodeB can connect up to 8 MMEs. Since 8 logical eNodeBs can be configured per HeNB-GW Network service, a total of 64 associations can be established between HeNB-GW and MME.

Example

Following command associates an MME pool named `mme_pool` with specific logical eNodeB:

```
associate mme-pool mme_pool
```
associate tai-list-db

Associates a previously configured TAI database name to this logical eNodeB. A TAI database name for TAI configuration must be configured in LTE Policy Configuration mode before using this configuration.

Product
HeNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > HENBGW-NETWORK Service Configuration > Logical eNodeB Configuration
configure > context context_name > hembgw-network-service service_name > logical-enb global-enb-id plmn_id mcc_id mcc_id nnc_id { home-enb-id henb_id | macro-enb-id mcnb_id }

Entering the above command sequence results in the following prompt:

[context_name]host_name (logical-enb) #

Syntax

associate tai-list-db tai_db_name

no associate tai-list-db

no

Removes the associated TAI database from this logical eNodeB configuration.

tai_db_name

Identifies the name of the pre-configured TAI database to associate with this logical eNodeB. tai_db_name is an alphanumeric string of 1 through 63 characters.

Usage

Use this command to bind/associate a pre-configured TAI database to the this logical eNodeB. The MME pool can be configured in LTE Policy configuration mode. The associate configuration is used to establish associations with other helper services in general.

A maximum number of 8 TAI databases are supported. Each TAI database can accommodate up to 256 configurations of Tracking Area Codes (TACs). Therefore a total of 2048 TACs are supported.

Example

Following command associates a TAI database named henb_tai_db with specific logical eNodeB:

associate tai-list-db henb_tai_db
**bind s1-mme**

Binds the pre configured Local SCTP IP Address for S1 association to MME.

**Product**
HeNB-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > HENBGW-NETWORK Service Configuration > Logical eNodeB Configuration

```
configure > context context_name > hnbgw-network-service service_name > logical-enb
global-enb-id plmn_id mcc mcc_id mnc mnc_id { home-enb-id henb_id | macro-enb-id menb_id }
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(logical-enb)#
```

**Syntax**

```
bind s1-mme { ipv4-address } ip_addr

no bind s1-mme
```

**Usage**

```
no
```

Removes the binding of S1-MME interface from this logical eNodeB configuration.

```
ip_addr
```

Identifies the IP address of the S1-MME interface to associate with this HeNB-GW Network service.

`addr_val` must be entered in the IPv4 (dotted decimal notation) or IPv6 (`/::` notation).

**Example**

Use this command to bind the pre configured IPv4/IPv6 address of the S1-MME interface to the logical eNodeB.

Following command binds the S1-MME interface having `192:168:100:101` IP address with specific logical eNodeB.

```
bind s1-mme ipv6-address 192:168:100:101
```
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**

Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Use this command to return to the parent configuration mode.
s1-mme ip qos-dscp

This command configures the quality of service (Do's) differentiated service code point (DSCP) marking for IP packets sent out on the S1-MME interface, from the HeNB-GW to the MME(s).

Product
HeNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > HENBGW-NETWORK Service Configuration > Logical eNodeB Configuration

```
configure > context context_name > henhbgw-network-service service_name > logical-enb
global-enb-id pimn_id mcc mcc_id mnc mnc_id {home-enb-id henhbgw | macro-enb-id menb_id}
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(logical-enb)#
```

Syntax

```
s1-mme ip qos-dscp { af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41
| af42 | af43 | be | cs0 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef }

default s1-mme ip qos-dscp
```

```
qos-dscp { af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41
| af42 | af43 | be | cs0 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef }
```

Default: af11

Specifies the DSCP for the specified QoS traffic pattern. qos-dscp can be configured to any one of the following:

- `af11`: Assured Forwarding 11 per-hop-behavior (PHB)
- `af12`: Assured Forwarding 12 PHB
- `af13`: Assured Forwarding 13 PHB
- `af21`: Assured Forwarding 21 PHB
- `af22`: Assured Forwarding 22 PHB
- `af23`: Assured Forwarding 23 PHB
- `af31`: Assured Forwarding 31 PHB
- `af32`: Assured Forwarding 32 PHB
- `af33`: Assured Forwarding 33 PHB
- `af41`: Assured Forwarding 41 PHB
- `af42`: Assured Forwarding 42 PHB
- `af43`: Assured Forwarding 43 PHB
- `be`: Best effort forwarding PHB
- `cs0`: Designates use of Class Selector 0 PHB. This is same as DSCP Value BE
- `cs1`: Designates use of Class Selector 1 PHB
- `cs2`: Designates use of Class Selector 2 PHB
- `cs3`: Designates use of Class Selector 3 PHB
- `cs4`: Designates use of Class Selector 4 PHB
cs5: Designates use of Class Selector 5 PHB
cs6: Designates use of Class Selector 6 PHB
cs7: Designates use of Class Selector 7 PHB
ef: Expedited forwarding PHB

Usage

DSCP levels can be assigned to specific traffic patterns to ensure that data packets are delivered according to the precedence with which they are tagged. The diffserv markings are applied to the IP header of every subscriber data packet transmitted over the S1-MME interface(s).

Example

The following command sets the DSCP-level for data traffic sent over the S1-MME interface to af12:

```
s1-mme ip qos-dscp af12
```
s1-mme sctp port

This command configures the local Stream Control Transmission Protocol (SCTP) port used for binding the SCTP socket to communicate with the MMEs over S1-MME interface.

**Product**
HeNB-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > HENBGW-NETWORK Service Configuration > Logical eNodeB Configuration

```
configure > context context_name > hengw-network-service service_name > logical-enb
  global-enb-id plmn_id mcc mcc_id mnc mnc_id { home-enb-id henb_id | macro-enb-id menb_id }
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(logical-enb)#
```

**Syntax**

```
s1-mme sctp port port_num

default s1-mme sctp port
```

**default s1-mme sctp port**

- **default**
  
  Sets the SCTP port to the default value of 36412 to communicate with the MMEs using S1-MME interface.

- **port_num**
  
  Specifies the SCTP port number to communicate with the HeNBs using S1-MME interface as an integer from 1 through 65535. Default: 36412

**Usage**

Use this command to assign the SCTP port with SCTP socket to communicate with the HeNB using S1AP. Only one SCTP port can be associated with one MME service.

**Example**

The following command sets the default SCTP port number 699 for to interact with Home eNodeB using S1AP on S1-MME interface:

```
default s1-mme sctp port
```
Chapter 196
Loopback Interface Configuration Mode Commands

Use the Loopback Interface Configuration mode to create and manage loopback interfaces that provide IP addresses that are always available and reachable from any interface within a given context.

**Mode**

Exec > Global Configuration > Context Configuration > Loopback Interface Configuration

```
configure > context context_name > interface interface_name loopback
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-loopback)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
**crypto-map**

Applies the specified IPSec crypto-map to this interface.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Loopback Interface Configuration

```
configure > context context_name > interface interface_name loopback
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-loopback)#
```

**Syntax**

```
crypto-map map_name [ secondary-address sec_ip_addr ]
```

- **no**
  Deletes the application of the crypto map on this interface.

- **map_name**
  Specifies the name of the crypto map being applied. The name is an alphanumeric string of 1 through 127 characters that is case sensitive.

- **secondary-address sec_ip_addr**
  Applies the crypto map to the secondary address for this interface that is specified by `sec_ip_addr`. `sec_ip_addr` must be specified using the IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

**Usage**

In order for ISAKMP and/or manual crypto maps to work, they must be applied to a specific interface using this command. Dynamic crypto maps should not be applied to interfaces. The crypto map must be configured in the same context as the interface.

**Example**

To apply the IPSec crypto map named cmap1 to this interface, use the following command:

```
crypto-map cmap1
```
**description**

Use this command to configure the descriptive text for the current interface.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > Loopback Interface Configuration  
configure > context context_name > interface interface_name loopback

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-loopback)#
```

**Syntax**

```
description text
no description
```

**Usage**

Set the description to provide any useful information on the interface’s primary function, services, end users.

**Example**

```
description sampleInterfaceDescriptiveText
```
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Use this command to return to the parent configuration mode.
ip

Use this command to configure the IP options for the current interface.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Loopback Interface Configuration

configure > context context_name > interface interface_name loopback

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-if-loopback)#

Syntax

ip address { ip_address ip_mask | ip_address/bitmask } [ secondary | srp-activate ]
no ip address ip_address

ip ranged-address { ip_address ip_mask | ip_address/bitmask}
no ip ranged-address

no

Deletes the IP address or range of IP address you specify from the interface configuration.

address {ip_address ip_mask | ip_address/bitmask} [ secondary | srp-activate ]

Configures the IP address and network mask for the interface.

Enter an ip_address ip_mask to specify an IP address and the subnet mask pair that identifies the IP address of the interface. ip_address is entered in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation. Currently, the only value accepted for ip_mask is 255.255.255.255 (IPv4) or 120 (IPv6).

For the network mask, ip_address/net_mask, enter the IP address and the length in bits of the network mask. For example, 192.168.1.0/32 (IPv4) or fe80::c0a8:100/32 (IPv6). Currently, the only value accepted for bit_mask is 32.

Use the secondary keyword ito configure a secondary IP address on the interface. This is referred to as multi-homing of the interface.

Use the srp-activate keyword to activate the IP address for Interchassis Session Recovery (ICSR).

range-address ip_address ip_mask | ip_address/bitmask

Configures the range or group of IP address for the loopback interface. This support is provided to enable the support of multiple Enterprise HA in one HA service.

ip_address specifies the IP address for the loopback interface and must be specified in IPv4 dotted-decimal notation.

ip_mask specifies the number of subnet bits, representing the subnet mask in CIDR notation and must be a value between 1 to 32 and bitmask specifies the subnet mask in IPv4 dotted-decimal notations.
**Important:** This interface configuration is allowed only for IPv4 addresses and MUST be bound to the HA Service.

**Usage**
Create and manage loopback interfaces for the current context.
IP range support is provided through `range-address` keyword. This keyword is added to provide Enterprise HA support on HA service to connect enhanced number of enterprise nodes. Refer *HA Administration Guide* for more information.

This IP address range configuration must meet the following criteria:
- The ranged address MUST be a primary address.
- The ranged-address MUST be unique across the interface configuration.
- The ranged-address MUST be unique across the Context.
- The address specified in the ranged address MUST NOT be part of any other interface.
- The ranged-address can be a SRP-activated address and the behavior is the same as with any SRP-activated address.

**Example**
The following command configures IP address to associate with the interface:

```
ip address 1.2.3.4 255.255.255.255
```

The following command removes the associated IP address for the interface:

```
no ip address 10.2.3.4
```

The following command configures the range of IP addresses for over this interface to be used with HA service configuration for Enterprise HA support:

```
ip range-address 10.2.3.0/24
```
ip vrf

Use this command to configure the IP VPN Routing Forwarding (VRF) instance for the current interface.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Loopback Interface Configuration

configure > context context_name > interface interface_name loopback

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-if-loopback)#

Syntax

ip vrf forwarding vrf_name

no vrf forwarding

no

Deletes the IP VRF instance you specify from the interface configuration.

vrf_name

Specifies the preconfigured IP VRF instance name to be used with this interface.

For vrf_name, enter a VRF instance name that was preconfigured via the ip vrf forwarding command in Context Configuration mode.

Usage

Use this command to associate a preconfigured IP VRF instance for the current interface.

Example

The following command associates a preconfigured IP VRF instance named vrf_1 with this interface:

ip vrf forwarding vrf_1
**ipv6 address**

Use this command to configure the IPv6 options for the current interface.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > Loopback Interface Configuration
configure > context context_name > interface interface_name loopback

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-loopback)#
```

**Syntax**

```
ipv6 address ipv6_address ip_mask [ srp-activate ]

no ipv6 address ipv6_address
```

**Usage**

Create and manage loopback interfaces for the current context and enable Session Redundancy Protocol (SRP) when appropriate.

**Example**

The following command configures an IPv6 address to associate with the interface and enables SRP:

```
ipv6 address 2001:268:2008:b::1021/128 srp-activate
```
Chapter 197
LTE Emergency Profile Configuration Mode Commands

This mode configures parameters supporting the IP Multimedia Subsystem (IMS) emergency bearer services. Connectivity to an emergency Packet Data Network (PDN) is statically configured in this mode.

**Mode**

Exec > Global Configuration > LTE Policy Configuration > LTE Emergency Profile Configuration

```
configure > lte-policy > lte-emergency-profile profile_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(lte-emergency-profile) #
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
ambr

Configures the maximum aggregated uplink and downlink bitrate values for this profile.

Product
MME

Privilege
Administrator

Mode
Exec > Global Configuration > LTE Policy Configuration > LTE Emergency Profile Configuration

configure > lte-policy > lte-emergency-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(lte-emergency-profile)#

Syntax

ambr max-\ul bitrate max-\dl bitrate

no ambr

no

Removes the aggregated maximum bitrate (AMBR) configuration for this emergency profile.

max-\ul bitrate

Configures the maximum aggregated bitrate value for the uplink as an integer from 0 through 1410065408.

max-\dl bitrate

Configures the maximum aggregated bitrate value for the downlink as an integer from 0 through 1410065408.

Usage

Use this command to configure uplink and downlink maximum aggregated bitrate values to be shared across all non-guaranteed bitrate bearers established for the emergency session.

Example

The following example configures the uplink AMBR value to 2000 bps and the downlink AMBR value to 2000 bps:

    ambr max-\ul 2000 max-\dl 2000
apn

Configures the name and PDN type of the access point name (APN) used for emergency PDN connections.

**Product**
MME

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > LTE Policy Configuration > LTE Emergency Profile Configuration

configure > lte-policy > lte-emergency-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(lte-emergency-profile)#

**Syntax**

```
apn apn_name pdn-type { ipv4 | ipv4v6 | ipv6 }
no apn
```

**no apn**

Removes the selected APN from the profile.

```
apn_name
```

*apn_name* specifies the name of a pre-configured APN profile to associate with this LTE emergency profile. For more information on APNs, refer to the *apn* command in the *Context Configuration Mode Commands* chapter.

```
pdn-type { ipv4 | ipv4v6 | ipv6 }
```

Configures the packet data network type supported by the APN and this profile.

*ipv4*: Specifies that the PDN supports IPv4 network traffic.

*ipv4v6*: Specifies that the PDN supports both IPv4 and IPv6 network traffic.

*ipv6*: Specifies that the PDN supports IPv6 network traffic.

**Usage**
Use this command to select the APN to be used for emergency bearer services. APNs are configured through the APN Configuration mode. For more information regarding APN configuration mode commands, refer to the *APN Configuration Mode Commands* chapter.

**Example**
The following command specifies that the APN named *apn-3.com* is to be used for emergency bearer services and that the PDN supports IPv4 traffic only:

```
apn apn-3.com pdn-type ipv4
```
associate

 Associates a location service with this LTE emergency profile.

 **Product**
 MME

 **Privilege**
 Administrator

 **Mode**
 Exec > Global Configuration > LTE Policy Configuration > LTE Emergency Profile Configuration

 configure > lte-policy > lte-emergency-profile profile_name

 Entering the above command sequence results in the following prompt:

 [local]host_name(lte-emergency-profile)#

 **Syntax**

 associate location-service location_svc_name

 no associate location-service

 no

 Disassociates a previously associated location service with this LTE emergency profile.

 location-service location_svc_name

 Associates a location service with this LTE emergency profile. Only one location service can be associated with an LTE emergency profile.

 location_svc_name specifies the name for a pre-configured location service to associate with the LTE emergency profile as an alphanumeric string of 1 through 63 characters.

 **Usage**

 Use this command to associate a pre-configured location service with an LTE emergency profile. This enables the associated location service to provide location information of emergency calls to the GMLC.

 For more information about Location Services (LCS), refer to the location-service command in the Context Configuration Mode Commands chapter as well as the Location Services Configuration Mode Commands chapter.

 Further details can be found in the Location Services chapter of the MME Administration Guide.
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```
pgw

Statically configures a P-GW to support emergency bearer services for this profile.

Product
MME

Privilege
Administrator

Mode
Exec > Global Configuration > LTE Policy Configuration > LTE Emergency Profile Configuration
configure > lte-policy > lte-emergency-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(lte-emergency-profile)#

Syntax

pgw fqdn fqdn

pgw ip-address address protocol { both | gtp | pmip } weight value

no pgw { fqdn | ip-address address }

no fqdn
Removes the specified P-GW Fully Qualified Domain Name (FQDN) or IP address from this profile.

fqdn fqdn
Specifies the domain name of the P-GW as an alphanumeric string of 1 through 256 characters.

**Important:** A maximum of one P-GW FQDN configuration is allowed per profile.

ip-address address
Specifies the IP address for the P-GW in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

**Important:** A maximum of four P-GW IP address configurations are allowed per profile.

protocol { both | gtp | pmip }
Specifies the protocol the P-GW supports. Options are:

• **both:** Specifies that both the GTP and PMIP protocols are supported.
• **gtp:** Specifies that only GTP is supported.
• **pmip:** Specifies that only PMIP is supported.
weight value
Assigns a weight to P-GW IP address to use as a preferred P-GW as an integer from 1 through 100. Lowest value has the least preference.

Usage
Use this command to statically configure the P-GW used to support emergency bearer services through this profile.

Example
The following command configures the P-GW supporting emergency bearer services for this profile as pdn-911.gov:

```
pgw fqdn P-GW FQDN
```

The following command configures the P-GW supporting emergency bearer services for this profile as having an IPv4 address of 10.2.3.4, supporting GTP only, and having a weight of 10:

```
pgw ip-address 10.2.3.4 protocol gtp weight 10
```
qos

Configures the quality of service (QoS) parameters for the emergency bearer service.

**Product**
MME

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > LTE Policy Configuration > LTE Emergency Profile Configuration

```bash
configure > lte-policy > lte-emergency-profile profile_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(lte-emergency-profile)#
```

**Syntax**

```bash
qos qci qci arp arp_value preemption-capability { may | shall-not } vulnerability { not-preemptable | preemptable }

no qos
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>qci qci</code></td>
<td>Specifies the QoS Class Identifier (QCI) for the emergency bearer profile as an integer from 0 through 255.</td>
</tr>
<tr>
<td><code>arp arp_value</code></td>
<td>Defines the address retention priority value as an integer from 1 through 15.</td>
</tr>
</tbody>
</table>
| `preemption-capability { may | shall-not }` | Specifies the preemption capability flag. Options are:  
  - `may`: Bearer may be preempted  
  - `shall-not`: Bearer shall not be preempted |
| `vulnerability { not-preemptable | preemptable }` | Specifies the vulnerability flag. Options are:  
  - `not-preemptable`: Bearer cannot be preempted.  
  - `preemptable`: Bearer can be preempted. |

**Usage**

Use this command to set the QoS ARP and QCI parameters for the emergency bearer configuration.

**Example**

The following command sets the QCI number to 7, the ARP value to 2, the preemption capability to “may”, and the vulnerability flag to “pre-emptable”:

```bash
qos qci 7 arp 2 preemption-capability may vulnerability preemptable
```
ue-validation-level

Configures the type of user equipment (UE) that can use the emergency bearer service through the profile.

**Product**
MME

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > LTE Policy Configuration > LTE Emergency Profile Configuration

```
configure > lte-policy > lte-emergency-profile profile_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(lte-emergency-profile)#
```

**Syntax**

```
ue-validation-level { auth-only | full | imsi | none }
```

```
default ue-validation-level
```

```
default
```

Returns the command to its default setting of “none”.

```
{ auth-only | full | imsi | none }
```

Specifies the type of UE allowed to use the emergency bearer service. Options are:

- **auth-only**: Specifies that UEs that have been authenticated are allowed to use the emergency bearer service. These UEs may be in a limited service state in that they may be in an area with restricted service or where they are restricted from services. Enabling this option also causes subscription and location validation to be bypassed.
- **full**: Specifies that only UEs that have been authenticated and have successfully passed subscription and location validation are allowed to use the emergency bearer service. Enabling this option indicates that only UEs that are capable of normal attach procedures will be allowed to use the emergency bearer service.
- **imsi**: Specifies that UEs with an International Mobile Subscriber Identity (IMSI) are allowed to use the emergency bearer service regardless of authentication. Even if authentication fails, the UE is granted access.
- **none**: Specifies that all UEs are allowed to use the service. This is the default value for the command.

**Usage**

Use this command to indicate which UEs can use the emergency bearer service through this profile.

**Example**

The following command configures the type of UE allowed to use the emergency bearer service to “IMSI required, authentication optional”:

```
ue-validation-level imsi
```
Chapter 198
LTE Forbidden Location Area Configuration Mode Commands

The LTE Forbidden Location Area Configuration Mode is used to create and manage forbidden 3G location area code (LAC) configurations.

Mode

Exec > Global Configuration > LTE Policy Configuration > LTE HO Restriction List Configuration > LTE Forbidden Location Area Configuration

```
configure > lte-policy > ho-restrict-list list_name > forbidden location-area plmnid plmn_id
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(forbidden_la)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

end

Usage

Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**
Use this command to return to the parent configuration mode.
**lac**

Configures a 3G location area code (LAC) or area codes where a UE, associated with this LTE policy, is restricted from participating in a handover scenario.

**Product**
MME

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > LTE Policy Configuration > LTE HO Restriction List Configuration > LTE Forbidden Location Area Configuration

```bash
configure > lte-policy > ho-restrict-list list_name > forbidden location-area plmn_id
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(forbidden_la)#
```

**Syntax**

```
[ no ] lac { area_code } +
```

*no*

Removes a configured forbidden handover area code or area codes from this policy. If no location area code is specified, then all location area codes are removed.

*area_code*

Specifies an area code or area codes from which UEs are restricted from participating in a handover as an integer from 0 through 65535. Multiple area codes can be entered (up to 128 in a single line, separated by spaces).

**Usage**

Use this command to configure 3G location-based area codes that will be forbidden to UEs associated with this LTE policy.

**Example**

The following command configures eight location-based area codes (1, 2, 3, 4, 5, 6, 7, 8) where a UE, associated with this LTE policy, is restricted from participating in a handover scenario:

```
lac 1 2 3 4 5 6 7 8
```
Chapter 199
LTE Forbidden Tracking Area Configuration Mode
Commands

The LTE Forbidden Tracking Area Configuration Mode is used to create and manage forbidden tracking area code (TAC) configurations.

Mode
Exec > Global Configuration > LTE Policy Configuration > LTE HO Restriction List Configuration > LTE Forbidden Tracking Area Configuration
configure > lte-policy > ho-restrict-list list_name > forbidden tracking-area plmnid plmn_id

Entering the above command sequence results in the following prompt:

[local]host_name(forbidden_ta)#

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
end

**Usage**
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Use this command to return to the parent configuration mode.
tac

Configures a tracking area code (TAC) or area codes where a UE, associated with this LTE policy, is restricted from participating in a handover scenario.

Product
MME

Privilege
Administrator

Mode
Exec > Global Configuration > LTE Policy Configuration > LTE HO Restriction List Configuration > LTE Forbidden Tracking Area Configuration

configure > lte-policy > ho-restrict-list list_name > forbidden tracking-area plmnid

Entering the above command sequence results in the following prompt:

[local]host_name(forbidden_ta)#

Syntax

[ no ] tac area_code

<table>
<thead>
<tr>
<th>no</th>
</tr>
</thead>
<tbody>
<tr>
<td>Removes a configured forbidden handover area code or area codes from this policy. If no tracking area code is specified, then all tracking area codes are removed.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>area_code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies a tracking area code or area codes from which UEs are restricted from participating in a handover as an integer from 0 to 65535. Multiple area codes can be entered (up to 128 in a single line, separated by spaces).</td>
</tr>
</tbody>
</table>

Usage
Use this command to configure tracking area codes that will be forbidden to UEs associated with this LTE policy.

Example
The following command configures two tracking area codes (1, 2, 3, 4, 5, 6, 7, 8) where a UE, associated with this LTE policy, is restricted from participating in a handover scenario:

    tac 1 2 3 4 5 6 7 8
Chapter 200
LTE Foreign PLMN GUTI Management Database
Configuration Mode Commands

The LTE Foreign PLMN GUTI Management Database Configuration Mode is used to create restrictions on foreign PLMNs, thereby avoiding DNS request attempts to foreign PLMNs.

**Mode**

Exec > Global Configuration > LTE Policy Configuration > Foreign PLMN GUTI Management Database

```plaintext
configure > lte-policy > foreign-plmn-guti-mgmt-db
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(foreign-plmn-guti-mgmt-db)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**

Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**
Use this command to return to the parent configuration mode.
plmn

Configures a foreign Public Land Mobile Network (PLMN) entry in the Foreign PLMN GUTI management database. This optional configuration is used to control the acceptance or immediate reject of Attach Requests and TAU Requests containing a GUTI from this PLMN.

Product
MME

Privilege
Administrator

Mode
Exec > Global Configuration > LTE Policy Configuration > Foreign PLMN GUTI Management Database
configure > lte-policy > foreign-plmn-guti-mgmt-db

Entering the above command sequence results in the following prompt:

[local]host_name(foreign-plmn-guti-mgmt-db)#

Syntax

plmn mcc { mcc_value | any } mnc { mnc_value | any } [ allow | reject ]

plmn mcc mcc_value mnc mnc_value

no

Removes the specified PLMN entry from the Foreign PLMN GUTI management database.

mcc mcc_value mnc mnc_value

mcc { mcc_value | any } : Specifies the mobile country code (MCC) portion of the PLMN identifier as an integer from 100 through 999. Use the optional any keyword to specify a wildcard, representing any MCC.
mnc { mnc_value | any } : Specifies the mobile network code (MNC) portion of the PLMN identifier a 2- or 3-digit integer from 00 through 999. Use the optional any keyword to specify a wildcard, representing any MNC.

Note: The any keyword can only be used for the MNC value when a specific MCC value is given. For example, the follow command is not allowed:
plmn mcc any mnc 456 allow

allow

Configures the MME to allow foreign GUTIs from this PLMN.

reject

Configures the MME to reject foreign GUTIs from this PLMN.
Usage

Use this command to create and configures a foreign Public Land Mobile Network (PLMN) entry in the Foreign PLMN GUTI management database. This optional configuration is used to control the acceptance or immediate reject of Attach Requests and TAU Requests containing a GUTI from this PLMN.

If the configured action is Reject, the MME takes the following actions:

- Attach Requests: a NAS Identity Request is sent to the UE to determine its IMSI, and no DNS lookup is performed to find a peer MME or SGSN.
- TAU Requests: a TAU Reject message is sent immediately with cause code 9 (UE Identity cannot be derived by the network), and no DNS lookup is performed to find a peer MME or SGSN.

If the configured action is Allow, the MME continues processing the Attach Request or TAU Request, and a DNS request may be made.

A maximum of 16 foreign PLMN entries can be added to a Foreign PLMN GUTI management database.

Example

The following command creates a plmn entry in the foreign PLMN GUTI management database. The entry specifies that GUTIs from PLMNs with the MCC of 123 and any MNC be rejected.

```
plmn mcc 123 mnc any reject
```
Chapter 201
LTE Handover Restriction List Configuration Mode Commands

The LTE Handover Restriction List Configuration Mode is used to create and manage the LTE handover restriction lists for LTE/SAE networks. Handover restriction lists are used to restrict user equipment (UE) from participating in specified handovers. The MME creates the handover restriction lists as part of its local policy and provides them to the eNobeB where the restrictions are enforced.

Mode

Exec > Global Configuration > LTE Policy Configuration > LTE HO Restriction List Configuration

configure > lte-policy > ho-restrict-list list_name

Entering the above command sequence results in the following prompt:

[local]host_name(ho-restrict-list)#

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
end

**Usage**
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Use this command to return to the parent configuration mode.
forbidden

Configures the handover restriction lists provided to eNodeBs where handover restrictions are enforced for UEs.

Product
MME

Privilege
Administrator

Mode
Exec > Global Configuration > LTE Policy Configuration > LTE HO Restriction List Configuration

configure > lte-policy > ho-restrict-list list_name

Entering the above command sequence results in the following prompt:

[local]host_name(ho-restrict-list)#

Syntax

[ no ] forbidden { inter-rat { all | cdma2000 | geran | utran } | location-area plmnid id | tracking-area plmnid id }

default forbidden inter-rat

Remove the forbidden inter-RAT configuration from the LTE policy.

no

Removes the forbidden configuration from the LTE policy.

inter-rat { all | cdma2000 | geran | utran }

Specifies that one or all Radio Access Technology (RAT) handovers are to be prohibited for UEs associated with the LTE policy.

all: Specifies that all inter-RAT handovers are to be prohibited for UEs associated with the LTE policy.

cdma2000: Specifies that all CDMA2000 handovers are to be prohibited for UEs associated with the LTE policy.

geran: Specifies that all GSM EDGE Radio Access Network (GERAN) handovers are to be prohibited for UEs associated with the LTE policy.

utran: Specifies that all UMTS Terrestrial Radio Access Network (UTRAN) handovers are to be prohibited for UEs associated with the LTE policy.

location-area plmnid id

Specifies that handovers to 3G location area codes defined through this keyword and subsequent configuration mode are to be prohibited for UEs associated with the LTE policy. Enters the LTE Forbidden Location Area Configuration Mode. id must be a valid PLMN ID expressed as an integer comprised of an MCC (Mobile Country Code) and MNC (Mobile Network Code) [five-digit minimum, six-digit maximum].

Important: Up to 16 forbidden location area PLMN IDs can be configured per handover restriction list.
Entering this command results in the following prompt:

```
[context_name]hostname(forbidden_la)#
```

LTE Forbidden Location Area Configuration Mode commands are defined in the *LTE Forbidden Location Area Configuration Mode Commands* chapter.

```
tracking-area plmnid id
```

Specifies that handovers to 4G tracking area codes defined through this keyword and subsequent configuration mode are to be prohibited for UEs associated with the LTE policy. Enters the LTE Forbidden Tracking Area Configuration Mode. *id* must be a valid PLMN ID and be an integer value comprising an MCC and MNC (five-digit minimum, six-digit maximum).

**Important:** Up to 16 forbidden tracking area PLMN IDs can be configured per handover restriction list.

```
[context_name]hostname(forbidden_ta)#
```

LTE Forbidden Tracking Area Configuration Mode commands are defined in the *LTE Forbidden Tracking Area Configuration Mode Commands* chapter.

### Usage

Use this command to create the list of restricted handover types that apply to all UEs associated with the LTE policy.

### Example

The following command prohibits UEs associated with this LTE policy from participating in a handover to a GERAN network type:

```
forbidden inter-rat geran
```

The following command prohibits UEs, associated with this LTE policy and a mobile network with a PLMN ID of 12345, from participating in a handover to location area codes defined in the Location Area Configuration Mode:

```
forbidden location-area plmnid 12345
```
Chapter 202
LTE Network Global MME ID Management Database Configuration Mode Commands

The LTE Network Global MME ID Management Database Configuration Mode is used to create associations between PLMN IDs and MME group ID ranges.

Mode

Exec > Global Configuration > LTE Policy Configuration > LTE Network Global MME ID Management Database Configuration

configure > lte-policy > network-global-mme-id-mgmt-db

Entering the above command sequence results in the following prompt:

[local]host_name(network-global-mme-id-mgmt-db)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
exit
```

Usage
Use this command to return to the parent configuration mode.
**plmn**

Configures associations between public land mobile network (PLMN) IDs and ranges of MME group IDs. On the S4-SGSN, this command allows the operators to configure a custom list of MME group IDs if networks have been configured with LACs in the 32768-65535 range for UMTS and GPRS coverage.

**Product**
MME
SGSN

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > LTE Policy Configuration > LTE Network Global MME ID Management Database Configuration

configure > lte-policy > network-global-mme-id-mgmt-db

Entering the above command sequence results in the following prompt:

```
[local]host_name(network-global-mme-id-mgmt-db)#
```

**Syntax**

```
[ no ] plmn mcc mcc_value mnc mnc_value mme-group-id-range first id last id
```

- **no**
  - Removes the selected PLMN ID to MME group ID range from the MME ID management database.

```
mcc mcc_value mnc mnc_value
```

- **mcc mcc_value**: Specifies the mobile country code (MCC) portion of the PLMN identifier as an integer from 100 through 999.
- **mnc mnc_value**: Specifies the mobile network code (MNC) portion of the PLMN identifier as a 2- or 3-digit integer from 00 through 999.

```
mme-group-id-range first id last id
```

- Specifies the range of MME group IDs to apply to the PLMN ID as an integer from 0 to 65535.

**Usage**

Use this command to create associations between PLMN IDs and a range of MME group IDs. On the S4-SGSN, use this command to create a custom list of MME group IDs on the S4-SGSN if networks have been configured with LACs in the 32768-65535 range for UMTS and GPRS coverage. The S4-SGSN will use this custom list to identify whether the received LAC is a native LAC or a LAC mapped from a globally unique temporary identifier (i.e., an MME group code part of GUTI). Once the **plmn** configuration is completed, operators must associate the configuration with the GPRS and/or SGSN services configured on the S4-SGSN using the **associate network-global-mme-id-mgmt-db** command. Refer to the **SGSN Service Configuration Mode** and **GPRS Service Configuration Mode** chapters in the **GPRS/UMTS Command Line Reference** for a description of this command.

**Example**

Cisco ASR 5x00 Command Line Interface Reference
The following command creates an association between a PLMN ID of 12323 and a set of MME group IDs with a range of 500 through 575:

```
plmn mcc 12323 mnc 23 mme-group-id-range first 500 last 575
```
Chapter 203
LTE Paging Map Configuration Mode Commands

The LTE Paging Map Configuration Mode is used to create and manage the LTE paging maps supporting MME configurations on the system.

Mode

Exec > Global Configuration > LTE Policy Configuration > LTE Paging Map Configuration

```
configure > lte-policy > paging-map map_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(paging-map)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Use this command to return to the parent configuration mode.
precedence

Enables the operator to apply a priority for different paging-profiles based on traffic type. When the MME service is associated with a paging map, the system checks the profile map to determine which paging-profile to adopt for a given paging trigger.

Product
MME

Privilege
Administrator

Mode
Exec > Global Configuration > LTE Policy Configuration > LTE Paging Map Configuration

configure > lte-policy > paging-map <map_name>

Entering the above command sequence results in the following prompt:

[local]host_name(paging-map)#

Syntax

precedence priority traffic-type { cs | ps } paging-profile <paging_profile_name>

no precedence precedence

no

Remove the paging map from the system.

precedence priority

precedence: For StarOS releases 16.5 and higher, enter an integer from 1 to 19, where 1 is the highest priority and 19 is the lowest priority. For StarOS releases prior to 16.5, enter an integer from 1 to 7, where 1 is the highest priority and 7 is the lowest priority.

traffic-type { cs | ps}

Defines the type of traffic of the incoming call.

- **cs** (Circuit Switched) - All data and control activities that involve CSFB. Paging requests from the MSC for mobile-terminated calls alone are treated as CS type. Paging requests for SMS are treated as PS type.
  
  If a sub-traffic-type is not configured then paging-profile configured for CS (with no sub traffic-type qualification) is applied. If no such entry exists, then default heuristics based paging behavior is applied.

- **ps** (Packet Switched) - All data and control activities that involve packet services. SRVCC is also mapped to this traffic-type as the voice is carried using PS service.

paging-profile <paging_profile_name>

The paging-profile to apply for paging UE.
**Important:** If the associated paging-map does not exist or does not have an entry matching the paging-trigger, the MME performs paging as outlined in 'Default Heuristics Paging Behavior' in the *Heuristic and Intelligent Paging* chapter in the MME Administration Guide.

**Usage**

Use this command to apply different paging-profiles based on traffic types. The command defines the order (1 - highest, 7 - lowest) in which the MME checks the entries in this paging-map. If the paging trigger (like Downlink Data Notification or MSC request) matches the traffic-type of that entry, then the corresponding paging-profile is used for paging the UE. If the paging trigger does not match, then the next entry in the precedence order is picked and checked for a match. If no match is found in the entire paging-map table then default heuristic paging profile is adopted.

If the MME receives another paging trigger (for example from the MSC for CSFB) while paging is already in progress, the MME checks whether a higher precedence paging profile can be applied. If the new trigger has a paging-map entry with a higher precedence, the MME restarts the paging process using the paging-profile associated with the new map entry.

Paging is typically triggered when either the MSC indicates that there is an incoming call to the UE (Call Service, CS), or when the S-GW sends a Downlink Data Notification (Packet Service, PS) to the MME, or when there is a bearer/PDN request coming from the P-GW/S-GW.

Refer to the *Heuristic and Intelligent Paging* chapter in the MME Administration Guide for more information.

**Related Commands**

Refer to the `paging-profile` command in the LTE Policy Configuration Commands chapter to create the paging profiles used in this command.
Chapter 204
LTE Paging Profile Configuration Mode Commands

The LTE Paging Map Configuration Mode is used to create and manage the paging profiles that control the different stages of paging for MME configurations on the system.

Mode

Exec > Global Configuration > LTE Policy Configuration > LTE Paging Profile Configuration

configure > lte-policy > paging-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(paging-profile)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
end

**Usage**
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**
Use this command to return to the parent configuration mode.
paging-stage

Enables the operator to configure different stages of paging in the order of desired execution with parameters that control the pace, volume, and behavior of a given paging stage.

Product
MME

Privilege
Administrator

Mode
Exec > Global Configuration > LTE Policy Configuration > LTE Paging Profile Configuration

configure > lte-policy > paging-profile profile_name

Entering the above command sequence results in the following prompt:

[local]host_name(paging-profile)#

Syntax

[ no ] paging-stage level match-criteria { ue-contact-time seconds | all } action { last-n-enb-last-tai max-n-enb value | all-enb-last-tai | all-enb-all-tai } t3413-timeout
seconds max-paging-attempts attempts

no

Remove the paging-stage from the system.

level

Defines different levels of paging-stages, each with a different match-criteria and different action. level must be a value 1 through 5.

match-criteria

Specifies the criteria for selecting a given paging stage.

•ue-contact-time seconds - Number of seconds elapsed since the MME last heard from UE. This time, if set, acts as an upper time limit to consider a given paging-stage for paging purposes. seconds must be a value from 0 through 86400.

•all - No criteria. Operator can use this match-criteria for the final paging stage.

action

Defines how the paging request should be formulated.

•last-n-enb-last-tai max-n-enb value - Send paging request to the last known number of eNodeBs (configured using max-n-enb value) and to the last known TAI. value must be a value from 1 through 5.

•all-enb-last-tai - Send paging request to all eNodeBs and to last known TAI.

•all-enb-all-tai - Send paging request to all eNodeBs and to all TAIs.
**t3413-timeout** *seconds*

Defines the time-interval in seconds between paging requests. The MME uses this timer for retransmission of an S1 Paging request to UE for PS paging. *timeout* must be a value from 0 through 20.

CS triggered S1 Paging requests are transmitted only once by the MME (no retransmission). For a CS paging to be sent again, another SGs paging request needs to be sent by MSC/VLR towards MME.

**max-paging-attempts** *attempts*

Defines the number of paging requests to be sent out during this paging-stage.

*attempts* must be a value from 0 through 5.

**Usage**

Use this command to configure paging procedure stages, which in turn control the pace, volume, and behavior of paging for each stage.

**Related Commands**

Refer to the **paging-map** command in the *LTE Policy Configuration Commands* chapter to assign a priority for this paging profile based on traffic type.
Chapter 205
LTE Peer Map Configuration Mode Commands

The LTE Peer Map Configuration Mode enables the operator to map LTE Policy to a peer profile based on matching criteria and precedence for the criteria.

**Mode**

Exec > Global Configuration > LTE Policy Configuration > LTE Peer Map Configuration

`configure > lte-policy > peer-map map_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(peer-map)#
```

**Important:** Available commands or keywords/variables vary based on platform type, product version, and installed license(s).
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**
Use this command to return to the parent configuration mode.
**precedence**

Configures the matching criteria and precedence for mapping an LTE Policy with a peer profile.

**Product**

P-GW
SAEGW
S-GW

**Privilege**

Administrator

**Mode**

Exec > Global Configuration > LTE Policy Configuration > LTE Peer Map Configuration

```
configure > lte-policy > peer-map map_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(peer-map) #
```

**Syntax**

```
precedence priority match-criteria { all peer-profile-name profile_name | peer-ip-address { ip_address | ip_address/mask } [ serving-plmnid mcc mcc mcc mcc ] peer-profile-name profile_name | serving-plmnid mcc mcc mcc mcc [ peer-ip-address { ip_address | ip_address/mask } ] peer-profile-name profile_name }
```

```
no precedence priority
```

Removing the selected precedence priority number from the peer map.

**priority**

(priority must be an integer from 1 to 1024.

**match-criteria**

Defines the criteria to be used to match peer nodes.

**all**

Specifies that all peer nodes are to be associated with the peer map.
To map a peer to a profile when there is no specific criteria required, use the all keyword.

**peer-profile-name profile_name**

Sets the peer profile with which the matching criteria is associated.

**profile_name** must be an existing peer profile expressed as an alphanumeric string of 1 through 64 characters.
**peer-ip-address ip_address | ip_address/mask**

Specifies the IP address of the peer node.

- `ip_address` must be specified using the standard IPv4 dotted decimal notation or colon notation for IPv6.
- `ip_address/mask` must be specified using the standard IPv4 dotted decimal notation or colon notation for IPv6, followed by the mask.

**serving-plmnid mcc mcc mnc mnc**

Specifies serving nodes with criteria matching the PLMN ID (MCC and MNC) are to be associated with a specified peer map.

- `mcc`: Specifies the mobile country code (MCC) portion of the PLMN ID. `mcc` must be a three-digit number between 100 and 999.
- `mnc`: Specifies the mobile network code (MNC) portion of the PLMN ID. `mnc` must be a two- or three-digit number between 00 and 999.

**Usage**

Use this command to map LTE Policy to a peer profile based on matching criteria and precedence for the criteria.

A maximum of 1024 precedence entries can be configured.

**Example**

The following command associates the peer profile named pp5 with peers associated with a serving node PLMN ID MCC of 111 and an MNC of 222:

```
precedence 100 match-criteria serving-plmnid mcc 111 mnc 222 peer-profile-name pp5
```
Chapter 206
LTE Policy Configuration Mode Commands

The LTE Policy Configuration Mode is used to create and manage the LTE policies supporting ePDG, MME, S-GW, SAEGW, SGSN and HeNBGW configurations on the system.

Mode

Exec > Global Configuration > LTE Policy Configuration
configure > lte-policy

Entering the above command sequence results in the following prompt:

[local]host_name(lte-policy)#

Important: Available commands or keywords/variables vary based on platform type, product version, and installed license(s).
cause-code-group

 Creates a new cause code group, or specifies an existing cause code group and enters the Cause Code Group Configuration Mode.

Product
MME

Privilege
Administrator

Mode
Exec > Global Configuration > LTE Policy Configuration

configure > lte-policy

Entering the above command sequence results in the following prompt:

[local]host_name(lte-policy)#

Syntax

cause-code-group group_name protocol s1ap

no cause-code-group group_name

no

Removes the specified cause code group with all related configuration from the LTE Policy.

 group_name

Specify a name of a cause-code-group to create, modify, or remove. This name must be an alphanumeric string of 1 through 16 characters. Each new cause-code-group must have a unique name.

A maximum of 4 cause code groups can be defined across all services (MME+GPRS+SGSN).

protocol

Specifies the protocol for the cause code group being created/accessed. Options include:

• S1-AP

Usage

Use this command to create or modify a group of cause codes.

Entering this command results in a prompt, with the protocol ID included, similar to the following:

[context_name]host_name(s1ap-cause-code)#

Depending upon the protocol you have selected, the Cause Code Group configuration commands are defined in the

• S1AP Cause Code Configuration Mode Commands chapter of this guide.

Example

The following command creates an S1-AP cause code group named move-ue-to-idle.
cause-code-group move-ue-to-idle protocol slap
congestion-action-profile

Creates an action profile for MME or ePDG critical, major and minor congestion thresholds. The profile defines the action to be taken when these thresholds are exceeded.

Product
- ePDG
- HeNBGW
- MME

Privilege
- Administrator

Mode
- Exec > Global Configuration > LTE Policy Configuration
  - configure > lte-policy

Entering the above command sequence results in the following prompt:

[local]host_name(lte-policy)#

Syntax

[ no ] congestion-action-profile profile_name

no

Removes the specified profile from the system.

profile_name

Specifies the name of the action profile. If the entered name does not refer to an existing profile, a new profile is created. profile_name is an alphanumeric string of 1 through 64 characters.

-noconfirm

Executes the command without any additional prompt and confirmation from the user.

Usage

Use this command to establish MME or ePDG action profiles to be associated with critical, major and minor congestion thresholds. This command is also used to remove an existing profile.

For information on setting the action to be taken within this profile, see the Congestion Action Profile Configuration Mode Commands chapter in this guide, and the Congestion Control chapter in the System Administration Guide.

Example

The following command creates a major congestion action profile named mme_major_profile and moves to the Congestion Action Profile Configuration mode:

congestion-action-profile mme_major_profile
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
end
```

**Usage**

Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Use this command to return to the parent configuration mode.
**foreign-plmn-guti-mgmt-db**

Creates a new, or enters the existing Foreign PLMN GUTI management database.

**Product**

MME

**Privilege**

Administrator

**Mode**

Exec > Global Configuration > LTE Policy Configuration

`configure > lte-policy`

Entering the above command sequence results in the following prompt:

```
[local]host_name(lte-policy)#
```

**Syntax**

```
foreign-plmn-guti-mgmt-db  db_name  [  -noconfirm  ]

no foreign-plmn-guti-mgmt-db  db_name
```

- **no**
  
  Remove the specified management database from the system.

- **-noconfirm**
  
  Executes the command without any additional prompt and confirmation from the user.

- **db-name**
  
  Specifies the name of the management database. If the name does not refer to an existing database, a new database is created.
  
  *db_name* is an alphanumeric string of 1 through 64 characters.

**Usage**

Use this command to create a new, or enter the existing Foreign PLMN GUTI management database. This management database allows for the optional configuration of foreign PLMNs for which Attach Requests or TAU Requests containing a GUTI from such a PLMN can either be allowed or immediately rejected.

A maximum of four separate Foreign PLMN GUTI management databases can be configured.

Entering this command results in the following prompt:

```
{context_name}hostname(foreign-plmn-guti-mgmt-db)#
```

Global MME ID management database commands are defined in the *LTE Foreign PLMN GUTI Management Database Configuration Mode Commands* chapter.

**Example**

The following command creates a Foreign PLMN GUTI management database named *fguti-db1*.

```
foreign-plmn-guti-mgmt-db  fguti-db1  -noconfirm
```
**henbgw mme-pool**

Creates or configures a specified MME or MME pool to which the HeNB-GW is to communicate and enters the MME pool configuration mode.

**Product**
HeNB-GW

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > LTE Policy Configuration
configure > lte-policy

Entering the above command sequence results in the following prompt:

```
[local]host_name(lte-policy)#
```

**Syntax**

```
[ no ] henbgw mme-pool pool_name [ -noconfirm ]
```

- **no**
  Removes an already configured MME or MME pool from the system.

- **pool_name**
  Specifies the name of the MME pool being created or accessed. If the pool name does not refer to an existing profile, a new pool is created. *pool_name* is an alphanumeric string of 1 through 63 characters.

- **-noconfirm**
  Executes the command without any additional prompt and confirmation from the user.

**Usage**

Use this command to enter the MME Pool Configuration Mode for an existing pool or for a newly defined MME pool. This command is also used to remove an existing MME pool.

**Important:** A maximum of eight MME pools are allowed per system.

Entering this command results in the following prompt:

```
[context_name]hostname(mme-pool)#
```

MME Pool Configuration Mode commands are defined in the *MME Pool Configuration Mode Commands* chapter.

**Example**

The following command helps entering the MME Pool Configuration Mode for a new or existing profile named *henb_mme_pool*.
mme pool henb_mme_pool
**henbgw overload-control**

Configures HeNBGW overload control parameters.

**Product**
HeNBGW

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > LTE Policy Configuration

configure > lte-policy

Entering the above command sequence results in the following prompt:

[local]host_name(lte-policy)#

**Syntax**

```
henbgw overload-control [ load-reduction-indicator percentage_value | ochl-guard-time minutes ]
```

```
default henbgw overload-control [ load-reduction-indicator | ochl-guard-time ]
```

---

default

Sets/Restores the default values assigned to HeNBGW overload control parameters. The default value of load Reduction indication is 99 percent.

---

**load-reduction-indicator** percentage_value

Designates the percentage of HeNBs to relay overload start message if traffic load Reduction indication IE is not present in the overload start message.

*percentage_value* is the percentage value, which is an integer between 1 and 99.

---

**ochl-guard-time** minutes

Designates the guard timeout value for sending overload stop messages if overload stop message is not received from MME to all the HeNBs in corresponding MME’s overload control HeNBs list.

*minutes* is the number of minutes, which is an integer between 0 and 2147483647.

**Usage**

Use this command to configure HeNBGW overload control parameters.

**Example**

The following command configures HeNBGW overload control parameter *ochl-guard-time* as 45 minutes:

```
henbgw overload-control ochl-guard-time 45
```
ho-restrict-list

Creates a handover (HO) restriction list or specifies an existing HO restriction list and enters the Handover Restriction List Configuration Mode.

Product
- MME
- ePDG
- SAEGW
- S-GW

Privilege
Administrator

Mode
Exec > Global Configuration > LTE Policy Configuration
configure > lte-policy

Entering the above command sequence results in the following prompt:

[local]hostname(lte-policy)#

Syntax

[ no ] ho-restrict-list  list_name  [ -noconfirm ]

<table>
<thead>
<tr>
<th>no</th>
</tr>
</thead>
<tbody>
<tr>
<td>Removes the specified restriction list from the system.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>-noconfirm</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executes the command without any additional prompt and confirmation from the user.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>list_name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the name of the HO restriction list. If the entered list name does not refer to an existing list, a new list is created. list_name is an alphanumeric string of 1 through 64 characters.</td>
</tr>
</tbody>
</table>

Usage

Use this command to enter the Handover Restriction List Configuration Mode for an existing list or for a newly defined list. This command is also used to remove an existing list.

Entering this command results in the following prompt:

[context_name]hostname(ho-restrict-list)#

Handover Restriction List Configuration Mode commands are defined in the LTE Handover Restriction List Configuration Mode Commands chapter.

Example

The following command enters the Handover Restriction List Configuration Mode for a new or existing list named ho_restrict_list1:
ho-restrict-list ho_restrict_list1
**lte-emergency-profile**

Creates an LTE emergency profile or specifies an existing emergency profile and enters the LTE Emergency Profile Configuration Mode.

**Product**
- MME
- ePDG
- SAEGW
- S-GW

**Privilege**
Adminstrator

**Mode**
Exec > Global Configuration > LTE Policy Configuration
   `configure > lte-policy`

Entering the above command sequence results in the following prompt:

```
[local]host_name(lte-policy)#
```

**Syntax**

```
[ no ] lte-emergency-profile profile_name [ -noconfirm ]
```

- **no**
  Removes an LTE emergency profile from the system.

- **profile_name**
  Specifies the name of the LTE emergency profile being created or accessed. If the profile name does not refer to an existing profile, a new profile is created. `profile_name` is an alphanumeric string of 1 through 64 characters.

- **-noconfirm**
  Executes the command without any additional prompt and confirmation from the user.

**Usage**

Use this command to enter the LTE Emergency Profile Configuration Mode for an existing profile or for a newly defined profile. This command is also used to remove an existing profile.

**Important:** A maximum of four LTE emergency profiles are allowed per system.

Entering this command results in the following prompt:

```
[context_name]hostname(lte-emergency-profile)#
```
LTE Emergency Profile Configuration Mode commands are defined in the LTE Emergency Profile Configuration Mode Commands chapter.

**Example**

The following command enters the LTE Emergency Profile Configuration Mode for a new or existing profile named `emergency_profile3`:

```
lte-emergency-profile emergency_profile3
```
mme paging cache

Enable or disables caching of the MME’s paging and provides the operator configurable paging cache controls.

Product
MME

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > LTE Policy Configuration
configure > lte-policy

Entering the above command sequence results in the following prompt:

[local]host_name(lte-policy)#

Syntax

mme paging cache { size cache_size | timeout time }

default mme paging cache { size | timeout }

default

Resets either the paging cache size or the paging cache timer to default settings.

size cache_size

cache_size: Enter an integer from 0 to 10000 to specify the maximum number of Tracking Area Code (TAC) entries to be cached.

Entering the ‘0’ value disables caching and should be followed by use of the mme paging cache clear command (in the Exec mode).

Default cache size = 5000 TAC entries per SessMgr.

timeout time

time: Enter an integer from 1 to 1440 to specify the number of minutes that each Tracking Area Code (TAC) entry remains valid.

A lower cache timeout helps to refresh the cache frequently and enables this functionality to quickly adapt to changes in the network. We recommend the timeout value be less than the expected eNodeB flap frequency; for example, if the eNodeBs connected to the MME are expected to disconnect and reconnect every 10 minutes (due to network issues), then the timeout configuration should be less than 10 minutes.

Default timeout = 5 minutes.

Usage

Both size and timeout must be configured to enable paging cache optimization. The mme paging cache command must be entered twice, once for each parameter.

Example

Set the paging cache timeout to match the eNodeB flap frequency of 10 minutes:

mme paging cache timeout 10
Set the paging cache size to disable caching:

```
  mme paging cache size 0

  end

  mme paging cache clear { all | instance sessmgr_instance }
```
network-global-mme-id-mgmt-db

Creates a new, or enters the existing MME group ID management database.

**Product**
- MME
- ePDG
- SAEGW
- S-GW
- SGSN

**Privilege**
Administrator

**Mode**
- Exec > Global Configuration > LTE Policy Configuration
- configure > lte-policy

Entering the above command sequence results in the following prompt:

```
[local] host_name(lte-policy)#
```

**Syntax**

```
[ no ] network-global-mme-id-mgmt-db
```

**Usage**

Use this command to create a new, or enter the existing MME group ID management database. The MME group ID management database is used to create associations between PLMN IDs and ranges of MME group IDs.

On the S4-SGSN, this command enables operators to create a MME group ID management database that can be associated with an SGSN service.

**Important:** Only one MME group ID management database can be created per system.

Entering this command results in the following prompt:

```
[context_name] host_name(network-global-mme-id-mgmt-db)#
```

Global MME ID management database commands are defined in the *LTE Network Global MME ID Management Database Configuration Mode Commands* chapter.
paging-map

Creates a paging map or specifies an existing paging map and enters the Paging Map Configuration Mode.

Product
MME
ePDG

Privilege
Administrator

Mode
Exec > Global Configuration > LTE Policy Configuration
configure > lte-policy
Entering the above command sequence results in the following prompt:

[local]host_name(lte-policy)#

Syntax

[ no ] paging-map paging_map_name [ -noconfirm ]

no
Remove the paging map from the system.

paging_map_name
Specifies the name of the paging map being created or accessed. If the map name does not refer to an existing map, a new map is created. paging_map_name must be an alphanumeric string of 1 through 64 characters.

-noconfirm
Executes the command without any additional prompt and confirmation from the user.

Usage

Enter the Paging Map Configuration Mode for an existing or newly defined map. This command is also used to remove an existing map.
Entering this command results in the following prompt:

hostname(paging-map)#

Paging Map Configuration Mode commands are defined in the LTE Paging Map Configuration Mode Commands chapter.
Refer to the Heuristic and Intelligent Paging chapter in the MME Administration Guide for more information about Paging Maps.

Example

The following command enters the existing Paging Map Configuration Mode (or creates it if it does not already exist) for the map named map1:

paging-map map1
paging-profile

Creates a paging profile or specifies an existing paging profile and enters the Paging Profile Configuration Mode.

**Product**
MME
ePDG

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > LTE Policy Configuration
configure > lte-policy

The above command sequence results in the following prompt:

```
[local]host_name(lte-policy)#
```

**Syntax**

```plaintext
[ no ] paging-profile paging_profile_name [ -noconfirm ]
```

- **no**
  Remove the paging map from the system.

- **paging_profile_name**
  Specifies the name of the paging profile being created or accessed. If the profile name does not refer to an existing profile, a new profile is created. `paging_profile_name` must be an alphanumeric string of 1 through 64 characters.

- **-noconfirm**
  Executes the command without any additional prompt and confirmation from the user.

**Usage**
Enter the Paging Profile Configuration Mode for an existing or newly defined paging profile. This command is also used to remove an existing profile.

Entering this command results in the following prompt:

```
hostname(paging-profile)#
```

Paging Profile Configuration Mode commands are defined in the *LTE Paging Profile Configuration Mode Commands* chapter.

Refer to the *Heuristic and Intelligent Paging* chapter in the *MME Administration Guide* for more information about Paging Profiles.

**Example**
The following command enters the existing Paging Profile Configuration Mode (or creates it if it does not already exist) for the profile named `profile1`:

```
paging-profile profile1
```
peer-map

Creates a peer map and enters the LTE Peer Map Configuration mode.

**Product**
- P-GW
- SAEGW
- S-GW

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > LTE Policy Configuration

configure > lte-policy

Entering the above command sequence results in the following prompt:

```
[local]host_name(lte-policy)#
```

**Syntax**

```
peer-map map_name [ -noconfirm ]
```

```
no peer-map map_name
```

- **map_name**
  Specify a name of a peer map to create, modify, or remove. This name must be an alphanumeric string of 1 through 64 characters. Each new peer map must have a unique name.

- **-noconfirm**
  Executes the command without any additional prompt and confirmation from the user.

**Usage**

Use this command to create or modify a peer map.

Entering this command results in the following prompt:

```
[local]host_name(peer-map)#
```

LTE Peer Map Configuration Mode commands are defined in the *LTE Peer Map Configuration Mode Commands* chapter of this guide.

**Example**

The following command creates a peer map named map5 and enters the LTE Peer Map Configuration mode:

```
peer-map map5
```
subscriber-map

Creates a subscriber map or specifies an existing subscriber map and enters the Subscriber Map Configuration Mode.

Product
- MME
- ePDG
- SAEGW
- S-GW

Privilege
- Administrator

Mode
- Exec > Global Configuration > LTE Policy Configuration
- configure > lte-policy

Entering the above command sequence results in the following prompt:

[local]host_name(lte-policy)#

Syntax

[ no ] subscriber-map map_name [ -noconfirm ]

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Removes the specified subscriber map from the system.</td>
</tr>
<tr>
<td>-noconfirm</td>
<td>Executes the command without any additional prompt and confirmation from the user.</td>
</tr>
<tr>
<td>map_name</td>
<td>Specifies the name of the subscriber map. If the map name does not refer to an existing map, a new map is created. map_name must be an alphanumeric string of 1 through 64 characters.</td>
</tr>
</tbody>
</table>

Usage

Enter the Subscriber Map Configuration Mode for an existing or newly defined map. This command is also used to remove an existing map.

Entering this command results in the following prompt:

hostname(subscriber-map)#

Subscriber Map Configuration Mode commands are defined in the LTE Subscriber Map Configuration Mode Commands chapter.

Example

The following command enters the existing Subscriber Map Configuration Mode (or creates it if it does not already exist) for the map named map1:

subscriber-map map1
**tai-list-db**

Creates or configures a list of Tracking Area Information (TAI). This list is called TAI List Database.

**Product**
HeNB-GW

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > LTE Policy Configuration

```
configure > lte-policy
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(lte-policy)#
```

**Syntax**

```
[ no ] tai-list-db  db_name [ -noconfirm ]
```

---

**no**

Removes the specified TAI list database from the system.

---

**-noconfirm**

Executes the command without any additional prompt and confirmation from the user.

---

**db_name**

Specifies the name of the TAI list database. If the name does not refer to an existing database, a new database is created. `db_name` is an alphanumeric string of 1 through 64 characters.

**Usage**

Enters the TAI List Database Configuration Mode for an existing or newly defined database. This command is also used to remove an existing database.

---

Important: Maximum of eight TAI List Database instances can be created in a system.

Entering this command results in the following prompt:

```
[context_name]hostname(tai-list-db)#
```

TAI List Database Configuration Mode commands are defined in the TAI List Database Configuration Mode Commands chapter.

**Example**

The following command enters the existing TAI List Database configuration mode (or creates it if it does not already exist) for the database named `tai_db1`:

```
tai-list-db  tai_db1
```
**tai-mgmt-db**

Creates a Tracking Area Identifier (TAI) Management Database or specifies an existing database and enters the TAI Management Database Configuration mode. On an S4-SGSN, this command is used as part of configuring S-GWs and their associated RAIs to bypass DNS resolution of RAI FQDN for obtaining the S-GW address.

**Product**
- MME
- ePDG
- SAEGW
- S-GW
- SGSN

**Privilege**
Administrator

**Mode**
- `Exec > Global Configuration > LTE Policy Configuration`
- `configure > lte-policy`

Entering the above command sequence results in the following prompt:

```
[local]host_name(lte-policy)#
```

**Syntax**

```
[ no ] tai-mgmt-db db_name [ -noconfirm ]
```

- no
  Removes the specified management database from the system.

- -noconfirm
  Executes the command without any additional prompt and confirmation from the user.

- db_name
  Specifies the name of the management database. If the name does not refer to an existing database, a new database is created. `db_name` is an alphanumeric string of 1 through 64 characters.

**Usage**

Enter the TAI Management Database Configuration Mode for an existing or newly defined database. This command is also used to remove an existing database.

On the S4-SGSN, once you have created a new, or accessed an existing, TAI Management database, a TAI Management Object must be created or accessed and the S-GWs and their associated RAIs configured using the `rai` and `sgw-address` commands. Refer to the `LTE TAI Object Configuration Mode` chapter for details on these two commands.

Entering this command results in the following prompt:

```
[context_name]host_name(tai-mgmt-db)#
```
TAI Management Database Configuration Mode commands are defined in the *TAI Management Database Configuration Mode Commands* chapter.

**Example**

The following command enters the existing TAI Management Database configuration mode (or creates it if it does not already exist) for the database named *tai_db1*:

```
tai-mgmt-db tai_db1
```
Chapter 207
LTE Subscriber Map Configuration Mode Commands

The LTE Subscriber Map Configuration Mode is used to create and manage subscriber maps for applying operator policy templates to individual subscribers and/or groups of subscribers.

Subscriber mappings are ordered lists containing explicit UE matching criteria. The maps are examined for specific UE identity information such as the UE’s IMSI. The system uses the first map that matches the criteria to associate an operator policy with the UE.

Subscriber maps can be modified but will only affect future subscribers and not subscribers already attached to UEs.

Mode

Exec > Global Configuration > LTE Policy Configuration > LTE Subscriber Map Configuration

configure > lte-policy > subscriber-map subscriber_map_name

Entering the above command sequence results in the following prompt:

[local]host_name(subscriber-map)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
end

**Usage**
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

exit

Usage
Use this command to return to the parent configuration mode.
precedence

Sets the order of precedence, the matching criteria and the association to an operator policy for subscribers meeting the match criteria.

Product
MME
SAEGW
S-GW

Privilege
Administrator

Mode
Exec > Global Configuration > LTE Policy Configuration > LTE Subscriber Map Configuration
configure > lte-policy > subscriber-map subscriber_map_name

Entering the above command sequence results in the following prompt:

[local]host_name(subscriber-map)#

Syntax

precedence number match-criteria all operator-policy-name policy_name

precedence number match-criteria imsi mcc mcc_num mnc mnc_num [ msein first start_range last end_range | service-plmnid id ] operator-policy-name policy_name

precedence number match-criteria [ imsi mcc mcc_num mnc mnc_num ] [ service-plmnid id ] ssid id operator-policy-name policy_name

precedence number match-criteria service-plmnid id operator-policy-name policy_name

no precedence number

no
Removes the selected precedence number from the subscriber map. number must be an integer value from 1 to 1024.

number
Specifies the order of precedence for the subscriber map. 1 is the highest precedence. number must be an integer value from 1 to 1024.

match-criteria
Specifies that the keyword following this keyword is the criteria to be used to match a UE.

all
Specifies that all UEs are to be associated with the operator policy.
###imsi mcc mcc_num mnc mnc_num [msin first start_range last end_range | service-plmnid id ]###

Specifies that UEs with criteria matching the International Mobile Subscriber Identifier (IMSI) information (MCC and MNC) are to be associated with a specified operator policy.

- **mcc mcc_num**: Specifies the mobile country code (MCC) portion of the IMSI identifier as an integer value between 100 and 999.
- **mnc mnc_num**: Specifies the mobile network code (MNC) portion of the IMSI identifier as a 2- or 3-digit integer value between 00 and 999.
- **msin first start_range last end_range**: Optionally specifies a range of Mobile Subscriber Identification Numbers that further narrows the match criteria for the IMSI match configuration.
  - *start_range* and *end_range* must each be an integer value of 10 digits.
- **service-plmnid id**: Optionally specifies a local service PLMN ID number used further narrow the IMSI-based operator policy selection. *id* must be an integer value of five digits minimum and six digits maximum (the combination of the MCC and MNC).

---

###service-plmnid id###

Specifies a local service PLMN ID number used for PLMN ID-based operator policy selection. *id* must be an integer value of five digits minimum and six digits maximum (the combination of the MCC and MNC).

---

###ssid id###

Specifies a local SSID used for SSID-based operator policy selection to support the SaMOG Local Break Out (LBO) feature. The operator policy and associated call control profile are selected based on the SSID received in the Called-Station-Id attribute in Access-Request.
- *id* must be an alphanumeric string of 1 through 32 characters.
- The SaMOG LBO feature is license dependant. Contact your Cisco account representative for more information.

---

###operator-policy-name policy_name###

Sets the operator policy with which the matching criteria is associated. *policy_name* must be an existing operator policy expressed as an alphanumeric string of 1 through 64 characters. Operator policies are configured in the Operator Policy Configuration Mode. For more information about operator policies, refer to the *Operator Policy Configuration Mode Commands* chapter.

---

###Usage###

The operator policy provides mechanisms to fine tune the behavior of subsets of subscribers above and beyond the behaviors described in the user profile. It is also used to control the behavior or visiting subscribers in roaming scenarios, enforce roaming agreements, and provide a measure of local protection against foreign subscribers.

---

###Example###

The following command associates the operator policy named *op_poll* with UEs associated with an IMSI MCC of 111, an MNC of 222, and a service PLMN ID of 123456:

```plaintext
precedence 100 match-criteria imsi mcc 111 mnc 222 service-plmnid 123456
operator-policy-name op_poll
```
Chapter 208
LTE TAI Management Database Configuration Mode Commands

The LTE TAI Management Database Configuration Mode is used to create and manage the LTE Tracking Area Identifier (TAI) management database on this system.

Mode

Exec > Global Configuration > LTE Policy Configuration > LTE TAI Management Database Configuration

configure > lte-policy > tai-mgmt-db db_name

Entering the above command sequence results in the following prompt:

[local]host_name(tai-mgmt-db)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
**end**

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**

Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
```
exit
```

**Usage**
Use this command to return to the parent configuration mode.
network-name

This command configures the long (full) and short network name used in the Long and Short network name IE in the EMM Information message that is sent to the UE from the MME.

Product
MME

Privilege
Administrator

Mode
Exec > Global Configuration > LTE Policy Configuration > LTE TAI Management Database Configuration
configure > lte-policy > tai-mgmt-db \( \text{db}_\text{name} \)

Entering the above command sequence results in the following prompt:

[local] \( \text{host}_\text{name}(\text{tai-mgmt-db}) \)#

Syntax

\[
\begin{align*}
[ \text{no} ] \ & \text{network-name} \ & [ \text{full} \ & \text{full}_\text{name} \ | \ & \text{short} \ & \text{short}_\text{name} ] \\
\text{no} \\
& \text{Removes a configured network-name.} \\
\text{full} \ & \text{full}_\text{name} \\
& \text{Defines the full (long) network name. } \text{full}_\text{name} \ & \text{is an alphanumeric string of 1 through 251 characters.} \\
\text{short} \ & \text{short}_\text{name} \\
& \text{Defines the short network name. } \text{short}_\text{name} \ & \text{is an alphanumeric string of 1 through 251 characters.}
\end{align*}
\]

Usage

Use this command to configure the full and short network name on the \( \text{tai-db} \) object.
This configuration affects the actions of the MME when the MME is configured to set the UE time. If this configuration exists, and there is no interaction with an MSC that sends a EMM INFORMATION message, the MME uses the above configuration while sending an EMM INFORMATION message.
There is no default for this configuration. If this configuration does not exist at the \( \text{tai-db} \) level and \( \text{tai-mgmt-object} \) level, no network name will be signaled in a EMM Information message.
tai-custom-list

Creates a new custom TAI list, and/or enters the tai-cstm-list configuration mode.

**Product**
MME

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > LTE Policy Configuration > LTE TAI Management Database Configuration
configure > lte-policy > tai-mgmt-db  *db_name*

Entering the above command sequence results in the following prompt:

```
[local]hostname(tai-mgmt-db)#
```

**Syntax**

tai-custom-list tac  *value*  [ -noconfirm ]

```
tac  *value*
```
Specifies the Tracking Area Code portion of the TAI as an integer from 1 through 65535.  
A maximum of 1000 Custom TAI Lists can be configured per TAI Management Database.

**Usage**
Use this command to enter the Custom TAI List Configuration Mode for an existing object or for a newly defined object.  
Prior to 17.0, the MME could have a tracking area in only one tracking area list (TAI List). Consequently, the tracking area list assigned to subscribers attaching from different TAI will be same, even if the adjacency of these tracking areas is not same. This resulted in the MME getting TAUs even as subscribers moved to the adjacent area.  
With this functionality, you can configure adjacency lists as TAI Lists, thus reducing the Tracking Area Updates (TAU) received by MME. This feature enables the MME to send configured customized TAI List in ATTACH_ACCEPT/TAU_ACCEPT when a request is received from the custom or border TAI.  
Entering this command results in the following prompt:

```
[local]hostname{tai-cstm-list}#
```

Custom TAI List Configuration Mode commands are defined in the LTE Custom TAI List Configuration Mode Commands chapter.

**Example**
The following command creates a Custom TAI List for TAC 2325 and enters the Custom TAI List Configuration Mode:

```
custom-tai-list tac 2325
```
tai-mgmt-obj

Creates new, or removes/enters existing, LTE Tracking Area Identifier (TAI) object configurations. On the S4-SGSN, this command is required as part of configuring S-GWs and their associated RAIs to bypass DNS resolution of RAI FQDN for obtaining the S-GW address.

Product
MME
SGSN

Privilege
Administrator

Mode
Exec > Global Configuration > LTE Policy Configuration > LTE TAI Management Database Configuration
configure > lte-policy > tai-mgmt-db db_name

Entering the above command sequence results in the following prompt:

[local]host_name(tai-mgmt-db)#

Syntax

[ no ] tai-mgmt-obj object_name [ -noconfirm ]

- no
Removes a configured TAI management object from the TAI management database.

- -noconfirm
Executes the command without any additional prompt and confirmation from the user.

- object_name
Specifies the name of the TAI management object and enters the LTE TAI Management Object Configuration Mode as an alphanumeric string of 1 through 64 characters.

Usage

Use this command to enter the LTE TAI Management Object Configuration Mode for an existing object or for a newly defined object. This command is also used to remove an existing object. 
On the S4-SGSN, after creating the TAI Management Object and entering TAI Management Object Configuration Mode, the rai and sgw-address commands are used to complete the S-GW for RAI configuration. Refer to the LTE TAI Management Object Configuration mode chapter for details on these commands.
Entering this command results in the following prompt:

[context_name]hostname(tai-mgmt-obj)#

LTE TAI Management Object Configuration Mode commands are defined in the LTE TAI Management Object Configuration Mode Commands chapter.
The following command creates a TAI management object called \textit{tai-obj3} and enters the LTE TAI Management Object Configuration Mode:

\texttt{tai-mgmt-obj tai-obj3}
**timezone**

Configures the timezone to be used for the UE timezone in S11 and Non Access Stratum (NAS) messages.

**Product**
MME

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > LTE Policy Configuration > LTE TAI Management Database Configuration

```bash
configure > lte-policy > tai-mgmt-db db_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(tai-mgmt-db)#
```

**Syntax**

```bash
timezone { + | - } hours value [ minutes { 0 | 15 | 30 | 45 } | daylight-savings-time-increment { 0 | 1 | 2 } ]
```

```bash
no timezone
```

Removes the timezone configuration from the management database.

**Usage**

Use this command to configure the timezone to be used for the UE timezone in S11 and NAS messages.
**Important:** Time zone configurations at the TAI Management Object level take precedence over time zone configurations at the TAI Management Database level. If neither is configured, the system defaults to the MME (system) time zone.

**Example**

The following command sets the timezone mapping for this management database to plus-3 hours and 15 minutes from UTC:

```
timezone + hours 3 minutes 15
```
Chapter 209
LTE TAI Management Object Configuration Mode Commands

The LTE TAI Management Object Configuration Mode is used to create and manage the LTE Tracking Area Identifiers for the TAI database.

Mode
Exec > Global Configuration > LTE Policy Configuration > LTE TAI Management Database Configuration > LTE TAI Management Object Configuration

```
configure > lte-policy > tai-mgmt-db db_name > tai-mgmt-objc obj_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(tai-mgmt-objc)#
```
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
exit
```

**Usage**
Use this command to return to the parent configuration mode.
**lai**

Configures a Location Area Identifier (LAI) for this TAI management object.

**Product**
MME

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > LTE Policy Configuration > LTE TAI Management Database Configuration > LTE TAI Management Object Configuration

`configure > lte-policy > tai-mgmt-db db_name > tai-mgmt-obj obj_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(tai-mgmt-obj)#
```

**Syntax**

```
lai mcc number mnc number lac area_code

no lai
```

**no lai**

Removes a configured LAI from the TAI management object.

```
mcc number
```

Specifies the mobile country code (MCC) portion of a PLMN identifier as an integer from 100 through 999.

```
mnc number
```

Specifies the mobile network code (MNC) portion of a PLMN identifier as a 2- or 3-digit integer from 00 through 999.

```
lac area_code
```

Specifies the Location Area Code portion of the TAI as an integer from 1 through 65535.

**Usage**

Use this command to configure an LAI for this management object.

**Example**

The following command adds an LAI to this management object with an MCC of **111**, an MNC of **22**, and a LAC of **101**:

```
lai mcc 122 mnc 22 lac 101
```
network-name

This command configures the long (full) and short network name used in the Long and Short network name IE in the EMM Information message that is sent to the UE from the MME.

Product
MME

Privilege
Administrator

Mode
Exec > Global Configuration > LTE Policy Configuration > LTE TAI Management Database Configuration > LTE TAI Management Object Configuration

configure > lte-policy > tai-mgmt-db db_name > tai-mgmt-obj obj_name

Entering the above command sequence results in the following prompt:

[local]host_name(tai-mgmt-obj)#

Syntax

[ no ] network-name [ full full_name | short short_name ]

no
Removes a configured network-name.

full full_name
Defines the full (long) network name. full_name is an alphanumeric string of 1 through 251 characters.

short short_name
Defines the short network name. short_name is an alphanumeric string of 1 through 251 characters.

Usage

Use this command to configure the full and short network name on the tai-mgmt-obj. This configuration affects the actions of the MME when the MME is configured to set the UE time. If this configuration exists, and there is no interaction with an MSC that sends an EMM INFORMATION message, the MME uses the above configuration while sending a EMM INFORMATION message. There is no default for this configuration. If this configuration does not exist at the tai-db level and tai-mgmt-object level, no network name will be signaled in a EMM Information message.
rai

Configures a Routing Area Identifier (RAI) for an associated S-GW for this TAI management object.

**Product**
SGSN

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > LTE Policy Configuration > LTE TAI Management Database Configuration > LTE TAI Management Object Configuration
configure > lte-policy > tai-mgmt-db db_name > tai-mgmt-obj obj_name

Entering the above command sequence results in the following prompt:

[local]host_name(tai-mgmt-obj)#

**Syntax**

```
rai mcc number mnc number lac area_code rac rac_value
```

```
no rai
```

**Usage**

On the S4-SGSN, use this command as part of the configuration of the selection of an SGW for RAI on the S4-SGSN for operators wishing to bypass the DNS resolution of RAI FQDN for obtaining the SGW address. Once the RAI is configured, the SGW address that serves this RAI must be configured with the `sgw-address` command. For details on this command, refer to the description of `sgw-address` in this chapter.

**Example**
The following command adds a RAI to this management object with an MCC of 111, an MNC of 22, and a LAC of 110:

```
rai mcc 111 mnc 22 lac 110
```
**sgw-address**

Configures an IP address for a Serving Gateway (S-GW), a supported S5/S8 protocol type, and selection weight used in a pool for S-GW selection. On an S4-SGSN, this command is used as part of the configuration to bypass DNS resolution of RAI FQDN for an S-GW.

**Product**
MME
SGSN

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > LTE Policy Configuration > LTE TAI Management Database Configuration > LTE TAI Management Object Configuration

```
configure > lte-policy > tai-mgmt-db db_name > tai-mgmt-obj obj_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(tai-mgmt-obj)#
```

**Syntax**

```
sgw-address ipv4_or_ipv6_address s5-s8-protocol { both | gtp | pmip } weight number

no sgw-address ipv4_or_ipv6_address s5-s8-protocol { both | gtp | pmip }

no sgw-address ipv4_or_ipv6_address s5-s8-protocol { both | gtp | pmip }
```

Removes the configured S-GW address from this TAI management object.

```
ipv4_or_ipv6_address
```

Specifies the IP address of the S-GW in the selection pool in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

Up to 32 S-GW addresses can be configured per TAI management object.

```
s5-s8-protocol { both | gtp | pmip }
```

Specifies the S5/S8 interface type found between the configured S-GW and the P-GW.

- **both**: Specifies that both the GTP and PMIP protocols are supported over the S5/S8 interface. The **both** option is not supported on the SGSN.
- **gtp**: Specifies that the GTP protocol is supported over the S5/S8 interface. This is the only option supported by the SGSN.
- **pmip**: Specifies that the PMIP protocol is supported over the S5/S8 interface. The **pmip** option is not supported on the SGSN.

```
weight number
```

Specifies the priority or weight of the S-GW address used during weighted round-robin selection within this TAI management object. **number** must be an integer from 1 through 100.
Usage
Use this command to configure a pool of S-GW addresses used for S-GW selection.
On the S4-SGSN, use this command to complete the configuration of bypassing DNS resolution of RAI
FQDN to obtain the S-GW address. This command is not valid on the S4-SGSN until the following
commands have been executed:

- `tai-mgmt-db` in *LTE Policy Configuration Mode*
- `tai-mgmt-obj` in *LTE Management Database Configuration Mode*
- `rai` in *LTE TAI Management Object Configuration Mode*

Example
The following command configures an S-GW with an IPv4 address of 10.2.3.4, a supported S5/S8 protocol
type of GTP, and a selection weight of 3:

```
sgw-address 10.2.3.4 s5-s8-protocol gtp weight 3
```
**tai**

Configures a Tracking Area Identifier (TAI) for this TAI management object.

**Product**
MME

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > LTE Policy Configuration > LTE TAI Management Database Configuration > LTE TAI Management Object Configuration

```
configure > lte-policy > tai-mgmt-db db_name > tai-mgmt-obj obj_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(tai-mgmt-obj)#
```

**Syntax**

```
[ no ] tai mcc number  mnc number { tac value } +
```

- **no**
  Removes a configured TAI from the TAI management object.

- **mcc number**
  Specifies the mobile country code (MCC) portion of a PLMN identifier as an integer from 100 through 999.

- **mnc number**
  Specifies the mobile network code (MNC) portion of a PLMN identifier as a 2- or 3-digit integer from 00 through 999.

- **tac value +**
  Specifies the Tracking Area Code portion of the TAI as an integer from 1 through 65535. Up to 16 TAC values can be entered on a single line.

**Usage**

Use this command to configure one or more TAIs for this management object. Up to 16 TAIs can be configured per management object.

**Example**

The following command adds a TAI to this management object with an MCC of 111, an MNC of 22, and a TAC value of 1001:

```
tai mcc 122 mnc 22 tac 1001
```
timezone

Configures the timezone to be used for the UE timezone in S11 and Non-Access Stratum (NAS) messages.

Product
MME

Privilege
Administrator

Mode
Exec > Global Configuration > LTE Policy Configuration > LTE TAI Management Database Configuration > LTE TAI Management Object Configuration

configure > lte-policy > tai-mgmt-db db_name > tai-mgmt-obj obj_name

Entering the above command sequence results in the following prompt:

[local]host_name(tai-mgmt-obj)#

Syntax

timezone { + | - } hours value [ minutes { 0 | 15 | 30 | 45 } | daylight-savings-time-increment { 0 | 1 | 2 } ]

no timezone

Removes the timezone configuration from the management object.

+ | -

Specifies the offset direction from Coordinated Universal Time (UTC).

hours value

Specifies the offset from UTC in hours as an integer from 0 through 14.

minutes { 0 | 15 | 30 | 45 }

Optionally specifies the offset minutes added to the hours value.

daylight-savings-time-increment { 0 | 1 | 2 }

Specifies the number of hours the timezone should be offset due to daylight savings time. This allows the MME to serve areas that have daylight savings time different than that of the MME. This keyword is available in release 14.0 and higher.

If the TAI management database/object is configured for daylight savings using this keyword, the daylight savings time adjustment is applied in these messages only if the system time is within a daylight savings period.

Usage

Use this command to configure the timezone to be used for the UE timezone in S11 and NAS messages.
**Important:** Time zone configurations at the TAI Management Object level take precedence over time zone configurations at the TAI Management Database level. If neither is configured, the system defaults to the MME (system) time zone.

**Example**

The following command sets the timezone mapping for this management object to plus-3 hours and 15 minutes from UTC:

```
timezone + hours 3 minutes 15
```
zone-code

Configures a zone code for the management object.

Product
MME

Privilege
Administrator

Mode
Exec > Global Configuration > LTE Policy Configuration > LTE TAI Management Database Configuration > LTE TAI Management Object Configuration

```
configure > lte-policy > tai-mgmt-db db_name > tai-mgmt-obj obj_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(tai-mgmt-obj)#
```

Syntax

```
zone-code zc_id

no zone-code
```

```
no

Removes the configured zone-code from the management object.

zc_id

Identifies the zone code configuration instance as an integer from 1 through 65535.

Usage

**Important:** While there is no limit to the number of zone codes that can be created, only 10 LACs per zone code can be defined.

Use this command to define zone code restrictions. Regional subscription data at the home subscriber service (HSS) is used to determine the regional subscription area in which the subscriber is allowed to roam. The regional subscription data consists of a list of zone codes which are comprised of one or more location areas (identified by a LAC) into which the subscriber is allowed to roam. Regional subscription data, if present in the Insert-Subscriber-Data-Request (IDR) and the Update-Location-Answer (ULA) from the HSS, defines the subscriber's subscription area for the addressed MME. It contains the complete list (up to 10 zone codes) that apply to a subscriber in the currently visited PLMN. During the Location Update procedure, the zone code list is received in the ULA from the HSS. The zone code list is validated against the configured values in this command. If matched, the Location Update procedure is allowed to proceed. If not matched, the response is that the Network Node Area is restricted and the Location Update procedure fails.

Example

The following command sets the zone code for this management object to 1:

```
zone-code 1
```
Chapter 210
MAG Service Configuration Mode Commands

The MAG Service Configuration Mode is used to create and manage a Mobility Access Gateway service in an HSGW (eHRPD network) or a P-MIP S-GW (LTE-SAE network). The MAG is the PMIP client and communicates with the Local Mobility Anchor (LMA) configured on a PDN Gateway (P-GW).

Mode

Exec > Global Configuration > Context Configuration > MAG Service Configuration

configure > context context_name > mag-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-mag-service)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
bind

Binds the service to a logical IP interface serving as the S2a (HSGW) or S5/S8 (S-GW) interface and specifies the maximum number of subscribers that can access this service over the configured interface.

Product
HSGW
S-GW

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > MAG Service Configuration

configure > context context_name > mag-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-mag-service)#

Syntax

bind address ip_address [ max-subscribers num ]

no bind address

no

Removes the interface binding from this service.

address ipv6_address

Specifies the IPv6 address of the interface configured as the S5/S8 interface. ipv6_address is specified in IPv6 colon-separated-hexadecimal notation.

max-subscribers num

Default: 1500000

Specifies the maximum number of subscribers that can access this service on this interface. num must be an integer from 0 through 3000000.

Important: The maximum number of subscribers supported depends on the installed license key and the number of active packet processing cards in the system. A fully loaded system can support 3,000,000 total subscribers. Refer to the license key command and the Usage section (below) for additional information.

Usage

Associate the MAG service to a specific logical IP address. The logical IP address or interface takes on the characteristics of an S2a or S5/S8 interface that provides the session connectivity to/from a P-GW. Only one interface can be bound to a service. The interface should be configured prior to issuing this command. This command also sets a limit as to the number of simultaneous subscribers sessions that can be facilitated by the service/interface at any given time.
When configuring the `max-subscribers` option, be sure to consider the following:

- The total number of S2a or S5/S8 interfaces you will configure
- The total number of subscriber sessions that all of the configured interfaces may handle during peak busy hours
- An average bandwidth per session multiplied by the total number of sessions
- The type of physical port to which these interfaces will be bound

Taking these factors into account and distributing your subscriber session across all available interfaces will allow you to configure your interfaces to optimally handle sessions without degraded performance.

**Example**

The following command would bind the logical IP interface with the address of 4551:0db8:85a3:08d3:3319:8a2e:0370:1344 to the MAG service and specifies that a maximum of 300,000 simultaneous subscriber sessions can be facilitated by the interface/service at any given time:

```
bind address 4551:0db8:85a3:08d3:3319:8a2e:0370:1344 max-subscribers 300000
```
encapsulation

Configures data encapsulation type to be used for specific MAG service.

Product
HSGW
S-GW

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > MAG Service Configuration

configure > context context_name > mag-service service_name

Entering the above command sequence results in the following prompt:

\[context_name]\host_name(config-mag-service)\$

Syntax

encapsulation { gre | ipip }

default encapsulation

default

Resets the encapsulation type to be used by this service to the default option of GRE.

gre: Specifies that GRE encapsulation is to be used for PMIPv6 tunnel data between the MAG and the Local Mobility Anchor (LMA). This is the default for this command.

ipip: Specifies that IP-in-IP encapsulation is to be used for PMIPv6 tunnel data between the MAG and the LMA.

Usage

Use this command to select the encapsulation type to be used for PMIPv6 tunnel data between the MAG and the LMA.

Example

The following command sets the encapsulation data to IP-in-IP:

encapsulation ipip
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Use this command to return to the parent configuration mode.
heartbeat

Configures the PMIPv6 heartbeat message interval, retransmission timeout, and max retransmission for the MAG Service.

Product
HSGW

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > MAG Service Configuration

configure > context context_name > mag-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-mag-service)#

Syntax

heartbeat { interval seconds | retransmission { max number | timeout seconds } }

default heartbeat { interval | retransmission { max | timeout } }

no heartbeat

no

Disables the PMIPv6 heartbeat functionality. The HSGW starts sending heartbeat request to peers when the heartbeat interval is configured.

default

Resets the specified parameter to the system default value.

interval seconds

The interval in seconds at which heartbeat messages are sent. seconds is an integer from 30 through 3600.
Default: 60

retransmission max number

The maximum number of heartbeat retransmissions allowed. number is an integer from 1 through 15.
Default: 3

retransmission timeout seconds

The timeout in seconds for heartbeat retransmissions. seconds is an integer from 1 through 20.
Default: 3
**Usage**

Proxy Mobile IPv6 (PMIPv6) is a network-based mobility management protocol to provide mobility without requiring the participation of the mobile node in any PMIPv6 mobility related signaling. The Mobile Access Gateway (MAG) service sets up tunnels dynamically to manage mobility for a mobile node. This command provides configuration of heartbeat messages between the MAG and LMA services to know the reachability of the peers, to detect failures, quickly inform peers in the event of a recovery from node failures, and allow a peer to take appropriate action.

**Example**

The following command enables PMIPv6 heartbeat messaging to known MAG service peers and sets the heartbeat interval to 160 seconds.

```
heartbeat interval 160
```
information-element-set

Identifies the information element set of mobility options to be used in Proxy Binding Update (PBU) messages sent by the MAG to the LMA.

Product
HSGW
S-GW

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > MAG Service Configuration
configure > context context_name > mag-service service_name
Entering the above command sequence results in the following prompt:
[context_name]host_name(config-mag-service)#

Syntax
information-element-set { custom1 | custom2 | standard }
default information-element-set

default
Resets the command to the default value of “standard”.

{ custom1 | standard }
custom1: Specifies that a custom set of mobility options will be used in proxy binding update messages that are sent in Vendor Specific Mobility Options. These options are:
• User Location Info
• Hardware Identifier
• Access Network Charging Identifier
custom2: Specifies that a custom set of mobility options will be used in proxy binding update messages that are sent in Vendor Specific Mobility Options. When enabled, BSID will be sent in S2a PMIPv6 message.
custom3: Specifies that a custom set of mobility options will be used in proxy binding update messages that are sent in Vendor Specific Mobility Options.
standard: Specifies that a standard set of mobility options are to be used in proxy binding update messages. 3GPP specification 29.275 defines these as Protocol Configuration Options.

Usage
Use this command to identify the type of information element set of mobility options to be used in PBU messages sent form the MAG to the LMA. The mobility options can be either standards-based (3GPP 29.275) or custom (vendor-specific as defined by 3GPP 29.275).

Example
The following command identifies the information element set of mobility options to use in PBU messages as custom:
information-element-set custom1
max-retransmissions

Configures maximum number of retransmissions of Proxy MIP control messages to the Local Mobility Anchor (LMA).

**Product**
- HSGW
- S-GW

**Privilege**
- Administrator

**Mode**
- Exec > Global Configuration > Context Configuration > MAG Service Configuration
- `configure > context context_name > mag-service service_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-mag-service)#
```

**Syntax**

```
max-retransmissions num
```

**default max-retransmissions**

```
default
```

Rests the maximum number of allowed retransmissions to the default value of 5.

```
num
```

Default: 5

Specifies the maximum number of times the MAG service will attempt to communicate with the LMA before it marks it as unreachable.

`count` must be an integer from 0 through 4294967295.

**Usage**

Use this command to limit the number of retransmissions to LMA before marking it as unreachable. If the value configured is reached, the call is dropped.

**Example**

The following command configures the maximum number of retransmissions for the MAG service to 3:

```
max-retransmissions 3
```
**mobility-option-type-value**

Changes the mobility option type value used in mobility messages.

**Product**
- HSGW
- S-GW

**Privilege**
- Administrator

**Mode**
- Exec > Global Configuration > Context Configuration > MAG Service Configuration
- configure > context context_name > mag-service service_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-mag-service)#
```

**Syntax**

```
mobility-option-type-value { custom1 | standard }
```

**default mobility-option-type-value**

- **default**
  - Sets the command to the default value of custom1.

- **custom1**
  - (Default) Non-standard type values used before they were defined by IANA.

- **standard**
  - Standard type values as defined by IANA. In addition, standard option uses type values defined in RFC 5844 for home address (HoA) options for the PMIPv6 PBU/PBA/revocation message.

**Usage**

Use this command to change the mobility option type value used in mobility messages.

**Example**

The following command changes the mobility option type value to standard:

```
mobility-option-type-value standard
```
policy

Configures policies applied to MAG service.

**Product**

HSGW

**Privilege**

Administrator

**Mode**

Exec > Global Configuration > Context Configuration > MAG Service Configuration

```bash
configure > context context_name > mag-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-mag-service)#
```

**Syntax**

```bash
policy include-bsid-binding-update { all | none { dereg | handoff | init | renew }
}
```

```
[ default ] policy include-bsid-binding-update
```

**default**

Restores the command to the default values of `init` and `handoff`.

```bash
include-bsid-binding-update { all | none { dereg | handoff | init | renew } }
```

Configures the MAG Service to include BSID (Base Station Identification) in the PBU (Proxy Binding Update) sent by MAG to the P-GW. By default, BSID information is included in the update (`handoff`) and initialization (`init`) packets.

- `all`: Include BSID in all the types of PBU that are sent.
- `none`: Include BSID in none of the PBUs.
- `dereg`: Include BSID in the PBU sent during deregistration.
- `handoff`: Include BSID in the PBU sent during handoff.
- `init`: Include BSID in the PBU sent during initialization.
- `renew`: Include BSID in the PBU sent during 'registration lifetime' renewal.

**Usage**

Configures policies applied to MAG service.

**Example**

The following command configures the MAG Service to include BSID in the PBU during initialization, ‘registration renewal’, and deregistration.

```bash
policy include-bsid-binding-update init renew dereg
```
reg-lifetime

Configures the Mobile IPv6 session registration lifetime for this service.

Product
HSGW
S-GW

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > MAG Service Configuration
configure > context context_name > mag-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-mag-service)#

Syntax
reg-lifetime seconds

default reg-lifetime

default
Resets the command value to the default setting of 600.

seconds
Default: 600
Sets the time value (in seconds) for session lifetimes for this service.
seconds must be an integer from 1 through 262140.

Usage
Use this command to limit PMIPv6 lifetime on this service. If the Proxy Binding Acknowledge (PBA) from the LMA contains a lifetime shorter or longer than what is specified, it is used instead.

Example
The following command sets the registration lifetime for Mobile IPv6 sessions using this service to 1200 seconds (20 minutes):

reg-lifetime 1200
renew-percent-time

Configures percentage of lifetime at which a registration renewal is sent to the Local Mobility Anchor (LMA).

**Product**
HSGW
S-GW

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > MAG Service Configuration

```
configure > context context_name > mag-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-mag-service)#
```

**Syntax**

```
renew-percent-time percent
```

```
default renew-percent-time
```

**Usage**

Use this command to specify when a registration renewal is sent to the LMA for subscribers using this service.

If the registration lifetime is 600 seconds (10 minutes) and this command is set to 75 (percent), then the registration renewal message is sent after 450 seconds of the registration lifetime has expired.

**Example**

The following command sets the registration renewal time for subscribers using this service to 90 percent of the registration lifetime:

```
renew-percent-time 90
```
retransmission-policy

Configures the retransmission policy for Proxy MIP control message retransmissions.

Product
HSGW

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > MAG Service Configuration

configure > context context_name > mag-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-mag-service)#

Syntax

retransmission-policy { exponential-backoff | normal }

default retransmission-policy

default

Returns the command to its default setting of exponential-backoff.

{ exponential-backoff | normal }

Sets the retransmission timeout behavior for this service.

exponential-backoff: Specifies that the Proxy Binding Update (PBU) retransmission uses an exponential backoff to increase the retransmission timeout for each retry.

normal: Specifies that the PBU retransmission uses the configured retransmission timeout value for all PBU retransmission retries.

Usage

Use this command to specify the retransmission policy for PMIP control messages.

Example

The following command sets the retransmission timeout policy for PMIP control packets to “normal”:

retransmission-policy normal
retransmission-timeout

Configures the maximum allowable time for the MAG service to wait for a response from the LMA before it attempts to communicate with the LMA again (if the system is configured to retry the LMA), or marks the LMA as unreachable.

Product
- HSGW
- S-GW

Privilege
- Administrator

Mode
- Exec > Global Configuration > Context Configuration > MAG Service Configuration
  - `configure > context context_name > mag-service service_name`

Syntax

```
retransmission-timeout time
```

```
[ default | no ] retransmission-timeout
```

- **default**
  - Resets the timeout setting to the default value of 3,000 milliseconds.

- **no**
  - Deletes a previously configured timeout value.

- **time**
  - Default: 3000
  - Specifies the maximum allowable time (in milliseconds) for the MAG service to wait for a response from the LMA before it: (a) attempts to communicate with the LMA again (if the system is configured to retry the LMA) or (b) marks the LMA as unreachable.
  - `time` must be an integer from 100 through 100000.

Usage

Use the retransmission timeout command in conjunction with the `max-retransmissions` command in order to configure the MAG services behavior when it does not receive a response from a particular LMA.

Example

The following command configures a retransmission timeout value of 5000 milliseconds:

```
retransmission-timeout 5000
```
**signalling-packets**

Enables the QoS Differentiated Services Code Point (DSCP) marking feature for IP headers carrying outgoing signalling packets.

**Product**
- HSGW
- S-GW

**Privilege**
- Administrator

**Mode**
- Exec > Global Configuration > Context Configuration > MAG Service Configuration
  
  ```
  configure > context context_name > mag-service service_name
  ```

  Entering the above command sequence results in the following prompt:

  ```
  [context_name]host_name(config-mag-service)#
  ```

**Syntax**

```
signalling-packets ip-header-dscp value
```

- **default**
  - Restores the specified parameter to its default setting of 0x0.

- **no**
  - Disables the specified functionality.

- **ip-header-dscp value**
  - Used to configure the QoS Differentiated Services Code Point (DSCP) marking for IP header encapsulation.
  - **value**: Represents the DSCP setting as the first six most-significant bits of the ToS field. It can be configured to any hexadecimal value from 0x0 through 0x3F. Default is 0x0.

**Usage**

Use this command to enable or disable the DSCP marking feature for IP headers carrying outgoing signalling packets. DSCP marking is disabled by default.

**Example**

The following command configures the HSGW service to support DSCP marking for IP headers carrying outgoing signalling packets:

```
signalling-packets ip-header-dscp 0x21
```
Chapter 211
MAP Service Configuration Mode Commands

The MAP Service Configuration Mode is used to configure properties for Mobile Application Part (MAP) service. Mobile Application Part (MAP) is a protocol which provides an application layer for the various nodes in the core mobile network and GPRS and UMTS core network to communicate with each other in order to provide services to mobile phone users. The MAP service provides the application-layer protocol support used to access the Home Location Register (HLR).

Mode

Exec > Global Configuration > Context Configuration > MAP Service Configuration

configure > context context_name > map-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-map-service-service_name)#

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
access-protocol

Configures access protocol parameters for the MAP service as defined for a specific SCCP network instance.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > MAP Service Configuration
configure > context context_name > map-service service_name
Entering the above command sequence results in the following prompt:

[context_name]host_name(config-map-service-service_name)#

Syntax

access-protocol sccp-network sccp_id ssn subsys_num
no access-protocol sccp-network sccp_id ssn subsys_num

<table>
<thead>
<tr>
<th>sccp-network sccp_id</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the ID number of the SCCP network to use for the SGSN connection.</td>
</tr>
<tr>
<td>sccp_id: Must be an integer from 1 to 16.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ssn subsys_num</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identifies the subsystem number for the destination.</td>
</tr>
<tr>
<td>subsys_num: Enter an integer from 1 through 255.</td>
</tr>
</tbody>
</table>

no

Removes the access protocol SCCP network instance ID from the configuration.

Usage
Use this command to associate access protocol parameters to a specific instance of the MAP service for an SCCP network.

Example
The following command associates the access protocols with the SCCP network ID #10:

access-protocol sccp-network 10
application-context-name

Configure the operation timer(s) for one or more MAP application contexts.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > MAP Service Configuration

configure > context context_name > map-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-map-service-service_name)#

Syntax

application-context-name application operation-timer value

default application-context-name application operation-timer

default

Resets the operation timers for all applications to system defaults.

application

Select one of the following applications to enable the application:

- **authentication-failure-report**: Sets the reporting operation timer for authentication failure. The setting range for this timer is 15 to 30 seconds and the default setting is 15 seconds.
- **cancel-location**: Sets the cancel location operation timer. The setting range for this timer is 15 to 30 seconds and the default setting is 15 seconds.
- **check-imei**: Sets the check-IMEI operation timer. The setting range for this timer is 15 to 30 seconds for releases 8.0 and 8.1 and 1 to 30 seconds for releases 9.0 and higher. The default setting is 15 seconds.
- **delete-subscriber-data**: Sets the delete subscriber data operation timer. The setting range for this timer is 15 to 30 seconds and the default setting is 15 seconds.
- **mo-fwd-sm**: Sets the operation timer for forwarding mobile-originated SMS. The setting range for this timer is 1 to 10 minutes and the default setting is 1 minute (60 seconds).
- **ms-purge**: Sets the operation timer for MS-purge function. The setting range for this timer is 15 to 30 seconds and the default setting is 15 seconds.
- **mt-fwd-sm**: Sets the operation timer for forwarding mobile-terminated SMS. The setting range for this timer is 1 to 10 minutes and the default setting is 1 minute (60 seconds).
- **ready-for-sm**: Sets the operation timer for the ready for SMS operation. The setting range for this timer is 15 to 30 seconds and the default setting is 15 seconds.
- **send-authentication-info**: Sets the operation timer for the sending authentication information operation. The setting range for this timer is 15 to 30 seconds and the default setting is 15 seconds.
• **stand-alone-insert-subscriber-data**: Sets the operation timer for the standalone insert subscriber data operation. The setting range for this timer is 15 to 30 seconds and the default setting is 15 seconds.

• **ugl-insert-subscriber-data**: Sets the operation timer for the insert subscriber data portion of the update GPRS location operation. The setting range for this timer is 15 to 30 seconds and the default setting is 15 seconds.

• **update-gprs-location**: Sets the operation timer for the update GPRS location operation. The setting range for this timer is 15 to 30 seconds and the default setting is 15 seconds.

---

**operation-timer value**

Configures the operation timer for the selected application. Timer values are indicated above.

---

**Usage**

Repeat this command entering a different application each time to enable multiple applications.

**Example**

```
application-context-name  stand-alone-insert-subscriber-data operation-timer operation-timer 20
```
auth-vectors

Configures the number of authorization vectors to be requested from the home location register (HLR) during call setup to provide subscriber authentication.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > MAP Service Configuration

`configure > context context_name > map-service service_name`

Entering the above command sequence results in the following prompt:

`
[context_name]host_name(config-map-service-service_name)#`

**Syntax**

`auth-vectors number-to-request number`

`default auth-vectors number-to-request`

**Usage**

Set the number of requests to be received from the HLR.

**Example**

```
auth-vectors number-to-request 4
```
end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

end

Usage

Use this command to return to the Exec mode.
**equipment-identity-register**

Defines the information relevant to the equipment-identity-register (EIR) used by the SGSN.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > MAP Service Configuration

```
configure > context context_name > map-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-map-service-service_name)#
```

**Syntax**

```
equipment-identity-register { isdn E.164_num | point code pt_code } [ check-imei-every-n-events times | source-ssn ssn] [ include-imsi ]
```

```
no equipment-identity-register { isdn E.164_num | point code pt_code ] [ include-imsi ]
```

---

**no**

Deletes the EIR configuration.

**isdn number**

Enter the E.164 number of the EIR.

*number* must be a string of 1 to 15 digits.

**point code pt_code**

Enter SS7 point code address of the EIR in dotted-decimal format according to variant settings:

- ITU Range 0.0.1 to 7.255.7
- ANSI Range 0.0.1 to 255.255.255
- TTC Range 0.0.1 to 15.31.255
- or a string of 1 to 11 characters

**source-ssn ssn**

Identifies the subsystem number (SSN) to be used.

*ssn* must be an integer from 1 to 255.

**check-imei-every-n-events times**

Configures the frequency with which a ‘check IMEI’ message is sent to the EIR. When set, the SGSN skips sending the ‘check IMEI’ message for the first N-1 where IMDI/IMEISV is received.

*times*:

- For releases 8.0 and 8.1, the value must be an integer from 1 to 15.
• For releases 15.0 and higher, the value must be an integer from 1 to 15.

**Important:** This feature requires the enabling of `verify-equipment-identity` for IMEI or IMEISV as specified with the `gmm retrieve-equipment-identity imei` command of the call-control-profile configuration mode.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>include-imsi</strong></td>
<td>Enables inclusion of IMSI checking during the IMEI check procedure. By default this function is not included.</td>
</tr>
</tbody>
</table>

**Usage**

Configure the identity of the EIR that the SGSN uses and the interaction parameters. Increasing the `check-imei-every-n-events` frequency enables the EIR to avoid overload as the number of data-only devices attaching to the network increases.

**Example**

Configure EIR with point code 1.255.1 to perform IMEI check after every 61st received Attach Request message:

```plaintext
equipment-identity-register point code 1.255.1 check-imei-every-n-events 62
```

Configure IMSI to be included in the MAP-CHECK-IMEI operation:

```plaintext
equipment-identity-register point code 1.255.1 check-imei-every-n-events 62 include-imsi
```
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Use this command to return to the parent configuration mode.
gmlc

This command identifies the gateway mobile location center (GMLC) associated with the Location Service functionality.

Product

SGSN

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > Context Configuration > MAP Service Configuration

configure > context context_name > map-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-map-service-service_name)#

Syntax

```
gmlc { isdn E.164_number | point-code point-code } [ gsn-address ipv4 address ] [ source-ssn SSN_value ]
```

```
no gmlc { isdn | point-code }
```

**no**

Deletes the GMLC configuration. When the **no** form of the command is used the SGSN aborts all active Location Requests towards that GMLC and stops the Location Service functions.

**isdn number**

Enter the E.164 number of the GMLC.

number: must be a string of 1 to 15 digits.

**Important:** **isdn** can not be used if **point-code** is used.

**point-code pt_code**

Enter SS7 point code address of the GMLC in dotted-decimal format according to variant settings:

- ITU Range 0.0.1 to 7.255.7
- ANSI Range 0.0.1 to 255.255.255
- TTC Range 0.0.1 to 15.31.255
- or a string of 1 to 11 characters

**Important:** **point-code** can not be used if **isdn** is used.
gsn-address  ipv4 address

Identifies the IP address of the GMLC of the local PLMN. The address will be published to the HLR in the MAP Update_GPRS_Location Request.

Important: Even though gsn-address is optional per the CLI grammar, this keyword is a mandatory parameter when configuring the GMLC for the location service feature in the SGSN.

source-ssn  ssn

Identifies the subsystem number (SSN) to be used.

ssn must be an integer from 1 to 255.

Usage

This command identifies the GMLC associated with the MAP Service configuration in support of the Location Services functionality enabled on the SGSN.

Only one GMLC can be defined per MAP Service configuration.

Related Commands:

• associate map-service in the Location Service configuration mode associates this MAP service when configuring Location Services functionality.

Example

Use a command similar to the following to define a gateway mobility location center (GMLC) with an ISDN ID of 491720499, a GSN address of 192.168.64.1, and an SSN of 131:

\[ \text{gmlc isdn 491720499 gsn-address 192.168.64.1 ssn 131} \]
This command enters the configuration mode for the home location register (HLR). The HLR is a database containing the subscriber profile information for all mobile stations (MS) / user equipment (UE) connecting to a specific GPRS or UMTS core network.

**Important:** The commands and options for this mode are documented in the HLR Configuration Mode chapter.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > MAP Service Configuration

```plaintext
configure > context context_name > map-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-map-service-service_name)#
```

**Syntax**

```plaintext
hlr
```
policy

This command configures the Transaction Capabilities Application Part (TCAP) -specific MAP policy for either ANSI or ITU SS7 variants.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > MAP Service Configuration
configure > context context_name > map-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-map-service-service_name)#

Syntax

[ default ] policy tcap { use-received-destination-address | use-received-source-address }

use-received-destination-address
Selecting this keyword overwrites stored CG and CD addresses with a new address received in first TC CNT msg

use-received-source-address
Selecting this keyword instructs the MAP service to use the received source address for the dialog.

Usage
Use this command to determine how TCAP will handle MAP messages.

Example

policy tcap use-received-destination-address
short-message-service

This command enables and disables the short message service (SMS service) and provides access to the SMS Service configuration mode.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > MAP Service Configuration
```
configure > context context_name > map-service service_name
```
Entering the above command sequence results in the following prompt:
```
[context_name]host_name(config-map-service-service_name)#
```

**Syntax**
```
short-message-service

no short-message-service
```

**Usage**
Disables the SMS service.

**Example**
Enter the command to access the SMS service configuration mode to fine tune the SMS functionality.
```
short-message-service
```
### timeout

Use this command to configure the m1 timeout value for the LCS procedure.

**Product**
SGSN

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > MAP Service Configuration

```
configure > context context_name > map-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-map-service-service_name)#
```

**Syntax**

```
timeout m1 seconds
```

**ml seconds**
This keyword sets the expiry value for the SGSN’s m1 timer, which sets the time the SGSN waits to send a negative PSL Response and clear the location request.

*seconds* is an integer from 60 to 600. Default is 120.

**Usage**
The m1 timer is used for location service (LCS) specific map message PSL (provide subscriber location). The gateway mobile location center (GMLC), associated with the LCS functionality, also maintains an m1 timer when it sends a PSL Request to the SGSN. If the GMLC’s timer expires before receiving a response from the SGSN, then the GMLC aborts the location procedure.

This command enables the operator to determine the amount of time the SGSN should wait before sending a negative PSL Response and clearing the location request to complete the LCS procedure.

**Example**
Set the expiry value of the m1 timer to 240 seconds.

```
timeout m1 240
```
Chapter 212
MIP HA Assignment Table Configuration Mode Commands

The Mobile IP HA Assignment Table Configuration Mode is used to assign specific Home Agent (HA) IP addresses to ranges of Mobile Node (MN) IP addresses.

Mode

Exec > Global Configuration > Context Configuration > MIP HA Assignment Table

configure > context context_name > mobile-ip ha assignment-table table_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-mobile-ip-ha-assignment)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
end

Exits the current configuration mode and returns to the Exec mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

end

**Usage**

Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**
Use this command to return to the parent configuration mode.
hoa-range

This command assigns ranges of Mobile Node (MN) IP addresses to specific Home agent IP addresses.

**Product**
HA

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > MIP HA Assignment Table

```
configure > context context_name > mobile-ip ha assignment-table table_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-mobile-ip-ha-assignment)#
```

**Syntax**

```
[ no ] hoa-range ip_address ip_address2 ha ip_address3
```

- **no**
  Removes the specified Home Agent assignment from the assignment table.

- **ip_address ip_address2**
  Specifies a range of MN IP addresses. *ip_address* and *ip_address2* must be specified in IPv4 dotted-decimal or IPv6 colon-separated notation.

- **ha ip_address3**
  Specifies the IP address of the Home Agent to assign to MNs that are within the specified range. *ip_address3* must be specified in IPv4 dotted-decimal or IPv6 colon-separated notation.

**Usage**

Use this command to assign ranges of MN IP addresses to specific HAs.

**Important:** A maximum of eight MIP HA assignment tables can be configured per context with a maximum of eight MIP HA assignment tables across all contexts.

**Important:** A maximum of 256 non-overlapping hoa-ranges can be configured per MIP HA Assignment table with a maximum of 256 non-overlapping hoa-ranges across all MIP HA Assignment tables.

**Example**

The following command assigns any MN IP address that falls in the range of 192.168.100.0 through 192.168.101.0 to the HA with the IP address of 192.168.200.10:

```
hoa-range 192.168.100.0 192.168.101.0 ha 192.168.200.10
```
Chapter 213
MIPv6 HA Service Configuration Mode Commands

The MIPv6 HA Service Configuration Mode is used to create and manage Mobile IPv6 (MIPv6) access privileges.

Mode

Exec > Global Configuration > Context Configuration > MIPv6HA Service Configuration
configure > context context_name > mipv6ha-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-mipv6ha-service)#

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
aaa accounting

Configures the sending of subscriber session AAA accounting by the Home Agent (HA) service.

Product
PDSN
HA

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > MIPv6HA Service Configuration
configure > context context_name > mipv6ha-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-mipv6ha-service)#

Syntax
[ no ] aaa accounting

  no

  Disables AAA accounting for the HA service.

Usage
Enabling the HA service will send all accounting data (start, stop, and interim) to the configured AAA servers. The default is AAA accounting enabled.

Important: In order for this command to function properly, AAA accounting must be enabled for the context in which the HA service is configured using the aaa accounting subscriber radius command.

Example
AAA accounting for the HA service can be disabled using the no version of the command.

The following command disables AAA accounting for the HA service:

  no aaa accounting
bind

Designates the address of the MIPv6HA service and specifies the maximum number of subscribers that can access this service over the interface.

Product
PDSN
HA

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > MIPv6HA Service Configuration

configure > context context_name > mipv6ha-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-mipv6ha-service)#

Syntax

bind address IPv6_address [ max-subscribers count ]

no bind address

no

Removes the bound address from the HA service.

address

Specifies the IPv6 address of the MIPv6HA service using IPv6 colon-separated-hexadecimal notation.

max-subscribers count

Default: 3000000

Specifies the maximum number of subscribers that can access this service on this interface.

count is an integer from 0 through 4000000.

Important: The maximum number of subscribers supported depends on the installed license key and the number of active packet processing cards installed in the system. Refer to the license key command for additional information.

Usage

Use this command to associate the HA service with a specific logical IP address. The logical IP address or interface takes on the characteristics of a Pi interface. Only one interface can be bound to a service. The interface should be configured prior to issuing this command.

This command also sets a limit as to the number of simultaneous subscribers sessions that can be facilitated by the service/interface at any given time.

When configuring the max-subscribers option, be sure to consider the following:

- The total number of interfaces that you will configuring for use as Pi interfaces
The maximum number of subscriber sessions that all of these interfaces may handle during peak busy hours

• The average bandwidth for each of the sessions
• The type of physical port to which these interfaces will be bound

Taking these factors into account and distributing your subscriber session across all available interfaces will allow you to configure your interfaces to optimally handle sessions without degraded performance.

Example

The following command binds the logical IP interface with the address of 2001:4A2B::1f3F to the HA service and specifies that a maximum of 600 simultaneous subscriber sessions can be facilitated by the interface/service at any given time.

```
bind address 2001:4A2B::1f3F max-subscribers 600
```

The following command disables a binding that was previously configured:

```
no bind address
```
default

Restore default values assigned for specified parameter.

Product
PDSN
HA

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > MIPv6HA Service Configuration

configure > context context_name > mipv6ha-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-mipv6ha-service)#

Syntax

default { aaa | refresh-advice-option | refresh-interval-percent | reg-lifetime | sequence-number-validate | setup-timeout | simul-bindings | subscriber | timestamp-replay-protection }

aaa
Restores the AAA setting configured by the aaa command to its default of enabled.

refresh-advice-option
Restores the refresh-advice-option setting to its default of disabled.

refresh-interval-percent
Restores the refresh-interval-percent setting to its default of 75.

reg-lifetime
Restores the Mobile IP session registration lifetime setting configured by the reg-lifetime command to its default: 600 seconds.

sequence-number-validate
Restores the sequence-number-validate setting to its default of enabled.

setup-timeout
Restore the maximum amount of time allowed for setting up a session to the default: 60 seconds.

simul-bindings
Restores the simultaneous bindings setting to its default: 1.
subscriber
Configures settings for the default subscriber.

timestamp-replay-protection
Restores the timestamp-replay-protection scheme according to RFC 4285.

Usage
After the system has been modified from its default values, this command is used to set or restore specific parameters to their default values.

Example
The following command is used to return the simultaneous bindings setting parameter to it’s default value:

default simul-bindings
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
exit

**Usage**
Use this command to return to the parent configuration mode.
refresh-advice-option

Configures inclusion of refresh advice option in the Binding Acknowledgement sent by the Home Agent (HA).

- **Product**: PDSN, HA
- **Privilege**: Security Administrator, Administrator
- **Mode**: Exec > Global Configuration > Context Configuration > MIPv6HA Service Configuration

```
configure > context context_name > mipv6ha-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-mipv6ha-service)#
```

- **Syntax**: `refresh-advice-option`

- **Usage**: Includes the refresh advice option in the binding acknowledgements sent by the home agent. Default is disabled.
refresh-interval-percent

Configures the percentage of the granted lifetime to be used in the refresh interval mobility option in the Binding Acknowledgement sent by the Home Agent (HA).

Product
PDSN
HA

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > MIPv6HA Service Configuration

configure > context context_name > mipv6ha-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-mipv6ha-service)#

Syntax

refresh-interval-percent value

value

value represents a percentage expressed as an integer from 1 through 99. Default is 75.

Usage
Use this command to configure the amount of the granted lifetime to be used in the refresh interval mobility option in the Binding Acknowledgement sent by the Home Agent (HA).

Example
The following command sets the refresh-interval-percent value to 50%:

refresh-interval-percent 50
**reg-lifetime**

Specifies the longest registration lifetime that the HA service will be allowed in any Registration Request message from the mobile node.

**Product**

PDSN

HA

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > MIPv6HA Service Configuration

```
configure > context context_name > mipv6ha-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-mipv6ha-service)#
```

**Syntax**

```
reg-lifetime time

no reg-lifetime
```

- **time**

  Specifies the registration lifetime in seconds. `time` is an integer from 1 through 262140. Default is 600.

- **no**

  Sets the registration lifetime to infinite.

**Usage**

Use to limit a mobile nodes’ lifetime. If the mobile node requests a shorter lifetime than what is specified, it is granted. However, Per RFC 2002, should a mobile node request a lifetime that is longer than the maximum allowed by this parameter, the HA service will respond with the value configured by this command as part of the Registration Reply.

**Example**

The following command configures the registration lifetime for the HA service to be 2400 seconds:

```
reg-lifetime 2400
```

The following command configures an infinite registration lifetime for MIPv6 calls:

```
no reg-lifetime
```
sequence-number-validate

Configures sequence number validation of the received MIPV6 control packet by the Home Agent (HA) according to RFC 3775.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > MIPv6HA Service Configuration

```bash
configure > context context_name > mipv6ha-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name] host_name(config-mipv6ha-service) #
```

**Syntax**

```bash
sequence-number-validate
```

**Usage**

Use this command to enable sequence number validation of the received MIPV6 control packet by the Home Agent (HA) as per RFC 3775. Default is enabled.
setup-timeout

The maximum amount of time allowed for session setup.

**Product**
- PDSN
- HA

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration > Context Configuration > MIPv6HA Service Configuration
  
- `configure > context context_name > mipv6ha-service service_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-mipv6ha-service)#
```

**Syntax**

```
setup-timeout seconds
```

seconds

Default: 60 seconds

The maximum amount of time (in seconds) to allow for setup of a session expressed as an integer from 1 through 1000000. Default is 60 seconds.

**Usage**

Use this command to set the maximum amount of time allowed for setting up a session.

**Example**

To set the maximum time allowed for setting up a session to 5 minutes (300 seconds), enter the following command:

```
setup-timeout 300
```
**simul-bindings**

Specifies the maximum number of “care-of” addresses that can be simultaneously bound for the same user as identified by NAI and Home address.

**Product**
- PDSN

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration > Context Configuration > MIPv6HA Service Configuration
  - `configure > context context_name > mipv6ha-service service_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-mipv6ha-service)#
```

**Syntax**

```
simul-bindings number
```

`number`

Configures maximum number of “care-of” addresses that can be simultaneously bound for the same user as identified by their NAI and home address. `number` is an integer from 1 through 3. Default is 1.

**Usage**

Per RFC 2002, the HA service creates a mobile binding record (MBR) for each subscriber session it is facilitating. Each MBR is associated with a care-of address. As the mobile node roams, it is possible that the session will be associated with a new care-of address.

Typically, the HA service will delete an old binding and create a new one when the information in the Registration Request changes. However, the mobile could request that the HA maintains previously stored MBRs. This command allows you to configure the maximum number of MBRs that can be stored per subscriber if the requested.

**Example**

The following command configures the service to support up to 2 addresses per subscriber:

```
simul-bindings 2
```
timestamp-replay-protection tolerance

Designates timestamp replay protection scheme as per RFC 4285.

Product
PDSN
HA

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > MIPv6HA Service Configuration

configure > context context_name > mipv6ha-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-mipv6ha-service)#

Syntax

```
timestamp-replay-protection tolerance seconds
```

tolerance seconds

Defines the acceptable difference in timing (between timestamps) before rejecting packet, in seconds.

seconds must be an integer from 0 through 65535. The default is 7.

Usage

Use this command to define the acceptable difference in timing (between timestamps) before rejecting packet.
Chapter 214
MME LAC Pool Area Configuration Mode Commands

The MME LAC Pool Area Configuration Mode is used to create and manage the Location Area Code (LAC) pool areas.

Mode

Exec > Global Configuration > Context Configuration > SGs Service Configuration > MME LAC Pool Area Configuration

configure > context context_name > sgs-service service_name > pool-area pool_area_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-sgs-pool-area)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

- **Product**: All
- **Privilege**: Security Administrator, Administrator
- **Syntax**: `exit`

**Usage**
Use this command to return to the parent configuration mode.
hash-value

Configures the Visitor Location Register (VLR) hash value mapping for this pool area.

**Product**
MME

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > SGs Service Configuration > MME LAC Pool Area Configuration

configure > context context_name > sgs-service service_name > pool-area pool_area_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgs-pool-area)#
```

**Syntax**

```
hash-value { value | non-configured-values | range value to value } use-vlr vlr_name

no hash-value { value | non-configured-values | range value to value }
```

---

**no**
Removes the configured hash-value from the pool-area configuration.

**value**
Specifies the VLR hash value to be used with the configured VLR. `value` must be an integer from 0 through 999.

**non-configured-values**
Specifies that the VLR configured in this command is to be used non-configured hash values.

**range value to value vlr_name**
Specifies a range of hash values to use with the configured VLR as an integer from 0 through 999.

**use-vlr**
Specifies the VLR to be used with the hash value configuration in this command.

---

**Usage**

Use this command to configure hash values to be used with VLRs.
In Release 12.2 and later, a maximum of 48 hash lists can be created per pool area. In older releases, a total of 32 hash lists can be created per pool area.
In a pool configuration, the MME selects the VLR that corresponds to the hash of the UE’s IMSI. If that VLR is inactive, the MME will use the default VLR (as defined by the `non-configured-value` option). If no
default VLR has been configured, or if the default VLR is inactive, the MME selects any other available VLR from the pool.
If the chosen VLR is active at the time of selection and then subsequently becomes inactive when the request is sent to it, the current request fails. On the next request from the UE, the VLR selection mechanism is applied again. A VLR that failed previously will only be selected again if it became active since the earlier failure.

**Example**

The following command configures all hash values within a range of 0 to 500 to use a VLR named `vlr1`:

```
hash-value range 0 to 500 use-vlr vlr1
```

The following command configures hash values of 501 to use a VLR named `vlr2`:

```
hash-value 501 use-vlr vlr2
```

The following command configures all non-configured hash values to use a VLR named `vlr3`:

```
hash-value non-configured-values use-vlr vlr3
```
lac

Configures a 3G location area code or area codes that define this pool area.

Product
MME

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > SGs Service Configuration > MME LAC Pool Area Configuration

configure > context context_name > sgs-service service_name > pool-area pool_area_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-sgs-pool-area)#

Syntax

```plaintext
[ no ] lac { area_code } +
```

- **no**
  Removes a configured forbidden handover area code or area codes from this policy. If no location area code is specified, then all location area codes are removed.

- **area_code**
  Specifies an area code or area codes used to select a VLR for the pool area as an integer from 0 through 65535. Multiple area codes can be entered (up to 16 in a single line, separated by spaces).

Usage

Use this command to configure 3G location-based area codes that define this pool area.

In Release 12.2 and later, a maximum of 96 areas can be added per pool area (in a single line, or separately).

In older releases, a total of 16 area codes can be added (in a single line, or separately).

Example

The following command configures eight location-based area codes (1, 2, 3, 4, 5, 6, 7, 8) that define this pool area:

`lac 1 2 3 4 5 6 7 8`
plmnid

Configures the Public Land Mobile Network (PLMN) identifier for the LAC pool area.

**Product**
MME

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > SGs Service Configuration > MME LAC Pool Area Configuration

```
configure > context context_name > sgs-service service_name > pool-area pool_area_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgs-pool-area)#
```

**Syntax**

```
plmnid { any | mcc mcc_value mnc mnc_value }

no plmnid
```

- **no**
  - Removes the configured PLMN identifier for the LAC pool area.

- **any**
  - This keyword specifies any PLMN identifier can be configured for the LAC pool area.

  ```
  mcc mcc_value
  ```
  - Specifies the mobile country code (MCC) portion of the PLMN identifier as an integer from 100 through 999.

  ```
  mnc mnc_value
  ```
  - Specifies the mobile network code (MNC) portion of the PLMN identifier as a 2- or 3-digit integer from 00 through 999.

**Usage**
Use this command to set the PLMN identifier for the LAC pool area. Any PLMN identifier can be configured for the LAC pool area or a specific PLMN identifier can be configured by providing the MCC and MNC of the PLMN identifier.

**Example**

The following command configures the PLMN identifier with MCC value as 102 and MNC value as 20 for this MME service:

```
plmnid mcc 102 mnc 20
```
Chapter 215
MME MSC Pool Area Configuration Mode

The MME MSC Pool Area Configuration Mode is used to create and manage the MSC Pool Areas used by the MME for communicating with the Mobile Switching Center (MSC) for Single Radio Voice Call Continuity (SRVCC).

*Important:* The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Use this command to return to the parent configuration mode.
hash-value

Configures the selection of MSC in a MSC pool area based on the hash value derived from the IMSI.

**Product**
MME

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > MME Service Configuration > Pool Area Configuration

```
configure > context context_name > mme-service service_name > pool-area pool_area_name
type hash
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-mme-pool-area-hash-value)#
```

**Syntax**

```
hash-value { hash_value | range start_value to end_value } use-msc msc_id

no hash-value { hash_value | range start_value to end_value }
```

**Usage**
This command associates an MSC with this pool. It also assigns an the MSC to use based on the hash value as computed from the IMSI digits \([(\text{IMSI} \text{ div } 10) \text{ modulo } 1000]\). A maximum of 24 hash values can be configured within each pool area. If no matching MSC is found, the SRVCC handover fails.

**Example**

```
Cisco ASR 5x00 Command Line Interface Reference
```
The following command configures hash values from 111 to 222 to use the MSC named `mscwest1` in this pool.

```
hash-value range 111 to 222 use-msc mscwest1 arg1
```
plmn-id

Associates a Public Land Mobile Network (PLMN) identifier with a Mobile Switching Center (MSC) pool area.

Product
MME

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > MME Service Configuration > Pool Area Configuration

configure > context context_name > mme-service service_name > pool-area pool_area_name
type hash-value

or
configure > context context_name > mme-service service_name > pool-area pool_area_name
type round-robin

Entering the above command sequences result in the following prompts, respectively:

[context_name]host_name(config-mme-pool-area-hash-value)#

[context_name]host_name(config-mme-pool-area-round-robin)#

Syntax

plmn-id mcc code mnc code

no plmn-id

no

Removes the configured plmn-id assigned to this MSC pool area.

mcc code

Specifies the Mobile Country Code for this mobile access network. code must be a three-digit integer from 200 to 999.

mnc code

Specifies the Mobile Network Code for this mobile access network. code must be a two or three-digit integer from 00 to 999.

Usage

Use this command to associate a PLMN with an MSC pool area. This PLMN is used to select an MSC pool area based on the target PLMN as specified in the SRVCC handover request.

When configured, the MME attempts to select an MSC using the following selection order:
1. Pool area that matches the PLMN and of type hash.
2. Pool area that matches the PLMN and of type round-robin.
3. Pool area that does not have PLMN associated and of type hash.
4. Pool area that does not have PLMN associated and of type round-robin.
When this command is used, only one PLMN can be assigned per pool area of the same type (either hash-value or round-robin). A hash value pool area and a separate round robin pool area can be configured with the same PLMN. In this case, the hash value pool has the higher priority.

If no matching MSC is found, the SRVCC handover fails.

**Example**

The following command identifies the mobile network with a MCC of 123 and a MNC of 12.

```
plmn-id mcc 123 mnc 12
```
**use-msc**

Associates a Mobile Switching Center (MSC) with the pool area.

**Product**
MME

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > MME Service Configuration > Pool Area Configuration
configure > context context_name > mme-service service_name > pool-area pool_area_name
type round-robin

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-mme-pool-area-round-robin)#
```

**Syntax**

```
[ no ] use-msc msc_name
```

- **no**
  - Removes the associated MSC name from this pool area.

**Example**

The following command associates the MSC named `mscsouth1` to this pool.

```
use-msc mscsouth1
```
The MME Pool configuration is used to configure one or more MMEs to which the HeNB-GW is to communicate. This configuration is available under lte-policy configuration mode. Adding or modifying an MME pool instance puts the user into the MME Pool configuration mode.

**Mode**

Exec > Global Configuration > LTE Policy Configuration > HeNBGW MME Pool Configuration

`configure > lte-policy > henbgw mme-pool mme_pool_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(mme-pool)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**
Use this command to return to the Exec mode.
**exit**

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**
Use this command to return to the parent configuration mode.
mme

Configures a specific MME to HeNBGW.

Product
HeNB-GW

Privilege
Administrator

Mode
Exec > Global Configuration > LTE Policy Configuration > HeNBGW MME Pool Configuration

configure > lte-policy > henbgw mme-pool mme_pool_name

Entering the above command sequence results in the following prompt:

[local]host_name(mme-pool)#

Syntax

[ no ] mme mme_name { ipv4-address ipv4_address [ ipv4-address ipv4_address ] | ipv6-address ipv6_address [ ipv6-address ipv6_address ] [ sctp port port_val ] }

no

Removes the configured MME to HeNBGW.

mme_name

It is the MMe name, a string of size 1 through 63.

ipv4-address ipv4_address

Specifies the remote SCTP IP Address for S1 association to MME. This must be followed by ipv4_address, the IPv4 address using dotted-decimal notation.

ipv6-address ipv6_address

Specifies the remote SCTP IP Address for S1 association to MME. This must be followed by ipv6_address, the IPv6 address using (::/::).

sctp

Configure the S1-MME SCTP parameters.

port port_val

Designates SCTP port.
port_val is an integer ranging from 1 through 65535.

Usage

Use this command to configure a specific MME to HeNBGW.
The following command configures the mme with name `my_mme`, `ipv4-address` 123.456.234.444 with SCTP `port` 302.

```
mme my_mme ipv4-address 123.456.234.444 sctp port 302
```
The MME Service Configuration Mode is used to create and manage the LTE Mobility Management Entity (MME) services for the LTE/SAE network. This service works in conjunction with MME-HSS Service and eGTP Service.

Mode

Exec > Global Configuration > Context Configuration > MME Service

configure > context context_name > mme-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-mme-service)#

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

**Caution:** Restarting the MME service leads to termination of UE sessions at the MME, purge of subscriber data and closure of all connections towards peer nodes such as eNodeB, HSS, S-GW, etc. It may also lead to termination of other services associated with the MME. It is strongly advised to make any configuration changes that restarts the service only while in maintenance mode or at startup.
**associate**

Associates or disassociates supportive services and policies, such as an Evolved GPRS Tunnelling Protocol (eGTP) service, an HSS peer service, or an MME policy subscriber map with an MME service.

**Product**
MME

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > MME Service

`configure > context context_name > mme-service service_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-mme-service)#
```

**Syntax**

```
associate { { egtp-service egtp_svc_name | egtp-sv-service egtp_sv_svc_name | foreign-plmn-guti-mgmt-db db_name | hss-peer-service hss_svc_name | location-service location_svc_name | lte-emergency-profile profile_name | network-global-mme-id-mgmt-db | sctp-param-template template_name | sgs-service sgs_svc_name | sgtpc-service sgtpc_svc_name } [ context ctx_name ] | subscriber-map map_name | tai-mgmt-db database_name }`

```

no associate { egtp-service | egtp-sv-service | foreign-plmn-guti-mgmt-db | hss-peer-service | location-service | lte-emergency-profile | network-global-mme-id-mgmt-db | sctp-param-template | sgs-service | sgtpc-service | subscriber-map | tai-mgmt-db }
```

**no**

Disassociates a previously associated service with this MME service.

**egtp-service egtp_svc_name**

Associates an eGTP service with MME service.

`egtp_svc_name` specifies the name for a pre-configured eGTP service to associate with the MME service. The eGTP service provides eGTP-C protocol interface support between EPS nodes. For more information on the eGTP service, refer to the `egtp-service` command in the **Context Configuration Mode Commands** chapter and the **eGTP Service Configuration Mode Commands** chapter.

Only one eGTP service can be associated with a service. The eGTP service should be configured prior to issuing this command.

**egtp-sv-service egtp_svc_name**

Associates an eGTP Sv service with this MME service.

`egtp_svc_name` specifies the name for a pre-configured eGTP Sv service to associate with the MME service. For more information on the eGTP Sv service, refer to the `egtp-service` command in the **Context Configuration Mode Commands** chapter.
**foreign-plmn-guti-mgmt-db**  
*db_name*

Associates a Foreign PLMN GUTI management database with this MME service.  
*db_name* specifies the name for a pre-configured foreign PLMN GUTI management database to associate with the MME service. For more information on the Foreign PLMN GUTI management database, refer to the **foreign-plmn-guti-mgmt-db** command in the LTE Policy Configuration Mode Commands chapter. Only one Foreign PLMN GUTI management database can be associated to an MME service. The Foreign PLMN GUTI management database should be configured prior to issuing this command. Multiple MME services can be associated to the same Foreign PLMN GUTI management database.

**hss-peer-service**  
*hss_svc_name*

Associates an HSS peer service with this MME service.  
*hss_svc_name* specifies the name for a pre-configured HSS peer service to associate with the MME service as an alphanumeric string of 1 through 64 characters. The HSS peer service provides S6a and S13 interface support via the Diameter protocol between the MME and an HSS (S6a) or EIR (S13). For more information about the HSS peer service, refer to the **hss-peer-service** command in the Context Configuration Mode Commands chapter and the HSS Peer Service Configuration Mode Commands chapter. Only one HSS peer service can be associated to a service. The HSS peer service should be configured prior to issuing this command.

**ipne-service**  
*ipne_svc_name*

Associates an IPNE service with this MME service.  
*ipne_svc_name* must be an alphanumeric string of 1 to 63 characters to identify a pre-configured, uniquely-named IPNE service. For more information about the IPNE service, refer to the sections for the IPNE Service Configuration Mode Commands and the IPNE Endpoint Configuration Mode Commands.

**location-service**  
*location_svc_name*

Associates a location service with this MME service. Only one location service should be associated with an MME Service.  
*location_svc_name* specifies the name for a pre-configured location service to associate with the MME service as an alphanumeric string of 1 through 64 characters. For more information about Location Services (LCS), refer to the **location-service** command in the Context Configuration Mode Commands chapter and the Location Services Configuration Mode Commands chapter.

**lte-emergency-profile**  
*profile_name*

Associates an LTE emergency profile with this MME service.  
*profile_name* specifies the name for a pre-configured LTE emergency profile to associate with the MME service as an alphanumeric string of 1 through 64 characters. For more information about the LTE emergency profile, refer to the **lte-emergency-profile** command in the LTE Policy Configuration Mode Commands chapter and the LTE Emergency Profile Configuration Mode Commands chapter.

**network-global-mme-id-mgmt-db**

Associates the configured global MME ID management database with this MME service. The global MME ID management database is configured through the LTE Policy Configuration Mode using the **network-global-mme-id-mgmt-db** command.

**sctp-param-template**  
*template_name*

Associates a Stream Control Transmission Protocol (SCTP) parameter template with this MME service.
associate

template_name specifies the name for a pre-configured SCTP parameter template to associate with this
MME service as an alphanumeric string of 1 through 63 characters. For more information on the SCTP
parameter template, refer to the sctp-param-template command in the Global Configuration Mode
Commands chapter and the SCTP Parameter Template Configuration Mode Commands chapter.

sgs-service  sgs_svc_name

Associates an SGs service with this MME service.
sgs_svc_name specifies the name for a pre-configured SGs service to associate with the MME service as an
alphanumeric string of 1 through 64 characters. For more information on the SGs service, refer to the sgs-
service command in the Context Configuration Mode Commands chapter and the MME SGs Service
Configuration Mode Commands chapter.

sgtpc-service  sgtpc_svc_name

Associates an SGTPC service with this MME service.
sgtpc_svc_name specifies the name for a pre-configured SGTPC service to associate with the MME service
as an alphanumeric string of 1 through 64 characters.

**Important:** When co-locating an SGSN and MME, the MME Service cannot be associated with the same SGTP
service that is used by the SGSN.

For more information on the SGTPC service, refer to the sgtpc-service command in the Context
Configuration Mode Commands chapter and the SGTP Service Configuration Mode Commands chapter.

context  ctx_name

Identifies a specific context name where the named service is configured. If this keyword is omitted, the
named service must exist in the same context as the MME service.
ctx_name is name of the configured context of the named service expressed as an alphanumeric string of 1
through 63 characters that is case sensitive.

subscriber-map  map_name

Associates this MME service with a pre-configured subscriber map.
map_name specifies the name of a pre-configured subscriber map to associate with the MME service as an
alphanumeric string of 1 through 64 characters. For more information on subscriber maps, refer to the
subscriber-map command in the LTE Policy Configuration Mode Commands chapter and the LTE
Subscriber Map Configuration Mode Commands chapter.

tai-mgmt-db  database_name

Associates this MME service with a pre-configured TAI Management Database.
database_name specifies the name of a pre-configured TAI Management Database to associate with the
MME service as an alphanumeric string of 1 through 64 characters. For more information on subscriber maps,
refer to the tai-mgmt-db command in the LTE Policy Configuration Mode Commands chapter and the LTE
TAI Management Database Configuration Mode Commands chapter.

**Usage**

Use this command to associate a pre-configured service or policy with an MME service.
Caution: This is a critical configuration. The MME service cannot be started without this configuration. Any change to this configuration will cause the MME service to be restarted. Removing or disabling this configuration will stop the MME service.

Example

The following command associates a pre-configured eGTP service called egtp1 in the dst_ctx context to an MME service:

associate egtp-service egtp1 context dst_ctx

The following command associates a pre-configured HSS peer service called hss1 in the same context as MME service to an MME service:

associate hss-peer-service hss1
bind s1-mme

Binds the MME service to a logical IP interface serving as the S1-MME interface.

**Important:** Before modifying this bind configuration using the `no bind s1-mme` command, we recommend that the MME Administrator use the `clear mme-service db record` command, under the Exec mode, to empty the MME records database.

**Product**
MME

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > MME Service

`configure > context context_name > mme-service service_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-mme-service)#
```

**Syntax**

```
bind s1-mme { ipv4-address address [ ipv4-address secondary_address ] | ipv6-address address [ ipv6-address secondary_address ] } [ crypto-template name ] [ max-subscribers number ]
```

**no bind s1-mme**

```
no
```

Removes a previously configured IP address used for binding the SCTP (local bind address) to communicate with the eNodeBs using an S1-MME interface.

```
{ ipv4-address address [ ipv4-address secondary_address ] | ipv6-address address [ ipv6-address secondary_address ] }
```

Specifies the IP address for the interface configured as an S1-MME interface in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation. Optionally configure a secondary IP address for either address type.

```
crypto-template name
```

Specifies an existing crypto template name used when implementing IP Security (IPSec) on the S1-MME interface. *name* is an alphanumeric string of 1 through 104 characters.

```
max-subscribers number
```

Specifies the maximum number of subscribers that can access this service on this interface as an integer from 0 through 8000000.
For Release 15.0, the ASR 5500 platform supports up to 10,000,000 MME UE sessions.
**Usage**

Use this command to associate the MME service with a specific logical IP address that will be used for binding the SCTP socket that communicates with the eNodeB using S1AP. Only one IP address can be configured with this command for one MME service. The MME passes the IP address during setting up the SCTP association with the eNodeB.

**Caution:** This is a critical configuration. The MME service can not be started without this configuration. Any change to this configuration will cause the MME service to be restarted. Removing or disabling this configuration will stop the MME service.

**Important:** Up to two IPv4 or IPv6 addresses can be configured to support SCTP multi-homing.

**Example**

The following command would bind the logical IP interface with the address of 192.168.3.1 to the MME service to interact with eNodeB:

```
bind s1-mme ipv4-address 192.168.3.1
```

The following command disables a binding that was previously configured:

```
no bind s1-mme ipv4address
```
csg-change-notification

This command enables or disables the Closed Subscriber Group (CSG) Information reporting (notification) mechanism on the MME. When enabled, the MME includes the CSG Information Reporting Action IE with the appropriate Action field for subscribers.

Product
MME

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > MME Service

configure > context context_name > mme-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-mme-service)#

Syntax

[ default | no ] csg-change-notification

---

default

Returns the command to its default value of disabled.

---

no

Disables the feature.

Usage

Use this command to enable or disable CSG change notification to the SGW/PGW. By default csg-change-notification is disabled; the MME does not send CSG notification to the SGW/PGW.
**dns**

Specifies the context where the Domain Name System (DNS) client service is configured for DNS query to select a P-GW, S-GW, peer SGSN or peer MME for this MME service.

**Product**
MME

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > MME Service

```
configure > context context_name > mme-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-mme-service)#
```

**Syntax**

```
dns { peer-mme | peer-sgsn | pgw | sgw } [ context ctx_name ]
```

```
no dns { peer-mme | peer-sgsn | pgw | sgw }
```

**no**

Removes a previously specified context having a DNS client service configured for DNS query to select a peer MME, peer SGSN, P-GW or S-GW with this MME service.

**peer-mme**

Specifies the context where a DNS client service is configured for DNS queries for selecting a peer MME.

**peer-sgsn**

Specifies the context where a DNS client service is configured for DNS queries for selecting a peer SGSN for inter-RAT handovers.

**pgw**

Specifies the context where a DNS client service is configured for DNS queries for selecting a P-GW.

**sgw**

Specifies the context where a DNS client service is configured for DNS queries for selecting an S-GW.

**context ctx_name**

Optionally associates the specific context name where the DNS client service is configured for this MME service. If this keyword is omitted, the DNS client service is configured to use the same context as this MME service.

`ctx_name` is name of the configured context of the DNS client service expressed as an alphanumeric string of 1 through 79 characters that is case sensitive.
Usage

Use this command to specify a pre-configured context where a DNS client service is configured. The DNS Client service configured in the specified context provides the DNS query support to locate peer MMEs, peer-SGSNs, P-GWs, or S-GWs for this MME service. For more information on DNS Client service and support, refer to the DNS Client Service Configuration Mode Commands chapter. A maximum of one context can be specified for each keyword.

Example

The following command associates a pre-configured context `dns_ctx1` where a DNS client service is configured for DNS query to P-GW for this MME service:

```
        dns pgw context dns_ctx1
```

The following command associates a pre-configured context `dns_ctx2` where a DNS client service is configured for DNS query to S-GW:

```
        dns sgw context dns_ctx2
```
# MME Service Configuration Mode Commands

## emm

Defines the Evolved Mobility Management timer parameters, such as timeout durations for timers and retransmission counts, for Non-Access Stratum (NAS) message retransmission in MME service.

**Product**
- MME

**Privilege**
- Administrator

**Mode**
- Exec > Global Configuration > Context Configuration > MME Service
- `configure > context context_name > mme-service service_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-mme-service)#
```

**Syntax**

```
emm { implicit-detach-timeout detach_dur | mobile-reachable-timeout mob_reach_dur | t3412-timeout t3412_dur | t3413-timeout t3413_dur | t3422-timeout t3422_dur | t3423-timeout t3423_dur | t3450-timeout t3450_dur | t3460-timeout t3460_dur | t3470-timeout t3470_dur }

default emm { implicit-detach-timeout | mobile-reachable-timeout | t3412-timeout | t3413-timeout | t3422-timeout | t3423-timeout | t3450-timeout | t3460-timeout | t3470-timeout }
```

### default

Resets the specified timer timeout to the system default value.

### implicit-detach-timeout detach_dur

Sets the timer timeout duration (in seconds) after which subscriber will implicitly detached from the network if there is no activity. Generally this timer value is 240 seconds (4 minutes) more than the timeout value of the T3423 timer.

This timer starts when mobile reachable timer expires while the network is in EMM-IDLE mode and ISR is activated and stops when a NAS signalling connection established.

`detach_dur` is an integer from 1 through 12000. Default: 3480

### mobile-reachable-timeout mob_reach_dur

Sets the timeout timer duration (in seconds) after which reachability procedure will be discarded and reattempt starts.

`mob_reach_dur` is an integer from 1 through 12000. Default: 3480

### t3412-timeout t3412_dur

Sets the timeout duration (in seconds) for the T3412 timer. This timer is used for periodic tracking area update (P-TAU). When this timer expires, the periodic tracking area updating procedure starts and the timer is set to its initial value for the next start.

This timer starts when the UE goes from EMM-CONNECTED to EMM-IDLE mode and stops when the UE enters EMM-CONNECTED mode.
t3412_dur is an integer from 1 through 11160. Default: 3240

**t3413-timeout t3413_dur**

Sets the timeout duration (in seconds) for the T3413 timer. The timer starts when MME initiates the EPS paging procedure to the EMM entity in the network and requests the lower layer to start paging. This timer stops for the paging procedure when a response received from the UE.

t3413_dur is an integer from 1 through 20. Default: 6

**t3422-timeout t3422_dur**

Sets the timeout duration (in seconds) for the T3422 timer. This timer starts when MME initiates the detach procedure by sending a DETACH REQUEST message to the UE and stops upon receipt of the DETACH ACCEPT message.

t3422_dur is an integer from 1 through 20. Default: 6

**t3423-timeout t3423_dur**

Sets the timeout duration (in seconds) for the T3423 timer. This timer starts when UE enters the EMM-DEREGISTERED state or when entering EMM-CONNECTED mode. It stops while the UE is in EMM-DEREGISTERED.NO-CELL-AVAILABLE state and Idle mode Signalling Reduction (ISR) is activated.

t3423_dur is an integer from 1 through 11160. Default: 3240

**t3450-timeout t3450_dur**

Sets the timeout duration (in seconds) for the T3450 timer. This timer starts when MME initiates the Globally Unique Temporary Identifier (GUTI) reallocation procedure by sending a GUTI REALLOCATION COMMAND message to the UE and stops upon receipt of the GUTI REALLOCATION COMPLETE message. This timer is also used for the Tracking Area update procedure.

t3450_dur is an integer from 1 through 20. Default: 6

**t3460-timeout t3460_dur**

Sets the timeout duration (in seconds) for the T3460 timer. This timer starts when the network initiates the authentication procedure by sending an AUTHENTICATION REQUEST message to the UE and stops upon receipt of the AUTHENTICATION RESPONSE message.

t3460_dur is an integer from 1 through 20. Default: 6

**t3470-timeout t3470_dur**

Sets the timeout duration (in seconds) for the T3470 timer. The MME starts this timer when the network initiates the identification procedure by sending an IDENTITY REQUEST message to the UE and stops upon receipt of the IDENTITY RESPONSE message.

t3470_dur is an integer from 1 through 20. Default: 6

**Usage**

Use this command to set EMM timers.
The following tables describe the triggers and states for timers:
<table>
<thead>
<tr>
<th>Timer</th>
<th>State</th>
<th>Cause of Start</th>
<th>Normal Stop</th>
<th>On Expiry</th>
</tr>
</thead>
<tbody>
<tr>
<td>T3402</td>
<td>• EMM-DEREGISTERED ED</td>
<td>• At attach failure and the attempt counter is equal to 5.</td>
<td>• ATTACH REQUEST sent</td>
<td>Initiation of the attach procedure or TAU procedure</td>
</tr>
<tr>
<td></td>
<td>• EMM-REGISTERED</td>
<td>• At tracking area updating failure and the attempt counter is equal to 5.</td>
<td>• TRACKING AREA UPDATE REQUEST sent</td>
<td></td>
</tr>
<tr>
<td>T3410</td>
<td>EMM-REGISTERED-INITIATED</td>
<td>ATTACH REQUEST sent</td>
<td>• ATTACH ACCEPT received</td>
<td>Start T3411 or T3402 as described in subclause 5.5.1.2.6</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• ATTACH REJECT received</td>
<td></td>
</tr>
<tr>
<td>T3411</td>
<td>• EMM-DEREGISTERED ED,</td>
<td>• At attach failure due to lower layer failure, T3410 timeout or attach rejected with other EMM cause values than those treated in subclause 5.5.1.2.5.</td>
<td>• ATTACH REQUEST sent</td>
<td>Retransmission of the ATTACH REQUEST or TRACKING AREA UPDATE REQUEST</td>
</tr>
<tr>
<td></td>
<td>ATTEMPTING TO ATTACH</td>
<td>• At tracking area updating failure due to lower layer failure, T3430 timeout or TAU rejected with other EMM cause values than those treated in subclause 5.5.3.2.5.</td>
<td>• TRACKING AREA UPDATE REQUEST sent</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• EMM-REGISTERED</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>. ATTEMPTING TO UPDATE</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T3412</td>
<td>EMM-REGISTERED</td>
<td>In EMM-REGISTERED, when EMM-CONNECTED mode is left.</td>
<td>• When entering state EMM-DEREGISTERED or</td>
<td>Initiation of the periodic TAU procedure</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• When entering EMM-CONNECTED mode.</td>
<td></td>
</tr>
<tr>
<td>Timer</td>
<td>State</td>
<td>Cause of Start</td>
<td>Normal Stop</td>
<td>On Expiry</td>
</tr>
<tr>
<td>---------</td>
<td>--------------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------</td>
<td>----------------------------------------</td>
</tr>
<tr>
<td>T3416</td>
<td>• EMM-REGISTERED-INITIATED</td>
<td>RAND and RES stored as a result of a UMTS authentication challenge</td>
<td>• SECURITY MODE COMMAND received</td>
<td>Delete the stored RAND and RES</td>
</tr>
<tr>
<td></td>
<td>• EMM-REGISTERED</td>
<td></td>
<td>• SERVICE REJECT received</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• EMM-DEREGISTERED-INITIATED</td>
<td></td>
<td>• TRACKING AREA UPDATE ACCEPT received</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• EMM-TRACKING-AREA-UPDATING-INITIATED</td>
<td></td>
<td>• AUTHENTICATION REJECT received</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• EMM-SERVICE-REQUEST-INITIATED</td>
<td></td>
<td>• AUTHENTICATION FAILURE sent</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• EMM-DEREGISTERED or EMM-NULL entered</td>
<td></td>
</tr>
<tr>
<td>T3417</td>
<td>EMM-SERVICE-REQUEST-INITIATED</td>
<td>• SERVICE REQUEST sent</td>
<td>• Bearers have been set up</td>
<td>Abort the procedure</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• EXTENDED SERVICE REQUEST sent in case f and g in subclause 5.6.1.1</td>
<td>• SERVICE REJECT received</td>
<td></td>
</tr>
<tr>
<td>T3417ext</td>
<td>EMM-SERVICE-REQUEST-INITIATED</td>
<td>• EXTENDED SERVICE REQUEST sent in case d in subclause 5.6.1.1</td>
<td>• Inter-system change from S1 mode to A/Gb mode or Iu mode is completed</td>
<td>Abort the procedure</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• EXTENDED SERVICE REQUEST sent in case e in subclause 5.6.1.1 and the CSFB</td>
<td>• Inter-system change from S1 mode to A/Gb mode or Iu mode is failed</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>response was set to “CS fallback accepted by the UE”.</td>
<td>• SERVICE REJECT received</td>
<td></td>
</tr>
<tr>
<td>Timer</td>
<td>State</td>
<td>Cause of Start</td>
<td>Normal Stop</td>
<td>On Expiry</td>
</tr>
<tr>
<td>-------</td>
<td>-------</td>
<td>----------------</td>
<td>-------------</td>
<td>-----------</td>
</tr>
</tbody>
</table>
| T3418 | • EMM-REGISTERED-INITIATED  
• EMM-REGISTERED  
• EMM-TRACKING-AREA-UPDATING-INITIATED  
• EMM-DEREGISTERED-INITIATED  
• EMM-SERVICE-REQUEST-INITIATED | AUTHENTICATION FAILURE (EMM cause = #20 “MAC failure” or #26 “Non-EPS authentication unacceptable”) sent | AUTHENTICATION REQUEST received | On first expiry, the UE should consider the network as false |
| T3420 | • EMM-REGISTERED-INITIATED  
• EMM-REGISTERED  
• EMM-DEREGISTERED-INITIATED  
• EMM-TRACKING-AREA-UPDATING-INITIATED  
• EMM-SERVICE-REQUEST-INITIATED | AUTHENTICATION FAILURE (cause = #21 “synch failure”) sent | AUTHENTICATION REQUEST received | On first expiry, the UE should consider the network as false |
<p>| T3421 | EMM-DEREGISTERED-INITIATED | DETACH REQUEST sent | DETACH ACCEPT received | Retransmission of DETACH REQUEST |</p>
<table>
<thead>
<tr>
<th>Timer</th>
<th>State</th>
<th>Cause of Start</th>
<th>Normal Stop</th>
<th>On Expiry</th>
</tr>
</thead>
</table>
| T3423 | EMM-REGISTERED | T3412 expires while the UE is in EMM-REGISTERED.NO-CELL-AVAILABLE and ISR is activated. | • When entering state EMM-DEREGISTERED or  
• When entering EMM-CONNECTED mode. | Set TIN to “P-TMSI” |
| T3430 | EMM-TRACKING-AREA-UPDATING-INITIATED | TRACKING AREA UPDATE REQUEST sent | • TRACKING AREA UPDATE ACCEPT received  
• TRACKING AREA UPDATE REJECT received | Start T3411 or T3402 as described in subclause 5.5.3.2.6 |
| T3440 | • EMM-REGISTERED-INITIATED  
• EMM-TRACKING-AREA-UPDATING-INITIATED  
• EMM-DEREGISTERED-INITIATED  
• EMM-SERVICE-REQUEST-INITIATED  
• EMM-REGISTERED | • ATTACH REJECT, DETACH REQUEST, TRACKING AREA UPDATE REJECT with any of the EMM cause values #11, #12, #13, #14 or #15  
• SERVICE REJECT received with any of the EMM cause values #11, #12, #13 or #15  
• TRACKING AREA UPDATE ACCEPT received after the UE sent TRACKING AREA UPDATE REQUEST in EMM-IDLE mode with no “active” flag | • Signalling connection released  
• Bearers have been set up | Release the signalling connection and proceed as described in subclause 5.3.1.2 |
| T3442 | EMM-REGISTERED | SERVICE REJECT received with EMM cause #39 | TRACKING AREA UPDATE REQUEST sent | None |

**NOTE 1:** The default value of this timer is used if the network does not indicate another value in an EMM signalling procedure.

**NOTE 2:** The value of this timer is provided by the network operator during the attach and tracking area updating procedures.

**NOTE 3:** The value of this timer may be provided by the network in the ATTACH ACCEPT message and TRACKING AREA UPDATE ACCEPT message. The default value of this timer is identical to the value of T3412.
NOTE 4: The value of this timer is provided by the network operator when a service request for CS fallback is rejected by the network with EMM cause #39 “CS domain temporarily not available”.

<table>
<thead>
<tr>
<th>Timer</th>
<th>State</th>
<th>Cause of Start</th>
<th>Normal Stop</th>
<th>On Expiry</th>
</tr>
</thead>
<tbody>
<tr>
<td>T3413</td>
<td>EMM-REGISTERED</td>
<td>Paging procedure initiated</td>
<td>Paging procedure completed</td>
<td>Network dependent</td>
</tr>
<tr>
<td>T3422</td>
<td>EMM-DEREGISTERED -INITIATED</td>
<td>DETACH REQUEST sent</td>
<td>DETACH ACCEPT received</td>
<td>Retransmission of DETACH REQUEST</td>
</tr>
<tr>
<td>T3450</td>
<td>EMM-COMMON-PROC-INIT</td>
<td>• ATTACH ACCEPT sent</td>
<td>• ATTACH COMPLETE received</td>
<td>Retransmission of the same message type, i.e. ATTACH ACCEPT, TRACKING AREA UPDATE COMPLETE or GUTI REALLOCATION COMMAND</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• TRACKING AREA UPDATE ACCEPT sent with GUTI</td>
<td>• TRACKING AREA UPDATE COMPLETE received</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• GUTI REALLOCATION COMMAND sent</td>
<td>• GUTI REALLOCATION COMPLETE received</td>
<td></td>
</tr>
<tr>
<td>T3460</td>
<td>EMM-COMMON-PROC-INIT</td>
<td>• AUTHENTICATION REQUEST sent</td>
<td>• AUTHENTICATION RESPONSE received</td>
<td>Retransmission of the same message type, i.e. AUTHENTICATI ON REQUEST or SECURITY MODE COMMAND</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• SECURITY MODE COMMAND sent</td>
<td>• AUTHENTICATION FAILURE received</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• SECURITY MODE COMPLETE received</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• SECURITY MODE REJECT received</td>
<td></td>
</tr>
<tr>
<td>T3470</td>
<td>EMM-COMMON-PROC-INIT</td>
<td>IDENTITY REQUEST sent</td>
<td>IDENTITY RESPONSE received</td>
<td>Retransmission of IDENTITY REQUEST</td>
</tr>
<tr>
<td>Mobile reachable timer</td>
<td>All except EMM-DEREGISTERED</td>
<td>Entering EMM-IDLE mode</td>
<td>NAS signalling connection established</td>
<td>Network dependent, but typically paging is halted on 1st expiry</td>
</tr>
<tr>
<td>Implicit detach timer</td>
<td>All except EMM-DEREGISTERED</td>
<td>The mobile reachable timer expires while the network is in EMM-IDLE mode and ISR is activated</td>
<td>NAS signalling connection established</td>
<td>Implicitly detach the UE on 1st expiry</td>
</tr>
</tbody>
</table>
| Table 34. EPS Mobility Management Timers – Network Side

<table>
<thead>
<tr>
<th>Timer</th>
<th>Cause of Start</th>
<th>Normal Stop</th>
<th>On Expiry</th>
</tr>
</thead>
<tbody>
<tr>
<td>T3413</td>
<td>Paging procedure initiated</td>
<td>Paging procedure completed</td>
<td>Network dependent</td>
</tr>
<tr>
<td>T3422</td>
<td>DETACH REQUEST sent</td>
<td>DETACH ACCEPT received</td>
<td>Retransmission of DETACH REQUEST</td>
</tr>
<tr>
<td>T3450</td>
<td>• ATTACH ACCEPT sent</td>
<td>• ATTACH COMPLETE received</td>
<td>Retransmission of the same message type, i.e. ATTACH ACCEPT, TRACKING AREA UPDATE COMPLETE or GUTI REALLOCATION COMMAND</td>
</tr>
<tr>
<td></td>
<td>• TRACKING AREA UPDATE ACCEPT sent with GUTI</td>
<td>• TRACKING AREA UPDATE COMPLETE received</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• GUTI REALLOCATION COMMAND sent</td>
<td>• GUTI REALLOCATION COMPLETE received</td>
<td></td>
</tr>
<tr>
<td>T3460</td>
<td>• AUTHENTICATION REQUEST sent</td>
<td>• AUTHENTICATION RESPONSE received</td>
<td>Retransmission of the same message type, i.e. AUTHENTICATI ON REQUEST or SECURITY MODE COMMAND</td>
</tr>
<tr>
<td></td>
<td>• SECURITY MODE COMMAND sent</td>
<td>• AUTHENTICATION FAILURE received</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• SECURITY MODE COMPLETE received</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• SECURITY MODE REJECT received</td>
<td></td>
</tr>
<tr>
<td>T3470</td>
<td>IDENTITY REQUEST sent</td>
<td>IDENTITY RESPONSE received</td>
<td>Retransmission of IDENTITY REQUEST</td>
</tr>
<tr>
<td>Mobile reachable timer</td>
<td>Entering EMM-IDLE mode</td>
<td>NAS signalling connection established</td>
<td>Network dependent, but typically paging is halted on 1st expiry</td>
</tr>
<tr>
<td>Implicit detach timer</td>
<td>The mobile reachable timer expires while the network is in EMM-IDLE mode and ISR is activated</td>
<td>NAS signalling connection established</td>
<td>Implicitly detach the UE on 1st expiry</td>
</tr>
</tbody>
</table>
### Table 35. EPS Session Management Timers – UE Side

<table>
<thead>
<tr>
<th>Timer</th>
<th>State</th>
<th>Cause of Start</th>
<th>Normal Stop</th>
<th>On Expiry1st, 2nd, 3rd, 4th EXPIRY (NOTE 1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>T3480</td>
<td>PROCEDURE</td>
<td>BEARER RESOURCE ALLOCATION REQUEST sent</td>
<td>ACTIVATE DEDICATED EPS BEARER CONTEXT REQUEST received or MODIFY EPS BEARER CONTEXT REQUEST received or BEARER RESOURCE ALLOCATION REJECT received</td>
<td>Retransmission of BEARER RESOURCE ALLOCATION REQUEST</td>
</tr>
<tr>
<td></td>
<td>TRANSACTION</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>PENDING</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T3481</td>
<td>PROCEDURE</td>
<td>BEARER RESOURCE MODIFICATION REQUEST sent</td>
<td>ACTIVATE DEDICATED EPS BEARER CONTEXT REQUEST received or MODIFY EPS BEARER CONTEXT REQUEST received or BEARER RESOURCE MODIFICATION REJECT received</td>
<td>Retransmission of BEARER RESOURCE MODIFICATION REQUEST</td>
</tr>
<tr>
<td></td>
<td>TRANSACTION</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>PENDING</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T3482</td>
<td>PROCEDURE</td>
<td>An additional PDN connection is requested by the UE which is not combined in attach procedure</td>
<td>ACTIVE DEFAULT EPS BEARER CONTEXT REQUEST received or PDN CONNECTIVITY REJECT received</td>
<td>Retransmission of PDN CONNECTIVITY REQUEST</td>
</tr>
<tr>
<td></td>
<td>TRANSACTION</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>PENDING</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T3492</td>
<td>PROCEDURE</td>
<td>PDN DISCONNECT REQUEST sent</td>
<td>DEACTIVATE EPS BEARER CONTEXT REQUEST received or PDN DISCONNECT REJECT received</td>
<td>Retransmission of PDN DISCONNECT REQUEST</td>
</tr>
<tr>
<td></td>
<td>TRANSACTION</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>PENDING</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

NOTE 1: Typically, the procedures are aborted on the fifth expiry of the relevant timer. Exceptions are described in the corresponding procedure description.

### Example

The following command sets the timeout value for EPS paging procedure timer T3413 for 10 seconds.

```
emm t3413-timeout 10
```
enb-cache-timeout

Configures the amount of time that eNodeB information is stored in cache after the eNodeB terminates the connection.

Product
MME

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > MME Service

configure > context context_name > mme-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-mme-service)#

Syntax

enb-cache-timeout min

default enb-cache-timeout

(default

Returns the command to its default value of 10.

min

Specifies the amount of time (in minutes) that the MME stores eNodeB information after the eNodeB terminates the connection. min is an integer value from 1 through 1440. Default: 10

Usage

Use this command to set the amount of time the MME stores eNodeB information in cache after the eNodeB terminates the connection.

Example

The following command sets the amount of time the MME stores eNodeB information to 15 minutes:

    enb-cache-timeout 15
encryption-algorithm-lte

Configures the precedence for LTE encryption algorithms to use for security procedures through this MME service.

**Product**
MME

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > MME Service

```bash
configure > context context_name > mme-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-mme-service)#
```

**Syntax**

```bash
encryption-algorithm-lte priority1 { 128-eea0 | 128-eea1 | 128-eea2 } [ priority2 { 128-eea0 | 128-eea1 | 128-eea2 } ] [ priority3 { 128-eea0 | 128-eea1 | 128-eea2 } ]
```

**default encryption-algorithm-lte**

**default**
Sets the default LTE encryption algorithm for security procedures with configured priority value. Lowest value has highest preference. Default configuration of LTE encryption algorithm is:
- priority1 with 128-eea0 encryption algorithm
- priority2 with 128-eea1 encryption algorithm
- priority3 with 128-eea2 encryption algorithm

**priority1**
Specifies the preference of integrity algorithm for security procedures on this MME service as priority 1.

**priority2**
Specifies the preference of integrity algorithm for security procedures on this MME service as priority 2.

**priority3**
Specifies the preference of integrity algorithm for security procedures on this MME service as priority 3.

**128-eea0**
Sets the Null ciphering algorithm (128-EAA0) for LTE encryption as the encryption algorithm for security procedures. Default: Enabled

**128-eea1**
This keyword sets the SNOW 3G synchronous stream ciphering algorithm (128-EAA1) for LTE encryption as the encryption algorithm for security procedures. SNOW 3G is a stream cipher that forms the base of the 3GPP confidentiality algorithm UEA2 and the 3GPP integrity algorithm UIA2. Default: priority2
128-eea2
Sets the Advance Encryption Standard (AES) ciphering algorithm (128-EEA2) for LTE encryption as the encryption algorithm for security procedures. Default: priority3

Usage
Use this command to set the LTE encryption algorithms for security procedures to use with this MME service.

⚠️ Caution: When this command is executed, all the existing priority-to-algorithm mappings will be removed and the newly configured ones will be applicable for security procedures.

⚠️ Caution: Configuration of the same algorithm to multiple priorities is prohibited.

Example
The following command sets the 128-EEA1 as the LTE encryption algorithm with priority 2 for security procedures with an MME service:

```
encryption-algorithm-lte priority2 128-eea1
```
end

Exits the current configuration mode and returns to the Exec mode.

**Product**: All

**Privilege**: Security Administrator, Administrator

**Syntax**

```plaintext
end
```

**Usage**

Use this command to return to the Exec mode.
esm

Defines the Evolved Session Management timer parameters like timeout durations for timers and retransmission counts for the retransmission of Non-Access Stratum (NAS) messages in MME service.

Product: MME
Privilege: Administrator
Mode
Exec > Global Configuration > Context Configuration > MME Service
configure > context context_name > mme-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-mme-service)#

Syntax

esm { t3485-timeout t3485_dur | t3486-timeout t3486_dur | t3489-timeout t3489_dur | t3495-timeout t3495_dur }
default esm { t3485-timeout | t3486-timeout | t3489-timeout | t3495-timeout }

default

Sets the specified Evolved Session Management timer timeout to the system default value.

t3485-timeout t3485_dur

Sets the timeout duration (in seconds) for the T3485 timer. This timer is used by the default EPS bearer context activation procedure.
This timer starts when the MME sends an ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST message to UE and stops when it receives ACTIVATE DEFAULT EPS BEARER CONTEXT ACCEPT or ACTIVATE DEFAULT EPS BEARER CONTEXT REJECT message from UE.
t3485_dur is an integer from 1 through 60. Default: 8

t3486-timeout t3486_dur

Sets the timeout duration (in seconds) for the T3486 timer. This timer is used by the default EPS bearer context modification procedure.
This timer starts when the MME sends a MODIFY EPS BEARER CONTEXT REQUEST message to the UE and stops when it receives a MODIFY EPS BEARER CONTEXT ACCEPT received or a MODIFY EPS BEARER CONTEXT REJECT message from UE.
t3485_dur is an integer from 1 through 60. Default: 8

t3489-timeout t3489_dur

Sets the timeout duration (in seconds) for the T3489 timer. This timer is used for the default EPS bearer context deactivation procedure.
This timer starts when the MME sends an ESM INFORMATION REQUEST message to the UE and stops when it receives a ESM INFORMATION RESPONSE message from the UE.
**t3495_dur** is an integer from 1 through 60. Default: 4

**t3495-timeout t3495_dur**

Sets the timeout duration (in seconds) for the T3495 timer. This timer is used for default EPS bearer context deactivation procedure. This timer starts when the MME sends a DEACTIVATE EPS BEARER CONTEXT REQUEST message to UE and stops when receives DEACTIVATE EPS BEARER CONTEXT ACCEPT or DEACTIVATE EPS BEARER CONTEXT REJECT message from UE. **t3495_dur** is an integer from 1 through 60. Default: 8

**Usage**

Use this command to set Evolved Session Management timers. The following tables describe the triggers and states for timers:

### Table 36. EPS Session Management Timers – Network Side

<table>
<thead>
<tr>
<th>Timer</th>
<th>State</th>
<th>Cause of Start</th>
<th>Normal Stop</th>
<th>On Expiry 1st, 2nd, 3rd, 4th EXPIRY (NOTE 1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>T3485</td>
<td>BEARER CONTEXT ACTIVE PENDING</td>
<td>• ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST sent</td>
<td>• ACTIVATE DEFAULT EPS BEARER CONTEXT REQUEST sent</td>
<td>Retransmission of the same message</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ACTIVATE DEDICATED EPS BEARER CONTEXT REQUEST sent</td>
<td>• ACTIVATE DEFAULT EPS BEARER CONTEXT ACCEPT received or</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• ACTIVATE DEDICATED EPS BEARER CONTEXT REJECT received or</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• ACTIVATE DEDICATED EPS BEARER CONTEXT ACCEPT received or</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• ACTIVATE DEDICATED EPS BEARER CONTEXT REJECT received</td>
<td></td>
</tr>
<tr>
<td>Timer</td>
<td>State</td>
<td>Cause of Start</td>
<td>Normal Stop</td>
<td>On Expiry 1st, 2nd, 3rd, 4th EXPIRY (NOTE 1)</td>
</tr>
<tr>
<td>-------</td>
<td>---------------------------------</td>
<td>------------------------------------------------------</td>
<td>-----------------------------------------------------------------</td>
<td>----------------------------------------------</td>
</tr>
<tr>
<td>T3486</td>
<td>BEARER CONTEXT MODIFY PENDING</td>
<td>MODIFY EPS BEARER CONTEXT REQUEST sent</td>
<td>• MODIFY EPS BEARER CONTEXT ACCEPT received or&lt;br&gt;• MODIFY EPS BEARER CONTEXT REJECT received</td>
<td>Retransmission of MODIFY EPS BEARER CONTEXT REQUEST</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T3489</td>
<td>PROCEDURE TRANSACTION PENDING</td>
<td>ESM INFORMATION REQUEST sent</td>
<td>ESM INFORMATION RESPONSE received</td>
<td>Retransmission of ESM INFORMATION REQUEST on 1st and 2nd expiry only</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T3495</td>
<td>BEARER CONTEXT INACTIVE PENDING</td>
<td>DEACTIVATE EPS BEARER CONTEXT REQUEST sent</td>
<td>DEACTIVATE EPS BEARER CONTEXT ACCEPT received</td>
<td>Retransmission of DEACTIVATE EPS BEARER CONTEXT REQUEST</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**NOTE 1:** Typically, the procedures are aborted on the fifth expiry of the relevant timer. Exceptions are described in the corresponding procedure description.

This command can be repeated to set each timer as needed. The retransmission of all type of NAS messages can be configured through `nas-max-retransmissions` command.

**Example**

The following command sets the timeout value for the default EPS bearer context activation procedure timer (T3485) for 10 seconds.

```
esm t3485-timeout 10
```
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Use this command to return to the parent configuration mode.
gtpv2

Configures GTPv2 piggybacking support from the MME to the P-GW. A piggybacking flag is sent by the MME to a P-GW in the S11 “Create Session Request” message and determines whether dedicated bearer creation (Create Bearer Request) is piggybacked onto the “Create Session Response” message or not.

**Product**
MME

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > MME Service
configure > context context_name > mme-service service_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-mme-service)#
```

**Syntax**

```
[ default | no ] gtpv2 piggybacking
```

- **default**
  Returns the command to its default setting of enabled.

- **no**
  Disables the feature.

- **piggybacking**
  Specifies that piggybacking is to be performed by the P-GW.

**Usage**

Use this command to enable the sending of a piggybacking flag to the P-GW over the S11 interface requesting that the Create Bearer Request message is piggybacked on the Create Session Response message (sent from the P-GW to the MME).

**Example**

The following command disables this feature:

```
no gtpv2 piggybacking
```
heuristic-paging

Enables or disables the heuristic or optimized paging feature for the service.

**Product**
MME

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > MME Service

configure > context context_name > mme-service service_name

Entering the above command sequence results in the following prompt:

\[context_name]host_name(config-mme-service)\

**Syntax**

```
[ default | no ] heuristic-paging [ paging-map paging_map_name ]
```

- **default**
  Returns the command to its default setting of disabled.

- **no**
  Disables the feature.

- **paging-map paging_map_name**
  Specifies the paging-map to be associated with this MME service. This keyword is only supported in Release 14.0 and higher.

**Usage**

⚠️ **Caution:** The paging profiles need to be configured prior to configuring TAI management objects (tai-mgmt-db and tai-mgmt-obj). Otherwise, the configuration would lead to high paging load in the MME node, at peak traffic time, causing service outage.

Use this command to enable or disable the heuristic paging feature for the service. Also known as idle-mode paging, enabling this feature prompts the MME service to keep track of the eNodeBs to which the access terminal (AT) most commonly attaches, thus reducing the signalling otherwise associated with continuous paging.

If no paging-map is associated when this command is issued, the default heuristic paging behavior is used (as opposed to intelligent paging behavior).

Refer to the *Heuristic and Intelligent Paging* chapter in the *MME Administration Guide* for more information about this command.
Important: Heuristic (optimized) Paging is a licensed feature and will not appear as a command option unless the proper licensed is installed.
integrity-algorithm-lte

Configures the precedence of LTE integrity algorithms to use for security procedures through this MME service. By default the integrity algorithm is enabled on MME service and cannot be disabled.

**Product**  
MME

**Privilege**  
Administrator

**Mode**  
Exec > Global Configuration > Context Configuration > MME Service  
`configure > context context_name > mme-service service_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-mme-service)##
```

**Syntax**

```
integrity-algorithm-lte priority1 { 128-eia1 | 128-eia2 } [ priority2 { 128-eia1 | 128-eia2 } ]
```

```
default integrity-algorithm-lte
```

**default**

Removes the preconfigured integrity algorithm and sets the default LTE integrity algorithm for security procedures. Default configuration of LTE integrity algorithm is:

- priority1 with 128-eia1 integrity algorithm
- priority2 with 128-eia2 integrity algorithm

```
priority1
```

Specifies the preference of integrity algorithm for security procedures on this MME service as priority 1. This is the mandatory and default priority keyword.

```
priority2
```

Specifies the preference of integrity algorithm for security procedures on this MME service as priority 2.

```
128-eia1
```

This keyword sets the SNOW 3G synchronous stream ciphering algorithm (128-EIA1) for LTE integrity as the integrity algorithm for security procedures. SNOW 3G is a stream cipher that forms the base of the 3GPP confidentiality algorithm UEA2 and the 3GPP integrity algorithm UIA2. Default: priority1

```
128-eia2
```

Sets the Advance Encryption Standard (AES) ciphering algorithm (128-EIA2) for LTE integrity as the integrity algorithm for security procedures. Default: Enabled
Usage

Use this command to set the LTE integrity algorithms for security procedures to use with this MME service.

⚠️ **Caution:** Integrity algorithm is a mandatory aspect and can not be disabled in MME service.

⚠️ **Caution:** When this command is executed, all the existing priority to algorithm mappings will be removed and the newly configured ones will be applicable for security procedures.

⚠️ **Caution:** Configuration of same algorithm to multiple priorities is prohibited.

Example

The following command sets the AES ciphering algorithms (128-EIA2) as the LTE integrity algorithm with priority as 1 for security procedures with an MME service:

```
integrity-algorithm-lte priority1 128-eia2
```
inter-rat-nnsf

Configures an NNSF (NAS Node Selection Functionality) entry to define a list of Served MMECs (MME codes) that is indicated to the eNodeB in the S1 Setup Response. This optional configuration is used to aid the eNodeB when selecting the MME for inter-rat handovers when the MME is co-located with an SGSN.

**Product**
MME

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > MME Service
configure > context context_name > mme-service service_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-mme-service)#
```

**Syntax**

```
[no] inter-rat-nnsf collocated-mme plmn-id mcc mcc_value mnc mnc_value group-id mme_group_id mme-codes mmec
```

- **no**
  - Removes the specified NNSF entry.

- **collocated-mme**
  - Specifies that the MME is co-located with an SGSN.

- **plmn-id mcc mcc_value mnc mnc_value**
  - Specifies the PLMN-ID for this MME service.
    - `mcc`: Specifies the mobile country code (MCC) portion of the PLMN identifier as an integer from 100 through 999.
    - `mnc`: Specifies the mobile network code (MNC) portion of the PLMN identifier as a 2- or 3-digit integer from 00 through 999.

- **group-id mme_group_id**
  - Configures the group id for this MME service.
    - `mme_group_id`: must be an integer value from 0 through 65536.

- **mme-codes mmec**
  - Configures a list of MMEC (MME codes) to be used.
    - `mmec`: must be entered as a series of codes, each separated by a space, such as: 10 25 102 103 105. Each code must be an integer from 0 through 255.
    - A maximum of 16 MME Codes are allowed to be configured per inter-rat-nnsf entry.
Usage

Use this command to indicate a list of served MMECs, in addition to the one assigned to the MME service. The complete list shall be notified to the eNodeB as Served MMECs in the S1 Setup Response. This would aid the eNodeB in selecting a co-located MME during 2G/3G to 4G handovers.

When a UE moves from 2G/3G to 4G, selecting a co-located MME is not possible without some explicit configuration. In this scenario, the entire second Most-Significant-Byte of P-TMSI is copied into the MME-Code (MMEC) field. Depending on the NRI length, this could result in 'n' different MMEC values for the same NRI value.

For example:
- NRI length = 6 bits
- NRI value = 5 (Binary 00 0101)
- Possible MMECs: Binary 00 0101 xx -> {20, 21, 22, 23}

Selecting a co-located MME is only possible if the eNodeB knows that any UE meant for the above set of MMECs should be directed to a given MME. This command enables the operator to specify MMECs that can possibly be mapped from a given NRI value.

A maximum of 16 MME Codes are allowed to be configured per inter-rat-nnsf entry. This allows 4 SGSNs with NRI length of 6, or 2 SGSNs with NRI length of 5. If more than 16 MMECs are required, an alternative is to pick a dummy MME-Group-ID value and create a new nnsf-entry. The Serving MME-Group-ID could also be used for this purpose as MME-Group-Id has no significance during MME node selection.

A Maximum of 32 inter-rat-nnsf entries are allowed. Regardless of the maximum entries configured, the maximum limits placed by S1AP stack take precedence. For example, if the number of plmns configured under 'network-sharing' and 'inter-rat-nnsf' exceeds the maxnoofPLMNPerMME(32) limit set by S1AP-S1-Setup-Response, then inter-rat-nnsf entries that exceed the limit(32) do not get included in the S1 Setup Response message.

Example

For NRI length = 6; NRI Value = 10 (Binary: 00 1010), when a UE moves from 2G/3G to 4G and maps MME Code (8 bits) from P-TMSI, the MME Code value could be:

- Binary: 00 1010 xx, where xx can be binary 10 or 01 or 00 or 11
- Decimal: 40 or 41 or 42 or 43

So, all of the above values should be configured as MMECs as part of `inter-rat-nnsf`, as follows:

```
inter-rat-nnsf collocated-mme plmn-id mcc 121 mnc 102 mme-id group-id 32000 mme-codes 40 41 42 43
```

When updating an existing NNSF entry, any new MMECs must be included with the existing MMECs. For example, to add additional MMECs (48 49 50 51) to the above command, enter the entire command again as follows:

```
inter-rat-nnsf collocated-mme plmn-id mcc 121 mnc 102 mme-id group-id 32000 mme-codes 40 41 42 43 48 49 50 51
```
isr-capability

Enables or disables the Idle-mode Signaling Reduction (ISR) feature on the MME service.

**Product**
MME

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > MME Service

configure > context context_name > mme-service service_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-mme-service)#
```

**Syntax**

```
[ no | default ] isr-capability
```

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Sets the ISR feature to the default setting (disabled) on MME service.</td>
</tr>
<tr>
<td>no</td>
<td>Disables the ISR feature on MME service.</td>
</tr>
</tbody>
</table>

**Usage**

Use this command to enable or disable the ISR feature on the MME service. When enabled, the MME can perform ISR functions with a peer SGSN which also supports ISR.

Refer to the Idle-mode Signaling Reduction chapter in the MME Administration Guide for more information about this command.

**Important:** This functionality is a license-controlled feature. A valid feature license must be installed to enable Idle-mode Signaling Reduction.
local-cause-code-mapping apn-mismatch

Configures the reject cause code to send to a UE when an APN mismatch occurs.

Product
MME

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > MME Service
configure > context context_name > mme-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-mme-service)#

Syntax


default local-cause-code-mapping apn-mismatch

Returns the cause code mapping to its default value: esm-failure esm-cause-code unknown-apn.


Specifies the EPS Mobility Management (EMM) cause code to return when an APN mismatch occurs.

•eps-service-not-allowed-in-this-plmn
•esm-failure esm-cause-code unknown-apn - Default.
  For the esm-failure cause code only, the unknown-apn ESM code is also reported to the UE.
•no-suitable-cell-in-tracking-area
•plmn-not-allowed
•roaming-not-allowed-in-this-tracking-area
•tracking-area-not-allowed

Usage

Use this command to configure the cause code returned to a UE when an APN mismatch occurs, such as when an APN is present in the HSS subscription but the HSS subscription for this IMSI has other APNs present in the subscription. By default, the MME sends the UE the #23 - ESM Failure cause code for this condition.
Related Commands:
If a condition is specified in both the call-control-profile associated with a call, and also the mme-service, the cause configured for the call-control-profile will be signalled to the UE. See also the `local-cause-code-mapping` command in the call-control-profile configuration mode. This command is described in the *Call Control Profile Configuration Mode Commands* chapter.

Example
The following command maps the “PLMN not allowed” cause code to the APN mismatch condition:

```
local-cause-code-mapping apn-mismatch emm-cause-code plmn-not-allowed
```
**local-cause-code-mapping apn-not-subscribed**

Gives the operator the option to specify the local cause-code mapping when the UE-requested APN is not subscribed.

**Product**  
MME

**Privilege**  
Security Administrator, Administrator

**Mode**  
Exec > Global Configuration > Context Configuration > MME Service  
`configure > context context_name > mme-service service_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-mme-service)#
```

**Syntax**  

```
local-cause-code-mapping apn-not-subscribed esm-cause-code requested-service-option-not-subscribed
```

```
default local-cause-code-mapping apn-not-subscribed
```

**Usage**

The operator can specify "Requested-Option-Not-Subscribed" cause code value #33 will be sent in the Reject message when the PDN Connectivity Request is rejected because no subscription is found. If the command option is not configured, then by default the MME uses the cause code value #27 (Unknown or Missing APN) in standalone PDN Connectivity Reject message when the UE-requested APN is not subscribed.

**Example**

The following instructs the MME to use cause code #33 ("Requested-Option-Not-Subscribed") in place of the default #27 (Unknown or Missing APN):.

```
local-cause-code-mapping apn-not-subscribed esm-cause-code requested-service-option-not-subscribed
```
local-cause-code-mapping auth-failure

Configures the reject cause code to send to a UE when an authentication failure occurs.

**Product**
MME

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > MME Service configure > context context_name > mme-service service_name

Entering the above command sequence results in the following prompt:

```
[context_name] host_name(config-mme-service) #
```

**Syntax**

```

default local-cause-code-mapping auth-failure
```

**Usage**

Use this command to configure the cause code returned to a UE when an authentication failure occurs. By default, the MME sends the UE the #3 - Illegal MS cause code when encountering a context transfer failure from an MME.

This condition occurs for TAU and ATTACH procedures in the following cases:
• The Authentication response from the UE does not match the expected value in the MME.
• Security Mode Reject is sent by the UE.
• The UE responds to any identity request with a different type of identity (ie, the MME could query for IMSI and the UE responds with IMEI).

The following are not considered for the authentication failure condition:
• HSS returning a result code other than SUCCESS.
• HSS not available.
• EIR failures.
• UE not responding to requests.

Related Commands:
If a cause code mapping is specified in both the call-control-profile associated with a call, and also the mme-service, the cause configured for the call-control-profile will be signalled to the UE. See also the `local-cause-code-mapping` command in the call-control-profile configuration mode. This command is described in the Call Control Profile Configuration Mode Commands chapter.

Example
The following command maps the "network-failure" cause code to the authentication failure condition:

```
local-cause-code-mapping auth-failure emm-cause-code network-failure
```
local-cause-code-mapping congestion

Configures the reject cause code to send to a UE when a procedure fails due to a congestion condition.

**Product**
MME

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > MME Service

```plaintext
configure > context context_name > mme-service service_name
```

Entering the above command sequence results in the following prompt:

```plaintext
[context_name]host_name(config-mme-service)#
```

**Syntax**

```plaintext

default local-cause-code-mapping congestion
```

Returns the cause code mapping to its default value: `emm-cause congestion esm-cause congestion`.

```plaintext
```

Specifies the EPS Mobility Management (EMM) cause code to return when a UE requests access when the system is exceeding any of its congestion control thresholds.

- **congestion** - Default
- **eps-service-not-allowed-in-this-plmn**
- **network-failure**
- **no-suitable-cell-in-tracking-area**
- **plmn-not-allowed**
- **roaming-not-allowed-in-this-tracking-area**
- **tracking-area-not-allowed**
esm-cause-code { congestion | insufficient-resources | service-option-temporarily-out-of-order }

Specifies the EPS Session Management (ESM) cause code to return when a UE requests access when the system is exceeding any of its congestion control thresholds.

- congestion - Default
- insufficient-resources
- service-option-temporarily-out-of-order

Usage

Use this command to configure the cause code returned to a UE when a UE procedure fails due to a congestion condition on the MME. By default, the MME sends the UE the #22 - Congestion EMM cause code and ESM cause code when encountering congestion.

Related Commands:

If a condition is specified in both the call-control-profile associated with a call, and also the mme-service, the cause configured for the call-control-profile will be signalled to the UE. See also the local-cause-code-mapping command in the call-control-profile configuration mode. This command is described in the Call Control Profile Configuration Mode Commands chapter.

Example

The following command maps the “network failure” cause code to the congestion event:

```
local-cause-code-mapping congestion emm-cause-code network-failure
```
local-cause-code-mapping ctxt-xferr-fail-mme

Configures the reject cause code to send to a UE when a UE context transfer failure from a peer MME occurs.

Product: MME
Privilege: Administrator
Mode: Exec > Global Configuration > Context Configuration > MME Service

configure > context context_name > mme-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-mme-service)#

Syntax:


default local-cause-code-mapping ctxt-xferr-fail-mme

default local-cause-code-mapping ctxt-xferr-fail-mme

Returns the cause code mapping to its default value: unknown-ue-context.


Specifies the EPS Mobility Management (EMM) cause code to return when a UE context transfer failure from an old MME occurs.

• eps-service-not-allowed-in-this-plmn
• network-failure
• no-suitable-cell-in-tracking-area
• plmn-not-allowed
• roaming-not-allowed-in-this-tracking-area
• tracking-area-not-allowed
• unknown-ue-context - Default
Usage

Use this command to configure the cause code returned to a UE when a UE context transfer failure from a peer MME occurs. By default, the MME sends the UE the #9 - MS identity cannot be derived by the network cause code for this condition.

After the peer node has been identified, the MME sends a Context Request to the peer node. If the peer node is an MME, and if the context transfer procedure fails, this condition is detected.

Related Commands:

If a cause code mapping is specified in both the call-control-profile associated with a call, and also the mme-service, the cause configured for the call-control-profile will be signalled to the UE. See also the local-cause-code-mapping command in the call-control-profile configuration mode. This command is described in the Call Control Profile Configuration Mode Commands chapter.

Example

The following command maps the “network-failure” cause code to the context transfer failure from MME condition:

```
local-cause-code-mapping ctxt-xfer-fail-mme emm-cause-code network-failure
```
local-cause-code-mapping ctxt-xfer-fail-sgsn

Configures the reject cause code to send to a UE when a UE context transfer failure from a peer SGSN occurs.

Product
MME

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > MME Service
configure > context context_name > mme-service service_name

Entering the above command sequence results in the following prompt:
[context_name]host_name(config-mme-service)#

Syntax


default local-cause-code-mapping ctxt-xfer-fail-sgsn

default local-cause-code-mapping ctxt-xfer-fail-sgsn

Returns the cause code mapping to its default value: unknown-ue-context.


Specifies the EPS Mobility Management (EMM) cause code to return when a UE context transfer failure from an old SGSN occurs.

• eps-service-not-allowed-in-this-plmn
• network-failure
• no-suitable-cell-in-tracking-area
• plmn-not-allowed
• roaming-not-allowed-in-this-tracking-area
• tracking-area-not-allowed
• unknown-ue-context - Default
Usage

Use this command to configure the cause code returned to a UE when a UE context transfer failure from a peer SGSN occurs. By default, the MME sends the UE the #9 - **MS identity cannot be derived by the network** cause code when encountering this condition.

After the peer node has been identified, the MME sends a Context Request to the peer node. If the peer node is an SGSN, and if the context transfer procedure fails, this condition is detected.

Related Commands:

If a cause code mapping is specified in both the call-control-profile associated with a call, and also the mme-service, the cause configured for the call-control-profile will be signalled to the UE. See also the `local-cause-code-mapping` command in the call-control-profile configuration mode. This command is described in the *Call Control Profile Configuration Mode Commands* chapter.

Example

The following command maps the “network-failure” cause code to the context transfer failure from SGSN condition:

```
local-cause-code-mapping ctxt-xfer-fail-sgsn emm-cause-code network-failure
```
local-cause-code-mapping gw-unreachable

Configures the reject cause code to send to a UE when a gateway (S-GW or P-GW) does not respond during an EMM procedure.

Product
MME

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > MME Service
configure > context context_name > mme-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-mme-service)#

Syntax


default local-cause-code-mapping gw-unreachable [ attach | tau ]

default local-cause-code-mapping gw-unreachable [ attach | tau ]

Returns the cause code mapping to its default value: #19 - ESM Failure cause code for Attach procedures, and no-bearers-active - #40 - NO-EPS-BEARER-CONTEXT-ACTIVATED for TAU procedures.


Specifies the EPS Mobility Management (EMM) cause code to return when a gateway does not respond.

- eps-service-not-allowed-in-this-plmn
- network-failure
- no-bearers-active
- no-suitable-cell-in-tracking-area
- plmn-not-allowed
- roaming-not-allowed-in-this-tracking-area
- tracking-area-not-allowed
[ attach [ tau ] | tau [ attach ] ] | { no-bearers-active tau }

Optionally, the MME can return separate cause codes for Attach procedures and TAU procedures. This capability is available for any of the above EMM cause codes except no-bearers-active, which can only be defined for TAU procedures.

Usage

Use this command to configure the cause code returned to a UE when a gateway does not respond. By default, the MME sends the UE the #19 - ESM Failure cause code when encountering this condition.

Defaults:
Prior to StarOS 15.0 MR5, the MME sends the UE the #19 - ESM Failure cause code when encountering this condition.
In StarOS 15.0 MR5 and higher releases, the MME sends the UE the #19 - ESM Failure cause code for Attach procedures, and #40 - NO-EPS-BEARER-CONTEXT-ACTIVATED for TAU procedures.

Related Commands:
If a cause code mapping is specified in both the call-control-profile associated with a call, and also the mme-service, the cause configured for the call-control-profile will be signalled to the UE. See also the local-cause-code-mapping command in the call-control-profile configuration mode. This command is described in the Call Control Profile Configuration Mode Commands chapter.

Example

The following command maps the “network-failure” cause code to the gateway unreachable condition:

    local-cause-code-mapping gw-unreachable emm-cause-code network-failure
local-cause-code-mapping hss-unavailable

Configures the reject cause code to send to a UE when the HSS does not respond.

Product
MME

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > MME Service
configure > context context_name > mme-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-mme-service)#

Syntax


remove local-cause-code-mapping hss-unavailable

default local-cause-code-mapping hss-unavailable

Returns the cause code mapping to its default value:


Specifies the EPS Mobility Management (EMM) cause code to return when the HSS does not respond.

• eps-service-not-allowed-in-this-plmn
• network-failure - Default
• no-suitable-cell-in-tracking-area
• plmn-not-allowed
• roaming-not-allowed-in-this-tracking-area
• tracking-area-not-allowed

Usage
Use this command to configure the cause code returned to a UE when the HSS does not respond. By default, the MME sends the UE the #17 - Network failure cause code when encountering this condition. This condition is detected in the following cases:

• HSS resolution fails in the MME.
• HSS does not respond in time.
The cause code configured for this condition will be signaled in TAU and ATTACH REJECT messages.

**Related Commands:**

If a cause code mapping is specified in both the call-control-profile associated with a call, and also the mme-service, the cause configured for the call-control-profile will be signalled to the UE. See also the `local-cause-code-mapping` command in the call-control-profile configuration mode. This command is described in the *Call Control Profile Configuration Mode Commands* chapter.

**Example**

The following command maps the “tracking-area-not-allowed” cause code to the HSS unavailable condition:

```
local-cause-code-mapping hss-unavailable emm-cause-code tracking-area-not-allowed
```
local-cause-code-mapping newcall-policy-restrict

Configures the EPS Mobility Management (EMM) reject cause code to send to a UE when a UE requests access but the call control profile has set the call disposition to reject.

Product
MME

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > MME Service
configure > context context_name > mme-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-mme-service)#

Syntax


default local-cause-code-mapping newcall-policy-restrict

default local-cause-code-mapping newcall-policy-restrict

Returns the cause code mapping to its default value: congestion.

newcall-policy-restrict emm-cause-code emm_cause_code

Specifies the EPS Mobility Management (EMM) cause code to return when a UE requests access but the call control profile has set the call disposition to reject. 

emm_cause_code must be one of the following options:

•congestion - Default.
•eps-service-not-allowed-in-this-plmn
•network-failure
•no-suitable-cell-in-tracking-area
•plmn-not-allowed
•roaming-not-allowed-in-this-tracking-area
•tracking-area-not-allowed

Usage

Use this command to configure the cause code returned to a UE when a UE procedure fails, such as when the UE requests access to a restricted zone. By default, the MME sends the UE the #22 - Congestion cause code when encountering this condition.
Example

The following command sets the “network-failure” cause code for newcall-policy-restrict calls:

```
local-cause-code-mapping newcall-policy-restrict emm-cause-code network-failure
```
local-cause-code-mapping no-active-bearers

Configures the reject cause code to send to a UE when the context received from a peer SGSN (during a TAU procedure) does not contain any active PDP contexts.

**Product**
MME

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > MME Service

```
configure > context context_name > mme-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-mme-service)#
```

**Syntax**

```

default local-cause-code-mapping no-active-bearers
```

Returns the cause code mapping to its default value: no-bearers-active.

```
```

Specifies the EPS Mobility Management (EMM) cause code to return when no active PDP context exists.

* eps-service-not-allowed-in-this-plmn
* network-failure
* no-bearers-active - Default
* no-suitable-cell-in-tracking-area
* plmn-not-allowed
* roaming-not-allowed-in-this-tracking-area
* tracking-area-not-allowed
Usage

Use this command to configure the cause code returned to a UE when the context received from a peer SGSN (during a TAU procedure) does not contain any active PDP contexts. By default, the MME sends the UE the #40 - No PDP context activated cause code when encountering this condition.

Related Commands:

If a cause code mapping is specified in both the call-control-profile associated with a call, and also the mme-service, the cause configured for the call-control-profile will be signalled to the UE. See also the local-cause-code-mapping command in the call-control-profile configuration mode. This command is described in the Call Control Profile Configuration Mode Commands chapter.

Example

The following command maps the “plmn-not-allowed” cause code to the no active bearer condition:

```
local-cause-code-mapping no-active-bearers emm-cause-code plmn-not-allowed
```
local-cause-code-mapping peer-node-unknown

Configures the reject cause code to send to a UE when peer node resolution is not successful.

**Product**
MME

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > MME Service
configure > context context_name > mme-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-mme-service)#

**Syntax**


default local-cause-code-mapping peer-node-unknown

Returns the cause code mapping to its default value: unknown-ue-context


Specifies the EPS Mobility Management (EMM) cause code to return when the peer node is not known.

- eps-service-not-allowed-in-this-plmn
- network-failure
- no-suitable-cell-in-tracking-area
- plmn-not-allowed
- roaming-not-allowed-in-this-tracking-area
- tracking-area-not-allowed
- unknown-ue-context - Default

**Usage**

Use this command to configure the cause code returned to a UE when peer node resolution is not successful. By default, the MME sends the UE the #9 - MS identity cannot be derived by the network cause code when encountering this condition. During processing of a TAU Request, the resolution of a peer MME that had allocated the temporary identity that is signaled to the UE takes several steps in the MME. This resolution can be done based on DNS or based
on local configuration. This condition occurs when all mechanisms for peer node resolution are done with no success.

Related Commands:
If a cause code mapping is specified in both the call-control-profile associated with a call, and also the mme-service, the cause configured for the call-control-profile will be signalled to the UE. See also the local-cause-code-mapping command in the call-control-profile configuration mode. This command is described in the Call Control Profile Configuration Mode Commands chapter.

Example
The following command maps the “plmn-not-allowed” cause code to the peer node unknown condition:

```
local-cause-code-mapping peer-node-unknown emm-cause-code plmn-not-allowed
```
local-cause-code-mapping pgw-selection-failure

Configures the reject cause code to send to a UE when a failure occurs during P-GW selection.

Product
MME

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > MME Service configure > context context_name > mme-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-mme-service)#

Syntax


default local-cause-code-mapping pgw-selection-failure

default local-cause-code-mapping pgw-selection-failure

Returns the cause code mapping to its default value: network-failure.


Specifies the EPS Mobility Management (EMM) cause code to return when a failure occurs during P-GW selection.

• eps-service-not-allowed-in-this-plmn
• network-failure - Default
• no-suitable-cell-in-tracking-area
• plmn-not-allowed
• roaming-not-allowed-in-this-tracking-area
• tracking-area-not-allowed

Usage

Use this command to configure the cause code returned to a UE when a failure occurs during P-GW selection. By default, the MME sends the UE the #17 - Network failure cause code when encountering this condition.
Related Commands:

If a cause code mapping is specified in both the call-control-profile associated with a call, and also the mme-service, the cause configured for the call-control-profile will be signalled to the UE. See also the `local-cause-code-mapping` command in the call-control-profile configuration mode. This command is described in the *Call Control Profile Configuration Mode Commands* chapter.

Example

The following command maps the “plmn-not-allowed” cause code to the P-GW selection failure condition:

```
local-cause-code-mapping pgw-selection-failure emm-cause-code plmn-not-allowed
```
local-cause-code-mapping restricted-zone-code

Configures the reject cause code to send to a UE when a procedure fails.

Product
MME

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > MME Service

configure > context context_name > mme-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-mme-service)#

Syntax

local-cause-code-mapping restricted-zone-code emm-cause-code { eps-service-not-allowed-in-this-plmn | no-suitable-cell-in-tracking-area | plmn-not-allowed | roaming-not-allowed-in-this-tracking-area | tracking-area-not-allowed }

default local-cause-code-mapping restricted-zone-code

default local-cause-code-mapping restricted-zone-code

Returns the cause code mapping to its default value: no-suitable-cell-in-tracking-area.

restricted-zone-code emm-cause-code emm_cause_code

Specifies the EPS Mobility Management (EMM) cause code to return when a UE requests access to a restricted zone.

emm_cause_code must be one of the following options:

- eps-service-not-allowed-in-this-plmn
- no-suitable-cell-in-tracking-area - Default.
- plmn-not-allowed
- roaming-not-allowed-in-this-tracking-area
- tracking-area-not-allowed

Usage

Use this command to configure the cause code returned to a UE when a UE procedure fails, such as when the UE requests access to a restricted zone. By default, the MME sends the UE the #15 - No Suitable Cells in Tracking Area cause code when encountering this condition.
Related Commands:

If a condition is specified in both the call-control-profile associated with a call, and also the mme-service, the cause configured for the call-control-profile will be signalled to the UE. See also the `local-cause-code-mapping` command in the call-control-profile configuration mode. This command is described in the Call Control Profile Configuration Mode Commands chapter.

Example

The following command maps the “PLMN not allowed” cause code to the restricted zone code event:

```
local-cause-code-mapping restricted-zone-code emm-cause-code plmn-not-allowed
```
local-cause-code-mapping sgw-selection-failure

Configures the reject cause code to send to a UE when a failure occurs during S-GW selection.

**Product**
MME

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > MME Service
configure > context context_name > mme-service service_name

Entering the above command sequence results in the following prompt:
[context_name]host_name(config-mme-service)#

**Syntax**

```shell

default local-cause-code-mapping sgw-selection-failure
```

**Usage**

Use this command to configure the cause code returned to a UE when a failure occurs during S-GW selection. By default, the MME sends the UE the #17 - Network failure cause code when encountering this condition.
Related Commands:

If a cause code mapping is specified in both the call-control-profile associated with a call, and also the mme-service, the cause configured for the call-control-profile will be signalled to the UE. See also the `local-cause-code-mapping` command in the call-control-profile configuration mode. This command is described in the *Call Control Profile Configuration Mode Commands* chapter.

Example

The following command maps the “plmn-not-allowed” cause code to the S-GW selection failure condition:

```
local-cause-code-mapping sgw-selection-failure emm-cause-code plmn-not-allowed
```
**local-cause-code-mapping vlr-down**

Configures the cause code to send in a ATTACH ACCEPT or TAU ACCEPT to a UE that attachment to the VLR has failed because a VLR down condition is present.

**Product**
MME

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > MME Service

```
configure > context context_name > mme-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-mme-service)#
```

**Syntax**

```
local-cause-code-mapping vlr-down emm-cause-code { congestion | cs-domain-unavailable | imsi-unknown-in-hlr | msc-temp-unreachable | network-failure }
```

```
default local-cause-code-mapping vlr-down
```

Returns the cause code mapping to its default value: `msc-temp-unreachable`.

```
vlr-down emm-cause-code  emm_cause_code
```

Specifies the EPS Mobility Management (EMM) cause code to return when a VLR down condition is present.

`emm_cause_code` must be one of the following options:

- `congestion`
- `cs-domain-unavailable`
- `imsi-unknown-in-hlr`
- `msc-temp-unreachable` - Default.
- `network-failure`

**Usage**

Use this command to configure the cause code returned to a UE when a VLR down condition is present. By default, the MME sends the UE the #16: “**MSC temporarily not reachable**” cause code when encountering this condition.
Related Commands:

If a condition is specified in both the call-control-profile associated with a call, and also the mme-service, the cause configured for the call-control-profile will be signalled to the UE. See also the `local-cause-code-mapping` command in the call-control-profile configuration mode. This command is described in the Call Control Profile Configuration Mode Commands chapter.

Example

The following command maps the “network failure” EMM cause code to the VLR down condition:

```
local-cause-code-mapping vlr-down emm-cause-code network-failure
```
**local-cause-code-mapping vlr-unreachable**

Configures the cause code to send in a ATTACH ACCEPT or TAU ACCEPT to a UE that attachment to the VLR has failed because a VLR unreachable condition is present.

**Product**
MME

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > MME Service

```plaintext
configure > context context_name > mme-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-mme-service)#
```

**Syntax**

```plaintext
local-cause-code-mapping vlr-unreachable emm-cause-code { congestion | cs-domain-unavailable | imsi-unknown-in-hlr | msc-temp-unreachable | network-failure }

default local-cause-code-mapping vlr-unreachable
```

**Usage**

Use this command to configure the cause code returned to a UE when a VLR unreachable condition is present. By default, the MME sends the UE the #16: “MSC temporarily not reachable” cause code when encountering this condition.
Related Commands:

If a condition is specified in both the call-control-profile associated with a call, and also the mme-service, the cause configured for the call-control-profile will be signalled to the UE. See also the `local-cause-code-mapping` command in the call-control-profile configuration mode. This command is described in the Call Control Profile Configuration Mode Commands chapter.

Example

The following command maps the “network failure” EMM cause code to the VLR unreachable condition:

```
local-cause-code-mapping vlr-unreachable emm-cause-code network-failure
```
location-reporting

Enables or disables the UE location reporting function on the MME service.

**Product**
MME

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > MME Service

```
configure > context context_name > mme-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-mme-service)#
```

**Syntax**

```
[ no | default ] location-reporting
```

- **default**
  - Disables the location reporting feature on MME service.

- **no**
  - Disables the location reporting feature on MME service.

**Usage**

Use this command to enable or disable the UE location reporting feature on the MME service. When enabled the MME forwards a location report request for a specific UE from the P-GW to the eNodeB.

**Important:** Location reporting, also known as User Location Information (ULI) Reporting, is a licensed feature and requires the purchase of the ULI Reporting feature license.

**Example**

The following command sets the MME service to allow for location reporting for UEs:

```
location-reporting
```
mapping

Configures how the MME maps the Target RNC-ID fields to the Target eNodeB-ID and TAC fields for Inter-RAT Gn/Gp handovers.

Product
MME

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > MME Service

`configure > context context_name > mme-service service_name`

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-mme-service)#`

Syntax

`mapping rncid-to-enbid { maptype-default-includes-only-enb | maptype1-includes-enb-tai }`
`no mapping rncid-to-enbid`

| no |
| Sets the command to use the default value of `maptype-default-includes-only-enb`. |

| maptype-default-includes-only-enb |
| Default mapping logic |
| Maps the Target RNC-ID fields to Target eNodeB-ID fields as follows: |
| • PLMN of LAI => PLMN of MME |
| • LAC of LAI => MME Group ID |
| • RAC => Not used. |
| • RNC-ID (12 or 16bits) => Lowest 12 or 16 bits of eNB ID. |
| • TAC is picked from the list of TAIs supported by the target eNB. |

| maptype1-includes-enb-tai |
| Maps the Target RNC-ID fields to Target eNodeB-ID fields as follows: |
| • PLMN of LAI => PLMN of TAI and eNB |
| • LAC of LAI => TAC of TAI |
| • RAC => Lowest 8 bits of eNB ID |
| • RNC-ID (12bits) => Highest 12 bits of eNB ID |
Usage

Use this command to configure how the MME maps the Target RNC-ID fields to the Target eNodeB-ID and TAC fields for Inter-RAT Gn/Gp handovers.
max-bearers per-subscriber

Specifies the maximum number of EPS bearers that a subscriber may simultaneously use to access this MME service.

Product
MME
Privilege
Administrator
Mode
Exec > Global Configuration > Context Configuration > MME Service
configure > context context_name > mme-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-mme-service)#

Syntax

max-bearers per-subscriber max_bearer

default max-bearers per-subscriber

default

Configures the maximum EPS bearers for a subscriber to use simultaneously to the default value of 11.

max_bearer

Specifies the maximum number of EPS bearers for a subscriber may simultaneously use to access this MME service.

max_bearer is an integer from 1 through 11. Default: 11

Usage

Use this command to set the maximum number of EPS bearers that a subscriber may simultaneously use to access this MME service.

Example

The following command specifies that a maximum of 6 simultaneous EPS bearers can be facilitated for a subscriber at any given time:

max-bearers per-subscriber 6
max-paging-attempts

This command configures the maximum number of paging attempts allowed for network requested service creation to a subscriber.

Product
MME

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > MME Service
configure > context context_name > mme-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-mme-service)#

Syntax

max-paging-attempts max_paging_attempts

default max-paging-attempts

default

Configures the maximum number of paging attempts to the default value of 3.

max_paging_attempts

Specifies the maximum number of paging attempts allowed for network requested service creation to a subscriber.

max_paging_attempts is an integer from 1 through 10. Default: 3

Usage

Use this command to set the maximum number of paging attempts allowed for network requested service creation to a subscriber.

When Heuristic Paging is enabled, this setting applies only to messages sent to all eNodeBs in all TAIIs present in the TAI list. Paging to the last known eNodeB and paging the TAI from which the UE was last heard is attempted only once. As a result, when max-paging-attempts is set to 3, a maximum of 5 paging retries are attempted with Heuristic Paging enabled.

Refer to the Heuristic and Intelligent Paging chapter in the MME Administration Guide for more information about Heuristic Paging.

Example

The following command specifies that a maximum of 6 paging attempt retransmissions allowed for network requested service creation to a subscriber:

max-paging-attempts 6
**max-pdns per-subscriber**

Specifies the maximum number of Packet Data Networks (PDNs) that a subscriber may simultaneously access through this MME service.

**Product**
MME

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > MME Service
configure > context context_name > mme-service service_name

Entering the above command sequence results in the following prompt:

> [context_name]host_name(config-mme-service)#

**Syntax**

```plaintext
max-pdns per-subscriber max_pdn

default max-pdns per-subscriber
default

max_pdn
```

**Usage**

Use this command to set the maximum number of PDNs that a subscriber may simultaneously access through this MME service.

**Example**

The following command specifies that a maximum of 2 simultaneous PDNs can be accessed by a subscriber at any given time through this MME service:

```plaintext
max-pdns per-subscriber 2
```
mme-id

Configures the MME identifier within an MME service. The MME identifier is constructed from the MME group ID and MME Code.

**Product**
MME

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > MME Service
configure > context context_name > mme-service service_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-mme-service)#
```

**Syntax**

```
mme-id group-id grp_id mme-code mme_code
```

```
no mme-id
```

- **group-id grp_id**
  Specifies the group identifier for the group of which this MME belongs as an integer from 0 through 65535.

- **mme-code mme_code**
  Specifies the unique code for this MME service as an integer from 0 through 255.

**Usage**

Use this command to set the MME identifier for this MME service. This MME identifier will be the identity of this MME in network.

**Caution:** Changing or removing the MME identifier is a disruptive operation; the MME service will be re-started or removed from service.

**Example**

The following command configures the MME identifier with group id as 41025 and MME code as 101 for this MME service:

```
mme-id group-id 41025 mme-code 101
```
mmemgr-recovery

Configures the recovery action for the MME manager.

**Product**
MME

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > MME Service
 configure > context context_name > mme-service service_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-mme-service)#
```

**Syntax**

```
mmemgr-recovery { no-reset | reset-s1-peers }
```

**Default**

```
default mmemgr-recovery
```

- **default**
  Resets the command to its default value.

- **no-reset**
  Specifies that the recovery action is to NOT reset S1 peers.

- **reset-s1-peers**
  Specifies that the recovery action is TO reset S1 peers.

**Usage**

Use this command to set a recovery action for the MME Manager.

**Example**

The following command configures the MME Manager recovery action to reset all S1 peers:

```
mmemgr-recovery reset-s1-peers
```
**msc**

Configures a Mobile Switching Center server enhanced with SRVCC (MSC) for the MME service. The MSC server acts as an endpoint for the Sv interface and is used for the Single Radio Voice Call Continuity (SRVCC) feature.

**Product**

MME

**Privilege**

Administrator

**Mode**

Exec > Global Configuration > Context Configuration > MME Service  
`configure > context context_name > mme-service service_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-mme-service)#
```

**Syntax**

```
msc msc_name ip-address ip_address [ offline | online ]

no msc msc_name
```

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>msc_name</td>
<td>Specifies a name for this peer MSC server. <code>msc_name</code> must be an alphanumeric string from 1 to 63 characters.</td>
</tr>
<tr>
<td>ip-address</td>
<td>Specifies the IP address of the peer MSC server in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.</td>
</tr>
<tr>
<td>offline</td>
<td>Mark this MSC server offline for maintenance. Once this command is issued, the MME will no longer send future handover requests to this MSC server. No GTPv2 messages are generated when offline/online mode is changed.</td>
</tr>
<tr>
<td>online</td>
<td>Mark this MSC server for online mode. Once this command is issued, the MSC server is added back into the MSC selection algorithm and normal operation is returned. By default, an MSC server is online unless the offline keyword is specified.</td>
</tr>
</tbody>
</table>

**Usage**

Use this command to configure a peer MSC server used during SRVCC handovers. This command also can also be used to mark an MSC server offline for maintenance.
Example

For Release 15.0 and higher:
The following command defines an MSC server `mscwest` with an IPv4 address of `10.2.3.4`:

```
msc mscwest ip-address 10.2.3.4
```

The following command marks the above MSC server offline:

```
msc mscwest ip-address 10.2.3.20 offline
```

The following command defines a default MSC server with an IPv4 address of `10.2.3.20`. The MME will select the default when MSC pool areas are not configured, or when an MSC address fails to be returned.

```
msc default ip-address 10.2.3.20
```

For Release 14.0 and earlier:
The following command specifies an IPv4 address for the peer MSC server as `10.2.3.4`:

```
msc 10.2.3.4
```
nas-max-retransmission

Sets the retransmission counter for all type of Non-Access Stratum (NAS) messages in an MME service.

Product
MME

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > MME Service
configure > context context_name > mme-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-mme-service)#

Syntax

nas-max-retransmissions nas_retrans_count

default nas-max-retransmissions

default

 Resets the retransmission counter to the default value of 4.

pack_retrans_count

Sets the maximum number of retransmission of NAS messages permitted during any procedure after which the activation procedure will be discarded.

pack_retrans_count is an integer from 1 through 10. Default: 4

Usage

Use this command to set maximum number of retries allowed for any type of NAS messages.

NAS Messages sent by the MME which require a response from the UE for procedure completion are retransmitted. Retransmission happens based on timer expiry. The timers are configured through the emm and esm commands. NAS messages are retransmitted per configuration, and if no response is received from the UE, the pending transaction is abandoned. If the transaction is a DETACH or PDN DISCONNECT REQUEST, the transaction is completed without further UE signaling.

The timeout duration configured through the emm and esm commands will be applicable between two retries.

Example

The following command sets the maximum number of retries allowed as 4 for all type of NAS messages in an MME service.

default nas-max-retransmissions
network-sharing

Configures additional PLMN IDs for this MME service. Refer to the plmn-id command to create the base PLMN identifier for an MME service. Each PLMN ID consists of the Mobile Country Code (MCC) and Mobile Network Code (MNC). A maximum of four network sharing entries can be configured per MME service. These PLMN IDs will be communicated to the eNodeBs in the S1 SETUP response and MME CFG Update messages.

Product
- MME

Privilege
- Administrator

Mode
- Exec > Global Configuration > Context Configuration > MME Service
- configure > context context_name > mme-service service_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-mme-service)#
```

Syntax

```
network-sharing plmn-id mcc number mnc number mme-id group-id id mme-code code
```

```
no network-sharing plmn-id mcc number mnc number
```

<table>
<thead>
<tr>
<th>no</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disables the network sharing mode on this MME service.</td>
</tr>
</tbody>
</table>

⚠️ **Caution:** Removing the PLMN identifier is a disruptive operation; the MME service will be restarted.

```
plmnid mcc number mnc number
```

Sets the mobile country code (MCC) and mobile network code (MNC) of the PLMN ID for this service.

- **mcc number:** Specifies the MCC portion of the PLMN identifier as an integer from 100 through 999.
- **mnc number:** Specifies the MNC portion of the PLMN identifier as a 2- or 3-digit integer from 00 through 999.

```
mme-id group-id id
```

Specifies the group identifier for the group to which this MME belongs as an integer from 0 through 65535.

```
mme-code code
```

Specifies the unique code for an MME service as an integer from 0 through 255.

Usage

Use this command to configure additional PLMN IDs for an MME service. In a given MME service, each PLMN ID (MCC and MNC) must be unique.
⚠️ **Caution:** Changing or removing the PLMN identifier is a disruptive operation; the MME service will be restarted.

**Example**

The following command configures the network sharing parameters to an MCC of 123, an MNC of 12, a MME-ID/Group ID of 100, and a MME code of 50:

```
network-sharing plmnid mcc 123 mnc 12 mme-id group-id 100 mme-code 50
```
nri

Configures the network resource identifier (NRI) length used for source SGSN discovery via NRI-FQDN (Fully Qualified Domain Name) based DNS resolution.

**Product**
MME

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > MME Service
configure > context context_name > mme-service service_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-mme-service)#
```

**Syntax**

```
[ no ] nri length length plmn-id mcc mcc_value mnc mnc_value
```

<table>
<thead>
<tr>
<th>no</th>
<th>Removes a configured NRI length.</th>
</tr>
</thead>
<tbody>
<tr>
<td>length length</td>
<td>Specifies the number of bits to be used in the P-TMSI (bits 23 to 18) to define the NRI as an integer from 1 through 8.</td>
</tr>
<tr>
<td>plmn-id mcc mcc_value mnc mnc_value</td>
<td>Specifies the PLMN-ID of the SGSN pool. mcc mcc_value: Specifies the mobile country code (MCC) portion of the PLMN identifier as an integer from 100 through 999. mnc mnc_value: Specifies the mobile network code (MNC) portion of the PLMN identifier as a 2- or 3-digit integer from 00 through 999.</td>
</tr>
</tbody>
</table>

**Usage**

Use this command to retrieve the NRI (identity of an SGSN) stored in bits 23 to 18 of the packet-temporary mobile subscriber identity (P-TMSI). Up to eight NRI length values can be configured.

**Important:** In the absence of this configuration, the MME treats the NRI as invalid. The MME will use a plain RAI-based FQDN (and not an NRI-based FQDN) for DNS queries made to resolve the source SGSN.

**Example**

The following command creates an NRI length of 5 and associates it with an SGSN pool with the PLMN-ID of 123:

```
nri length 5 plmnid mcc 123 mnc 23
```
peer-mme

Configures parameters that, when matched by another MME, specifies that MME as a peer for inter-MME relocations.

Product
MME

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > MME Service

configure > context context_name > mme-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-mme-service)#

Syntax

peer-mme { gummei mcc number mnc number group-id id mme-code code address ipv4_address |
   tai-match priority value mcc number mnc number tac { area_code | any | start_area_code to
   end_area_code } address ipv4_address }

no peer-mme { gummei mcc number mnc number group-id id mme-code code | tai-match priority
   value

no

Removes the configured peer Globally Unique MME Identifier (GUMMEI) or TAI match priority from this service.

---

gummei mcc number mnc number group-id id mme-code code address ipv4_address

Specifies that an MME with values matching those configured in this GUMMEI is to be considered a peer MME. This variable supports the lookup of an IP address for a peer MME based on the exact match of the supporting keyword below (which make up the GUMMEI).
mcc number: Sets the mobile country code (MCC) for peer match as an integer from 100 through 999.
mnc number: Sets the mobile network code (MNC) for this peer match as a 2- or 3-digit integer from 00 through 999.
group-id id: Specifies the group identifier for the group to which this MME belongs as an integer from 0 through 65535.
mme-code code: Specifies the unique code for an MME service as an integer from 0 through 255.
address ipv4_address: Specifies the IP address of the peer MME in IPv4 dotted-decimal notation.

---

tai-match priority value mcc number mnc number tac { area_code | any |
   start_area_code to end_area_code } address ipv4_address

Specifies that an MME with values matching those configured in this Tracking Area Identifier (TAI) match, is to be considered a peer MME. This keyword provides a priority-ordered list of TAI descriptions where the Tracking Area Code (TAC) field may be either an exact value, a range of values, or a “wildcard” value. It also provides an IP address of the peer MME corresponding to the TAI description.
priority value:
mcc number: Sets the mobile country code (MCC) for peer match as an integer from 100 through 999.
mnc number: Sets the mobile network code (MNC) for this peer match as an integer from 00 through 999.

tac area_code: Sets a specific Tracking Area Code (TAC) for the peer MME match as an integer from 1 through 65535.

tac any: Specifies that any TAC value can be considered for a peer MME.

tac start_area_code to end_area_code: Specifies a range of TACs. MMEs within this range and matching the rest of the criteria in this command are to be considered peer MMEs. start_area_code and end_area_code are integers from 1 through 268435455.

address ipv4_address: Sets a specific IP address for this TAI peer MME match in IPv4 dotted-decimal notation.

Usage

Use this command to configure parameters that, when matched by another MME, specifies that MME as a peer for inter-MME relocations.

This command allows configuration for two relocation scenarios:

• gummei: an MME receives either an Attach or a TAU request with a Globally Unique Temporary Identity (GUTI) that originated from another MME.

• tai-match: an MME receives an S1 Handover Required message and must select a new MME based on the TAI.

Up to 32 peer-mme gummei or tai-match entries may be configured per MME service.

Example

The following command identifies a peer MME with GUMMEI parameters:

peer-mme gummei mcc 123 mnc 12 group-id 40000 mme-code 100 address 10.2.3.4
peer-sgsn

Statically configures peer SGSN environments to facilitate MME-SGSN relocations over S3 or Gn/Gp interfaces.

**Product**
MME

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > MME Service

```
configure > context context_name > mme-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-mme-service)#
```

**Syntax**

```
peer-sgsn rai mcc mcc_value mnc mnc_value [ nri value ] rac value lac value address ip_address capability [ gn ] [ gp ] [ s16 ] [ s3 ]
```

```
no peer-sgsn rai mcc mcc_value mnc mnc_value [ nri value ] rac value lac value
```

```
peer-sgsn rnc-id mcc mcc_value mnc mnc_value rnc value address ip_address capability [ gn ] [ gp ] [ s16 ] [ s3 ]
```

```
no peer-sgsn rnc-id mcc mcc_value mnc mnc_value rnc value
```

**rai**

Configures Routing Area Identity (RAI) parameters used to facilitate a lookup for a specific peer SGSN.

**rnc-id**

Configures Radio Network Controller Identification (RNC-ID) parameters used to facilitate a lookup for a specific peer SGSN.

**mcc mcc_value**

Specifies the mobile country code (MCC) portion of the PLMN identifier as an integer from 100 through 999.

**mnc mnc_value**

Specifies the mobile network code (MNC) portion of the PLMN identifier as a 2- or 3-digit integer from 00 through 999.

**nri value**

Specifies the Network Resource Identifier (NRI) value used as an additional identity along with the RAC within the RAI parameters as an integer from 0 through 65535.
### MME Service Configuration Mode Commands

**peer-sgsn**

---

**rac value**

Specifies the Routing Area Code (RAC) used to facilitate a lookup for a specific peer SGSN as an integer from 0 through 255.

---

**rnc value**

Specifies the Radio Network Controller (RNC) identification number used to facilitate a lookup for a specific peer SGSN as an integer from 0 through 65535.

---

**lac value**

Specifies the Location Area Code (LAC) value used to facilitate a lookup for a specific peer SGSN as an integer from 0 through 65535.

---

**address ip_address**

Specifies an existing IP address of the peer SGSN in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

---

**capability [ gn ] [ gp ] [ s16 ] [ s3 ]**

Configures the GTP interface capability of the peer SGSN.

- **gn**: Specifies that the peer SGSN is capable of communication over the Gn interface.
- **gp**: Specifies that the peer SGSN is capable of communication over the Gp interface.
- **s16**: Specifies that the peer SGSN is capable of communication over the S16 interface.
- **s3**: Specifies that the peer SGSN is capable of communication over the S3 interface.

---

**Usage**

Use this command to configure parameters that, when matched by an SGSN, specifies that SGSN as a peer for inter-RAT relocations.

This command allows configuration for two relocation scenarios:

- **rai**: the lookup of an IP address for a peer MME based on the exact match of the RAI (and optionally NRI).
- **rnc-id**: the lookup of an IP address for a peer SGSN based on the exact match of the RNC-ID.

Multiple peer-sgsn RNC-ID records can be configured for the same MCC/MNC/RNC, each with different IP addresses. During a handover, if the initial peer SGSN rejects the forward relocation request, the MME will step through any alternate peer SGSNs to attempt the handover.

Up to 32 peer-SGSN RAI and RNC-ID entries may be configured per MME service.

---

**Example**

The following command configures an SGSN lookup using RNC-ID parameters with Gn interface capability:

```
peer-sgsn rnc-id mcc 123 mnc 12 rnc 2000 address 10.2.3.4 capability gn
```
pgw-address

Configures the IPv4 or IPv6 address of the PDN Gateway (P-GW), specifies the protocol for S5 and S8 interfaces, and sets other parameters within the MME service. By default S5 and S8 use GTP protocol for this.

Product
MME

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > MME Service
configure > context context_name > mme-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-mme-service)#

Syntax

pgw-address ip_address [ s5-s8-protocol pmip ] [ weight weight ]

no pgw-address address [ s5-s8-protocol pmip ]

no

Removes a previously configured IP address for a P-GW along with the S5 and S8 interface of P-MIP protocol type, and other parameters from this MME service.

address

Specifies the IP address of the P-GW in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

s5-s8-protocol pmip

Specifies that Proxy-MIP is to be used for S5 and S8 interfaces with the P-GW. By default S5 and S8 interface uses GTP protocol.

pmip Sets the protocol to Proxy-MIP for S5 and S8 interface.

weight weight

Specifies the weight (preference) assigned to the address P-GW for load balancing. weight is an integer from 1 through 100 where 1 is the least preferred and 100 is the most preferred. If no weight is specified, the P-GW address is assigned a default weight of 1.

If a weight is assigned to an address, the weights of the P-GW(s) (that are operational) are totaled, and then a weighted round-robin selection is used to distribute new primary PDP contexts among the P-GW(s) according to their weights. As with all weighted round-robin algorithms, the distribution does not look at the current distribution, but simply uses the weights to distribute new requests. For example, two P-GWs assigned weights of 70 and 30 would distribute 70% of calls to one, and 30% to the other. The sum of all weights do not need to total 100.
Usage

Use this command to configure the PDN Gateway (P-GW) addresses to use with MME service. This command also changes the default protocol from GTP to P-MIP for the S5 and S8 interface, and assigns a weight to use when sharing the load between associated P-GWs. A maximum of 16 P-GW addresses can be configured with this command.

This command only changes the use of protocol for the S5 and S8 interface. By default a P-GW uses GTP protocol for S5 and S8 interfaces. This command allows an operator to change the protocol to P-MIP for S5 and S8 interface.

When weight is used, the weights of the operational P-GW(s) are totaled and then weighted round-robin selection is used to distribute new default bearer contexts among P-GW(s).

Example

The following command associates the P-GW IP address of 192.168.3.1 to the MME service with S5 and S8 protocol as P-MIP and weight as 90:

```
pgw-address 192.168.3.1 s5-s8-protocol pmip weight 90
```

The following command removes the above configured P-GW IP address and other parameters:

```
no pgw-address 192.168.3.1 s5-s8-protocol pmip
```
plmn-id

Configures the Public Land Mobile Network (PLMN) identifier for this MME service. The PLMN identifier consists of the Mobile Country Code (MCC) and Mobile Network Code (MNC). A single PLMN ID can be configured per MME service.

**Product**
MME

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > MME Service
configure > context context_name > mme-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-mme-service)#

**Syntax**

```
plmn-id mcc mcc_value mnc mnc_value
no plmn-id mcc mcc_value mnc mnc_value
```

no

Removes the configured PLMN identifier for this MME service.

⚠️ **Caution:** Removing the PLMN identifier is a disruptive operation; the MME service will be restarted.

**mcc mcc_value**

Specifies the mobile country code (MCC) portion of the PLMN identifier as an integer from 100 through 999.

**mnc mnc_value**

Specifies the mobile network code (MNC) portion of the PLMN identifier as a 2- or 3-digit integer from 00 through 999.

**Usage**

Use this command to set the PLMN identifier for this MME service.

⚠️ **Caution:** Changing or removing the PLMN identifier is a disruptive operation; the MME service will be restarted.

One PLMN identifier is supported per MME service.

⚠️ **Important:** To configure additional PLMN IDs for this MME service, refer to the `network-sharing` command described in this chapter.
Example

The following command configures the PLMN identifier with MCC value as 102 and MNC value as 20 for this MME service:

```plaintext
plmn-id mcc 102 mnc 20
```
policy attach

Configures parameters for the UE Attach procedure.

**Product**
MME

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > MME Service

```bash
configure > context context_name > mme-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-mme-service)#
```

**Syntax**

```

default policy attach { imei-query-type | set-ue-time }
```

**default**

Returns the command to its default setting of `none` for `imei-query-type` and `disabled` for `set-ue-time`.

**imei-query-type { imei | imei-sv | none }**

Configures the IMEI query type for UE attach.

- **imei**: Specifies that the MME is required to query the UE for its International Mobile Equipment Identity (IMEI).
- **imei-sv**: Specifies that the MME is required to query the UE for its International Mobile Equipment Identity - Software Version (IMEI-SV).
- **none**: Specifies that the MME does not need to query for IMEI or IMEI-SV.

**verify-equipment-identity [ allow-on-eca-timeout | deny-greylisted | deny-unknown | verify-emergency ]**

Specifies that the identification (IMEI or IMEI-SV) of the UE is to be performed by the Equipment Identity Register (EIR) over the S13 interface.

- **allow-on-eca-timeout**: Configures the MME to allow equipment that has timed-out on ECA during the attach procedure.
- **deny-greylisted**: Configures the MME to deny grey-listed equipment during the attach procedure.
- **deny-unknown**: Configures the MME to deny unknown equipment during the attach procedure.
- **verify-emergency**: Configures the MME to ignore the IMEI validation of the equipment during the attach procedure in emergency cases. This keyword is only supported in release 12.2 and higher.
set-ue-time { disable | enable [ prefer-mme | prefer-msc ] }

Configures the MME to set the time in the UE during the Attach procedure. Default: disabled.
[ prefer-mme | prefer-msc ]: Specifies which UE-time to use when delivering EMM messages to the UE for cases when a UE performs combined registration.
- prefer-mme: The MME shall always send its UE-time information (based on the MME’s own settings), and ignore any EMM Information messages sent by the MSC.
- prefer-msc: In cases where a successful Location Update is performed to a MSC, the MME shall NOT send MME configured information to the UE, and shall transmit only MSC-sent information. In cases where a Location Update procedure is not required (for example, for UEs that are performing EPS only ATTACH), or in cases where the Location Update Procedure is unsuccessful, the MME shall send the MME configured information.

Usage

Use this command to configure various MME settings used during the UE Attach procedure.

Example

The following command configures the MME to query the UE for its IMEI and to verify the UEs equipment identity over the S13 interface with an EIR:

    policy attach imei-query-type imei verify-equipment-identity
policy idle-mode

Configures the user-defined policies of session management for an LTE subscriber in an MME service.

**Product**
MME

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > MME Service

`configure > context context_name > mme-service service_name`

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-mme-service)#`

**Syntax**

```
policy idle-mode detach { explicit | implicit }
[ default ] policy idle-mode detach
```

- `default`
  Sets the policy of idle mode detach for a subscriber to its default behavior as implicit.

- `idle-mode detach`
  Configures the IDLE mode Detach behavior of a UE.

- `detach`
  Defines the Detach procedure while the UE is in IDLE mode.

- `explicit`
  Enables the Explicit Detach while a UE is in IDLE mode. The system will page the UE before Detach procedure is started, and then perform the Explicit Detach procedure. Default: Enabled

- `implicit`
  Enables the Implicit Detach while a UE is in IDLE mode. The system never sends any message to the UE before Detach, and executes the Implicit Detach procedure immediately. Default: Disabled

**Usage**

Use this command to set the user-defined policies for session management in this MME service.

**Example**

The following command sets the Idle Mode Detach policy to Implicit for a user in this MME service:

```
policy idle-mode detach implicit
```
policy inter-rat

Configures inter-RAT policy settings.

**Product**
MME

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > MME Service
configure > context context_name > mme-service service_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-mme-service)#
```

**Syntax**

```
policy inter-rat { ignore-sgsn-context-id | indirect-forwarding-tunnels always | select-topologic-sgw }

no policy inter-rat { ignore-sgsn-context-id | indirect-forwarding-tunnels | select-topologic-sgw }
```

**no**
Disables the function.

**ignore-sgsn-context-id**
Configures the MME to ignore any Context-ID mismatch between HSS and HLR and to use the Context-ID from the HSS to override the Context-ID from the source SGSN. If this option is disabled (default), the MME will drop the PDN when there is a Context-ID mismatch.

**indirect-forwarding-tunnels always**
Enables establishment of Indirect Data Forwarding Tunnels (IDFT) for Gn/Gp-based Serving Radio Network Subsystem (SRNS) relocations. By default, the MME is configured to never establish IDFT.

**select-topologic-sgw interface gn**
Configures the MME to select the S-GW based on topological closeness to the P-GW for Gn/Gp handoff scenarios. Weighted distribution will occur across node pairs in the same degree and same order. By default this functionality is disabled.
During inter-RAT Gn/Gp based handoffs, the MME does not learn the P-GW host name from the old Gn/Gp SGSN as part of UE context. Without the P-GW host name, selection of the topologically closest S-GW is not possible per 3GPP standards. This functionality enables the MME to use a proprietary mechanism for learning the P-GW host name. For S3 & S10 cases, there is no need to enable this command, as GTPv2 allows the P-GW host name to be communicated to/from S4-SGSN/MME.
This functionality requires the **gw-selection co-location or gw-selection topology** commands to be enabled in the call-control-profile mode.
Note: The P-GW is anchored in the inter-RAT handoff scenarios, so regardless of the preferred weight specified in `gw-selection`, the MME always considers the S-GW’s weight for weighted distribution purposes.

**Usage**

Use this command to enable or disable establishment of indirect data forwarding tunnels for Gn/Gp-based SRNS relocations, and to enable or disable Context-Identifier overriding, and to enable or disable learning the P-GW host name during Gn/Gp handoffs for purposes of topologically-close S-GW distribution.

**Example**

The following command enables establishment of indirect data forwarding tunnels for Gn/Gp-based SRNS relocations:

```
policy inter-rat indirect-forwarding-tunnels always
```
policy network

Configures the MME to indicate to the P-GW that all peer SGSNs support dual-addressing for bearers and, subsequently, dual-addressing must be supported for all IPv4 and IPv6 PDNs. Dual-addressing on SGSNs is based on the UE’s capability to support inter-RAT roaming.

Product
MME

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > MME Service
configure > context context_name > mme-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-mme-service)#

Syntax

[ default | no ] policy network dual-addressing-supported

---

default
Returns the command to its default setting of disabled.

---

no
Removes the ability to send dual-addressing support messaging from the MME to the P-GW.

---

dual-addressing-supported
Specifies that the MME shall indicate to the P-GW that dual-addressing is supported.

Usage
Use this command to configure the MME to send messaging to the P-GW that indicate that all peer SGSNs support dual-addressing for bearers and, subsequently, dual-addressing must be supported for all IPv4 and IPv6 PDNs.

---

Important: This command can be used for Pre-release 8 and Release 8 SGSNs.
policy overcharge-protection

Enables overcharge protection where the MME can detect and signal a Loss of Signal Contact to the S-GW which in turn informs the P-GW to stop charging.

**Product**
MME

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > MME Service

`configure > context context_name > mme-service service_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-mme-service)#
```

**Syntax**

```
policy overcharge-protection slap-cause-code-group group_name
[ default | no ] policy overcharge-protection
```

**default**

Returns the command to its default setting of disabled. This provides the same behavior as the `no` keyword option.

**no**

Disables overcharge protection. This provides the same behavior as the `default` keyword option.

```
slap-cause-code-group group_name
```

`group_name`: Specify the name of a preconfigured S1-AP Cause Code Group.

When the received cause code from the eNodeB matches any the cause codes defined in this Cause Code Group, the MME sets the ARRL (Abnormal Release of Radio Link) bit in the Indication IE of the Release Access Bearer Request to the S-GW.

For more information about creating an S1-AP Cause Code Group, refer to the `cause-code-group` command in the LTE Policy Configuration Mode Commands chapter, and the `class` command in the SIAP Cause Code Configuration Mode Commands chapter.

**Usage**

**Important**: Overcharge protection is a license-controlled feature. A valid feature license must be installed prior to configuring this feature. Contact your Cisco account representative for more information.

Use this command to enable or disable overcharging protection for this MME service. When enabled, the MME can detect and signal a Loss of Signal Contact to the S-GW which in turn informs the P-GW to stop charging for the UE.
Refer to the *Overcharging Protection* chapter of the *MME Administration Guide* for more information about this feature.

**Example**

The following command enables overcharging protection for the S1-AP cause code defined in the S1AP Cause Code Group *group1*:

```
policy overcharge-protection s1ap-cause-code-group group1
```
policy overload

Configures the traffic overload policy to control congestion in this service.

**Product**
MME

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > MME Service
configure > context context_name > mme-service service_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-mme-service)#
```

**Syntax**

```
policy overload { drop | reject }
default policy overload
```

---

**default**
Sets the traffic overload policy action to the fault behavior of Reject.

**drop**
 Specifies that the system is to drop the incoming packets with new session requests to avoid overload on MME node. Default: Disabled

**reject**
 Configures the system to reject the new session/call request and responds with a reject message when the threshold for allowed call sessions is crossed on the MME node. Default: Enabled

**Usage**

Use this command to set the user-defined policies for new call connection attempts when an MME service is overloaded.

Congestion policies at the service-level can be configured for an individual service. When congestion control functionality is enabled, these policies dictate how services respond when the system detects that a congestion condition threshold has been crossed.

**Example**

The following command sets the nw call connect policy to reject the new session/call request in an MME service:

```
policy overload reject
```
policy pdn-reconnection

Configures the action by the MME when a PDN connection request to an already connected APN is being processed by the MME service.

Product
MME

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > MME Service
configure > context context_name > mme-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-mme-service)#

Syntax

policy pdn-reconnection { multiple | reject | restart }

[ default ] policy pdn-reconnection

---

default
Sets the policy for PDN reconnection to its default behavior of Reject.

multiple
Allows multiple connections to a PDN with the same APN and PDN Type. In this case, the existing connection is left unchanged, and the MME attempts to establish an additional connection to the PDN. Default: Disabled

reject
Configures the MME to deny or reject the request, by sending a PDN Connection Reject command. This is the default behavior. Default: Enabled

restart
Deletes the existing connection and initiates an attempt to establish a new connection. Default: Disabled

Usage

Use this command to set the user-defined policies for PDN reconnection attempt procedures initiated by a UE in an MME service.

While attached the UE can request connections to PDNs. The PDNs are identified by APN (Access Point Name) and PDN Type (ipv4, ipv6 or ipv4v6).

If the UE requests connection to a PDN for which a connection with the same APN name and PDN type already exists, the MME can: 1) deny or reject the request, by sending a PDN connection reject command; 2)
allow multiple connections to a PDN with same APN and PDN Type; or 3) delete the existing connection, and attempt to establish a new connection.

**Example**

The following command sets the PDN reconnect policy to delete the existing PDN and start the attempt to establish a new connection in an MME service:

```
policy pdn-reconnection restart
```
policy s1-reset

Configures how the MME responds to an S1 interface reset.

Product
MME

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > MME Service

configure > context context_name > mme-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-mme-service)#

Syntax

policy s1-reset { detach-ue | idle-mode-entry }

default policy s1-reset

<table>
<thead>
<tr>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Returns the command to its default setting of idle-mode-entry.</td>
</tr>
</tbody>
</table>

| { detach-ue | idle-mode-entry } |
|-------------------------------|
| Specifies the action to perform when the S1 interface is reset. |
| detach-ue: Specifies that UEs are to be implicitly detached from the service upon S1 interface reset. |
| idle-mode-entry: Specifies that UEs are to be placed into an idle mode condition during S1 interface reset. |

Usage
Use this command to configure how the MME reacts to an S1 interface reset condition.

Example
The following command configures the MME to place UEs into an idle state while the S1 interface is being reset:

s1-reset idle-mode-entry
policy sctp-down

Configures how the MME responds to a failure of the Stream Control Transmission Protocol (SCTP) connection from the eNodeB.

Product
MME

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > MME Service

configure > context context_name > mme-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-mme-service)#

Syntax

policy sctp-down { detach-ue | idle-mode-entry }

default policy sctp-down

default

Returns the command to its default setting of idle-mode-entry.

{ detach-ue | idle-mode-entry }

Specifies the action to perform when the SCTP connection from the eNodeB fails.

detach-ue: Specifies that UEs are to be detached from the service upon SCTP failure.

idle-mode-entry: Specifies that UEs are to be placed into an idle mode condition upon SCTP failure.

Usage

Use this command to configure how the MME reacts to an SCTP connection failure condition.

Example

The following command configures the MME to place UEs into an idle state while the SCTP connection from the eNodeB fails:

sctp-down idle-mode-entry
policy service-request

Configure the behavior of the MME when an initial context setup failure is received during a service request or extended service request procedure.

Product
MME

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > MME Service
configure > context context_name > mme-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-mme-service)#

Syntax

policy service-request initial-context-setup-failure slap-cause-code-group group_name action idle-mode-entry

default policy service-request initial-context-setup-failure

default

Returns the command to its default behavior, where it detaches the UE when an initial context setup failure is received during a service request or extended service request procedure.

initial-context-setup-failure slap-cause-code-group group_name action idle-mode-entry

Configures the behavior of the MME when an initial context failure is received from the eNodeB during a service request or extended service request. By default, the MME detaches the UE. This command configures the MME to move the UE to IDLE MODE instead.

group_name: Specify the name of a preconfigured Cause Code Group. The MME takes the configured action to move the UE to IDLE MODE when the cause code returned from the eNodeB matches any of the cause codes defined in this Cause Code Group.

Refer to the cause-code-group command in the LTE Policy Configuration Mode Commands chapter, and the class command in the S1AP Cause Code Configuration Mode Commands chapter for more information.

action idle-mode-entry : Configures the MME to move the UE to IDLE MODE when the cause code returned from the eNodeB matches any of the cause codes in the specified S1-AP cause code group.

Usage

Use this command to configure the behavior of the MME when an initial context setup failure is received during a service request or extended service request procedure.

Example

The following command configures the MME to detach the UE when an initial context failure occurs and the eNodeB returns a cause code which matches any of the cause codes configured in the idle S1-AP cause code group:
policy service-request initial-context-setup-failure s1ap-cause-code-group idle action idle-mode-entry
policy tau

Configures parameters for the tracking area update (TAU) procedure.

**Product**
MME

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > MME Service
configure > context context_name > mme-service service_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-mme-service)#
```

**Syntax**

```
policy tau { imei-query-type { imei | imei-sv | none } | verify-equipment-identity [ allow-on-eca-timeout | deny-greylisted | deny-unknown | verify-emergency ] } | initial-context-setup-failure slap-cause-code-group group_name action detach-ue | set-ue-time { disable | enable [ prefer-mme | prefer-msc ] } }
```

```
default policy tau { imei-query-type | initial-context-setup-failure | set-ue-time }
```

**default**

Returns the command to its default settings:

```
imei-query-type: none
initial-context-setup-failure: Returns the MME to the default behavior, where it moves the UE to IDLE MODE when an initial context setup failure is received during a TAU procedure.
set-ue-time: disabled
```

**imei-query-type { imei | imei-sv | none }**

Configures the IMEI query type for TAUs.

- **imei**: Specifies that the MME is required to query the UE for its International Mobile Equipment Identity (IMEI).
- **imei-sv**: Specifies that the MME is required to query the UE for its International Mobile Equipment Identity - Software Version (IMEI-SV).
- **none**: Specifies that the MME does not need to query for IMEI or IMEI-SV.

**verify-equipment-identity [ allow-on-eca-timeout | deny-greylisted | deny-unknown | verify-emergency ]**

Specifies that the identification (IMEI or IMEI-SV) of the UE is to be performed by the Equipment Identity Register (EIR) over the S13 interface.

- **allow-on-eca-timeout**: Configures the MME to allow equipment that has timed-out on ECA during the attach procedure.
- **deny-greylisted**: Configures the MME to deny grey-listed equipment during the attach procedure.
- **deny-unknown**: Configures the MME to deny unknown equipment during the attach procedure.

- **verify-emergency**: Configures the MME to ignore the IMEI validation of the equipment during the attach procedure in emergency cases. This keyword is only supported in release 12.2 and higher.

```bash
initial-context-setup-failure slap-cause-code-group group_name action detach-ue
```

Configures the behavior of the MME when an initial context failure is received from the eNodeB during the processing of a TAU request. By default, the MME moves the UE to IDLE MODE. This keyword configures the MME to detach the UE.

- **group_name**: Specify a preconfigured Cause Code Group. The MME takes the configured action to detach the UE when the cause code returned from the eNodeB matches any of the cause codes defined in this Cause Code Group.

- **action detach-ue**: Configures the MME to detach the UE when the cause code returned from the eNodeB matches any of the cause codes in the specified S1-AP cause code group.

```bash
set-ue-time { disable | enable [ prefer-mme | prefer-msc ] }
```

Configures the MME to set the time in the UE during the TAU procedure. Default: disabled.

- **[ prefer-mme | prefer-msc ]**: Specifies which UE-time to use when delivering EMM messages to the UE for cases when a UE performs combined registration.

- **prefer-mme**: The MME shall always send its UE-time information (based on the MME’s own settings), and ignore any EMM Information messages sent by the MSC.

- **prefer-msc**: In cases where a successful Location Update is performed to a MSC, the MME shall NOT send MME configured information to the UE, and shall transmit only MSC-sent information. In cases where a Location Update procedure is not required (for example, for UEs that are performing EPS only ATTACH), or in cases where the Location Update Procedure is unsuccessful, the MME shall send the MME configured information.

**Usage**

Use this command to configure various MME settings used during the tracking area update (TAU) procedure.

**Example**

The following command configures the MME to query the UE for its IMEI and to verify the UEs equipment identity over the S13 interface with an EIR:

```bash
policy tau imei-query-type imei verify-equipment-identity
```

The following command configures the MME to detach the UE when an initial context failure occurs and the eNodeB returns a cause code which matches any of the cause codes configured in the “detach” S1-AP cause code group:

```bash
policy tau initial-context-setup-failure slap-cause-code-group detach action detach-ue
```
pool-area

Creates an MSC server pool area for the Sv interface or specifies an existing pool area, and enters MME MSC Server Pool Area Configuration Mode.

**Product**
MME

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > MME Service

configure > context context_name > mme-service service_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-mme-service) #
```

**Syntax**

```plaintext
pool-area pool_area_name type { hash-value | round-robin }

no pool-area pool_area_name
```

**no**
Removes the configured pool-area for this MME service.

```plaintext
pool_area_name
```
Specifies the name of the pool-area as an alphanumeric string of 1 through 63 characters.

```plaintext
type { hash-value | round-robin }
```
Defines the MSC server selection scheme, either:

**hash-value**: The MME selects the MSC server based on the result of the IMSI \([\text{IMSI} \div 10] \mod 1000\].

**round-robin**: The MME selects the MSC server based on the round-robin scheme.

**Usage**

Use this command to create an MSC server pool area for the Sv interface or specify an existing pool area configuration and enter the MME Pool Area Configuration Mode.

The command also defines the MSC server selection method for the pool area, using either the IMSI hash value, or round-robin.

This command is also used to remove an existing pool area.

A maximum of 24 pool areas can be configured per MME service.

When configured, the MME attempts to select an MSC using the following selection order:

1. Pool area that matches the PLMN and of type hash.
2. Pool area that matches the PLMN and of type round-robin.
3. Pool area that does not have PLMN associated and of type hash.
4. Pool area that does not have PLMN associated and of type round-robin.

Entering this command results in one of the following prompts, based on the pool selection method specified:
Additional commands are defined in the *MME MSC Server Pool Area Configuration Mode Commands* chapter.

**Example**

The following command defines a pool area named `msc_pool_east` and configures it for the round robin selection mode.

```
pool-area msc_pool_east type round-robin
```
**relative-capacity**

Configures a relative capacity variable that is sent to the eNodeB for use in selecting an MME in order to load balance the pool.

**Product**
MME

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > MME Service

```bash
configure > context context_name > mme-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-mme-service)#
```

**Syntax**

```bash
relative-capacity number
```

**default relative-capacity**

```
default
```

Returns the command to its default setting of 255.

```
number
```

Specifies the relative capacity or weight of an MME compared to others in an MME pool as an integer from 0 through 255.
Default: 255

**Usage**

Use this command to configure the relative capacity or weight of this MME in comparison to other MMEs in a pool. This value is sent to the eNodeB in the S1AP S1 SETUP RESPONSE message. If this value is changed after the S1 interface is initialized, the MME CONFIGURATION UPDATE message is used to update the eNodeB with the change.

**Example**

The following command sets this MME with a relative capacity or weight of 100:

```bash
relative-capacity 100
```
### s1-mme ip

Configures the quality of service (QoS) differentiated service code point (DSCP) used when sending packets of a particular 3GPP QoS class over the S1-MME interface.

**Product**
MME

**Privilege**
Administrator

**Mode**

```
Exec > Global Configuration > Context Configuration > MME Service
configure > context context_name > mme-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-mme-service)>
```

**Syntax**

```
s1-mme ip qos-dscp { af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 |
| af42 | af43 | be | cs0 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef }

default s1-mme ip qos-dscp
```

**qos-dscp**

```
qos-dscp { af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 |
| af42 | af43 | be | cs0 | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef }
```

Default: af11

Specifies the DSCP for the specified QoS traffic pattern. *qos-dscp* can be configured to any one of the following:

- **af11**: Assured Forwarding 11 per-hop-behavior (PHB)
- **af12**: Assured Forwarding 12 PHB
- **af13**: Assured Forwarding 13 PHB
- **af21**: Assured Forwarding 21 PHB
- **af22**: Assured Forwarding 22 PHB
- **af23**: Assured Forwarding 23 PHB
- **af31**: Assured Forwarding 31 PHB
- **af32**: Assured Forwarding 32 PHB
- **af33**: Assured Forwarding 33 PHB
- **af41**: Assured Forwarding 41 PHB
- **af42**: Assured Forwarding 42 PHB
- **af43**: Assured Forwarding 43 PHB
- **be**: Best effort forwarding PHB
- **cs0**: Class Selector 0 PHB
- **cs1**: Class Selector 1 PHB
- **cs2**: Class Selector 2 PHB
- **cs3**: Class Selector 3 PHB
- **cs4**: Class Selector 4 PHB
- **cs5**: Class Selector 5 PHB
- **cs6**: Class Selector 6 PHB
- **cs7**: Class Selector 7 PHB
ef: Expedited forwarding PHB

Usage

DSCP levels can be assigned to specific traffic patterns to ensure that packets are delivered according to the precedence with which they are tagged. The diffserv markings are applied to the IP header of every subscriber packet transmitted over the S1-MME interface(s).

Example

The following command sets the DSCP-level for traffic sent over the S1-MME interface to af12:

```
s1-mme ip qos-dscp af12
```
s1-mme sctp port

Configures the source Stream Control Transmission Protocol (SCTP) port that will be used for binding the SCTP socket to communicate with the eNodeB using S1AP with this MME service.

Product
MME

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > MME Service

configure > context context_name > mme-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-mme-service)#

Syntax

s1-mme sctp port port_num

default s1-mme sctp port

default

Sets the SCTP port to the default value of 36412 to communicate with the eNodeBs using S1-MME interface.

port_num

Specifies the SCTP port number to communicate with the eNodeBs using S1-MME interface as an integer from 1 through 65535. Default: 36412

Usage

Use this command to assign the SCTP port with SCTP socket to communicate with the eNodeB using S1AP. Only one SCTP port can be associated with one MME service.

Example

The following command sets the default SCTP port number 699 for to interact with eNodeB using S1AP on S1-MME interface:

    default s1-mme sctp port
setup-timeout

Configures the timeout duration for setting up MME calls in this MME service.

Product
MME

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > MME Service

configure > context context_name > mme-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-mme-service)#

Syntax

setup-timeout dur

default setup-timeout

default
Sets the call setup timeout duration to the default value of 60 seconds.

dur
Specifies the call setup timeout duration (in seconds) for MME calls after which the attempt will be discarded.
dur is an integer from 1 through 10000. Default: 60

Usage

Use this command to configure the timeout duration for setting up an MME call with an MME service. Once this timer expires, the call setup procedure will be discarded within this MME service.

Example

The following command sets the default setup timeout duration of 60 seconds for MME calls:

default setup-timeout
snmp trap

Enables or disables the SNMP trap for S1 interface connection establishment.

**Product**
MME

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > MME Service

    configure > context context_name > mme-service service_name

Entering the above command sequence results in the following prompt:

    [context_name]host_name(config-mme-service)#

**Syntax**

    [ default | no ] snmp trap { s1-initial-establishment | s1-path-establishment }

---

**default**

Returns the command to its default setting of disabled.

---

**no**

Disables the SNMP trap.

---

**s1-initial-establishment**

Specifies that the SNMP trap for the initial S1 interface connection establishment is to be enabled or disabled.

---

**s1-path-establishment**

Specifies that the SNMP trap for the S1 path establishment is to be enabled or disabled.

---

**Usage**

Use this command to enable or disabled the SNMP trap for S1 interface connection establishment.
ue-db

Configures the UE database that is maintained by the MME as a cache of EPS contexts per UE keyed by IMSI/GUTI to allow the UE to attach by a Globally Unique Temporary Identity (GUTI) and reuse previously established security parameters. This cache will be maintained in each session manager where the first attach occurred for the UE.

Product
MME

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > MME Service

configure > context context_name > mme-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-mme-service)#

Syntax

ue-db purge-timeout dur_mins

default ue-db purge-timeout

Usage
Use this command to set timeout duration for MME to hold UE database information in cache memory. The MME DB acts as a cache for storing subscriber related information. This subscriber related information helps reduce signaling traffic. The MME DB is a part of the Session Manager and interfaces between the Session Manager Application and Evolved Mobility Management Manager to provide access to the cached data.

Example
The following command configures the MME database cache timer to hold the UE information up to 7 days (10080 minutes) in the MME Database:

default ue-db purge-timeout
Chapter 218
MME SGs Service Configuration Mode Commands

The MME SGs Service Configuration Mode is used to create and manage the LTE Mobility Management Entity (MME) SGs services on this system. The SGs service creates an SGs interface between the MME and a Mobile Switching Center/Visitor Location Register (MSC/VLR).

Mode

Exec > Global Configuration > Context Configuration > MME SGs Service Configuration

`configure > context context_name > sgs-service service_name`

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-sgs-service)#`

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
associate

Associates or disassociates a Stream Control Transmission Protocol (SCTP) parameter template with the SGs service.

Product
MME

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > MME SGs Service Configuration

configure > context context_name > sgs-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-sgs-service)#

Syntax

associate sctp-param-template template_name

no associate sctp-param-template

no

Removes the SCTP parameter template association.

template_name

Associates an SCTP parameter template with the SGs service.

.template_name specifies the name for a pre-configured SCTP parameter template to associate with this SGs service as an alphanumeric string of 1 through 63 characters. For more information on the SCTP parameter template, refer to the sctp-param-template command in the Global Configuration Mode Commands chapter and the SCTP Parameter Template Configuration Mode Commands chapter.

Usage

Use this command to associate a pre-configured SCTP parameter template with the SGs service.

⚠️ Caution: This is a critical configuration. Any change to this configuration will cause the SGs service to restart.

ℹ️ Important: If no SCTP parameter template is specified, all default settings for the configurable parameters in the SCTP Parameter Template Configuration Mode apply.

Example

The following command associates a pre-configured SCTP parameter template called sctp-3 to the SGs service:

associate sctp-param-template sctp-3
**bind**

Binds the service to a logical IP interface serving as the SGs interface.

**Product**
MME

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > MME SGs Service Configuration

```
configure > context context_name > sgs-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgs-service)#
```

**Syntax**

```
bind { ipv4-address ipv4_address [ ipv4-address ipv4_address ] | ipv6-address ipv6_address [ ipv6-address ipv6_address ] }
```

**no bind**

Removes the interface binding from this service.

```
no bind
```

**ipv4-address ipv4_address [ ipv4-address ipv4_address ]**

Specifies the IP address of the SGs interface in IPv4 dotted-decimal notation. A secondary IPv4 address can be configured to support SCTP multi-homing.

```
ipv4-address ipv4_address [ ipv4-address ipv4_address ]
```

**ipv6-address ipv6_address [ ipv6-address ipv6_address ]**

Specifies the IP address of the SGs interface in IPv6 colon-separated-hexadecimal notation. A secondary IPv6 address can be configured to support SCTP multi-homing.

```
ipv6-address ipv6_address [ ipv6-address ipv6_address ]
```

**Usage**

Associate the SGs service to a specific logical IP address. The logical IP address or interface takes on the characteristics of an SGs interface that provides the session connectivity for circuit switched fallback (CSFB) to/from a Mobile Switching Center/Visitor Location Register (MSC/VLR). Only one interface can be bound to a service. The interface should be configured prior to issuing this command.

**Caution:** This is a critical configuration. Any change to this configuration will cause the SGs service to restart. Removing or disabling this configuration will stop the SGs service.

**Example**

The following command binds the logical IP interface with the IPv4 address of 192.68.10.22 to the SGs service:

```
bind ipv4-address 192.68.10.22
```
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**
Use this command to return to the parent configuration mode.
non-pool-area

Configures a non-pool area where a group of Location Area Code (LAC) values use a specific visitor Location Register (VLR).

Product
MME

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > MME SGs Service Configuration

configure > context context_name > sgs-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-sgs-service)#

Syntax

non-pool-area name use-vlr vlr_name [ lac value(s) ] [ plmnid { any | mcc mcc_value mnc mnc_value } ]

no non-pool-area name [ lac value(s) ]

no non-pool-area name [ lac value(s) ]

Removes the configured non-pool-area from this service. Optionally, removes a specific LAC or LACs from this non-pool area. name is the name of an existing non-pool-area expressed as an alphanumeric string of 1 through 63 characters. value(s) is an existing LAC integer value from 1 through 65535.

name

Specifies the name of the non-pool area as an alphanumeric string of 1 through 63 characters.

use-vlr vlr_name

Specifies the VLR to be used in this non-pool area configuration as an alphanumeric string of 1 through 63 characters.

lac value(s)

Specifies the location area code or codes to be used with the configured VLR in this non-pool area configuration. value(s) is an integer(s) from 1 through 65535.
In Release 12.2 and later, a maximum of 96 areas can be added per non pool area (in a single line, or separately). In older releases, a total of 16 area codes can be added (in a single line, or separately).

plmnid { any | mcc mcc_value mnc mnc_value }

Specifies the Public Land Mobile Network (PLMN) identifier to be used with the VLR in this non-pool area configuration.
any: Specifies that any PLMN ID can be used with the VLR in this configuration.
**mcc mcc_value mnc mnc_value:** Specifies the mobile country code (MCC) and mobile network code (MNC) of the PLMN identifier. `mcc_value` must be an integer from 101 through 998. `mnc_value` must be a 2- or 3-digit integer from 00 through 998.

### Usage

Use this command to configure a non-pool area where LAC values and/or PLMN IDs are associated with a specific VLR.

In Release 12.2 and later, a maximum of 48 combined non pool areas and pool areas can be created. In older releases, a maximum of 8 combined non pool areas and pool areas can be created.

### Example

The following command creates a non-pool area named `svlr1` associated with a VLR named `vlr1` and containing LAC values of 1, 2, 3, 4, 5, 6, 7, and 8:

```
non-pool-area svlr1 use-vlr vlr1 lac 1 2 3 4 5 6 7 8
```
pool-area

Creates a location area code (LAC) pool area configuration or specifies an existing pool area and enters the LAC Pool Area Configuration Mode.

**Product**
MME

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > MME SGs Service Configuration

```
configure > context context_name > sgs-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgs-service)#
```

**Syntax**

```
[ no ] pool-area pool_name [ -noconfirm ]
```

- **no**
  Removes the selected pool area configuration from the SGs service.

- **pool_name**
  Specifies the name of the LAC pool area configuration. If `pool_name` does not refer to an existing pool, a new pool is created. `pool_name` must be an alphanumeric string of 1 through 64 characters.

**Usage**

Use this command to enter the LAC Pool Area Configuration Mode for an existing pool area configuration or for a newly defined pool area configuration. This command is also used to remove an existing pool area configuration.

In Release 12.2 and later, a maximum of 48 combined pool areas and non pool areas can be created. In older releases, a maximum of 8 combined pool areas and non pool areas can be created.

Entering this command results in the following prompt:

```
[context_name]host_name(config-sgs-pool-area)#
```

LAC Pool Area Configuration Mode commands are defined in the *MME LAC Pool Area Configuration Mode Commands* chapter.

**Example**

The following command enters the LAC Pool Area Configuration Mode for a new or existing pool area configuration named `pool1`:

```
pool-area pool1
```
sctp

Configures the Stream Control Transmission Protocol (SCTP) port number for this service.

**Product**
MME

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > MME SGs Service Configuration

`configure > context context_name > sgs-service service_name`

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-sgs-service)#`

**Syntax**

```
sctp port port_number

no sctp
```

---

**no**

Removes the SCTP configuration for this service.

---

**port port_number**

Specifies the SCTP port number used to communicate with the MSC/VLR using the SGs interface as an integer from 1 through 65535.

---

**Usage**

Use this command to assign the SCTP port with SCTP socket to communicate with the MSC/VLR through the SGs interface. A maximum of one SCTP port can be associated with one SGs service.

**Example**

The following command sets the SCTP port to 29118 for this service:

```
sctp port 29118
```
tac-to-lac-mapping

Maps any Tracking Area Code (TAC) value or a specific TAC value to a LAC value.

Product
MME

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > MME SGs Service Configuration
configure > context context_name > sgs-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-sgs-service)#

Syntax

```
tac-to-lac-mapping { any-tac | tac value } map-to lac value +
no tac-to-lac-mapping { any-tac | { tac value } + }
```

```
any-tac | tac value
```

Specifies the TAC to map to the LAC.

any-tac: Specifies that any TAC value is to be mapped to the specified LAC.

```
tac value
```

Maps a specific TAC value to a LAC value expressed as an integer from 1 through 65535. For specific TAC values, multiple mappings can be entered on the same line (see Example).

```
map-to lac value
```

Specifies the LAC value that the selected TAC value, or any TAC value is mapped as an integer from 1 through 65535. For specific TAC values, multiple mappings can be entered on the same line (see Example).

Usage

Use this command to map TAC values to LAC values.
Enter up to 8 mappings per line.
In Release 12.2 and later, a maximum of 64 mapping lists can be created. In older releases, a maximum of 32 mapping lists can be created.
If no mapping is entered, the default behavior is TAC equals LAC.

Example

The following command maps a TAC value of 2 to a LAC value of 3, a TAC value of 4 to a LAC value of 5, and a TAC value of 6 to a LAC value of 7:

```
tac-to-lac-mapping tac 2 map-to lac 3 tac 4 map-to lac 5 tac 6 map-to lac 7
```
**timer**

Configures the SGs-AP timer values.

**Product**
MME

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > MME SGs Service Configuration

```plaintext
configure > context context_name > sgs-service service_name
```

Entering the above command sequence results in the following prompt:

```plaintext
[context_name]host_name(config-sgs-service)#
```

**Syntax**

```plaintext
timer { ts6-1 value | ts10 value | ts12-1 value | ts12-2 value | ts13 value | ts8 value | ts9 value }
default timer { ts10 | ts12-1 | ts12-2 | ts13 | ts6-1 | ts8 | ts9 }
```

Returns the timer to its default setting.

**ts10 value**

Specifies the Ts10 timer value (in seconds) as an integer from 1 through 30. This timer is used to guard the Implicit IMSI detach from non-EPS services procedure. Default: 4.

**ts12-1 value**

Specifies the Ts12-1 timer value (in seconds) as an integer from 8 through 23048. This timer is used to control the reset of the 'MME-Reset' variable. It is expected to take a value greater than the longest periodic tracking area update timer running on the MME, plus the transmission delay on the radio interface. Default: 36000.

**ts12-2 value**

Specifies the Ts12-2 timer value (in seconds) as an integer from 1 through 120. This timer is used to guard the MME reset procedure. There is one Ts12-2 timer per VLR for which the MME has an SGs association. Default: 4.

**ts13 value**

Specifies the Ts13 timer value (in seconds) as an integer from 1 through 30. This timer configures the retransmission interval for sending SGs message SGsAP-EPS-DETACH-INDICATION to MSC/VLR due to an Implicit IMSI detach from EPS services. If no SGsAP-EPS-DETACH-ACK is received, the MME will resend SGsAP-EPS-DETACH-INDICATION message upon expiry of this timer. Default: 4.
**ts6-1 value**

Specifies the Ts6-1 timer value (in seconds) as an integer from 10 through 90. This timer is used to guard the Location Update procedure. It is expected to take a value greater than 2 times the maximum transmission time in the SGs interface, plus the supervision timer of the Update Location procedure (as defined in 3GPP TS 29.002 [15]).

Default: 15.

**ts8 value**

Specifies the Ts8 timer value (in seconds) as an integer from 1 through 30. This timer is used to guard the Explicit IMSI detach from EPS services procedure.

Default: 4.

**ts9 value**

Specifies the Ts9 timer value (in seconds) as an integer from 1 through 30. This timer guards the Explicit IMSI detach from non-EPS services procedure.

Default: 4.

**Usage**

Use this command to configure the SGs-AP timers.

**Example**

The following command sets the SGs-AP Ts6-1 timer to 20 seconds:

```
timer ts6-1 20
```
vlr

Configures the Visitor Location Register (VLR) to be used by this service.

Product
MME

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > MME SGs Service Configuration
configure > context context_name > sgs-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-sgs-service)#

Syntax

vlr vlr_name { ipv4-address ipv4_address [ ipv4-address ipv4_address ] | ipv6-address ipv6_address [ ipv6-address ipv6_address ] } port port_number

no vlr vlr_name

no

Removes the configured VLR from this service.

vlr_name

Specifies the name of the VLR as an alphanumeric string of 1 through 63 characters.

ipv4-address ipv4_address [ ipv4-address ipv4_address ]

Specifies the IP address of the VLR in IPv4 dotted-decimal notation.
A secondary IPv4 address can be configured to support SCTP multi-homing.

ipv6-address ipv6_address [ ipv6-address ipv6_address ]

Specifies the IPv6 address of the VLR. ipv6_address must be entered in colon-separated-hexadecimal notation.
A secondary IPv6 address can be configured to support SCTP multi-homing.

port port_number

Specifies the SCTP port number as an integer from 1 through 65535.

Usage

Use this command to configure the VLR used by this SGs service.
In Release 12.2 and later, a maximum of 48 separate VLRs can be created. In older releases, a maximum of 32 separate VLRs can be created.
Each individual VLR can be defined with up to 10 separate associations to a single MSS pool. Each of these associations support SCTP multi-homing by defining a primary/secondary IP address. Application layer
messages are transmitted to the first available association for a particular VLR. If a complete failure of the underlying SCTP layer for a given association (for example, both SCTP paths in a multi-homed configuration) occurs, the VLR association is removed as a candidate for application message transmission until it recovers. A given MMS (VLR) will remain available as long as at least one related association remains available.

Example

The following command configures a VLR to be used by this service with a name of `vlr1`, with an SCTP multi-homed primary IPv4 address of 10.2.3.4, a secondary IPv4 address of 10.2.10.1, and a port number of 29118:

```
vlr vlr1 ipv4-address 10.2.3.4 ipv4-address 10.2.10.1 port 29118
```
Chapter 219
MPLS-IP Configuration Mode Commands

The MPLS-IP Configuration Mode is used for configuration of Multiprotocol Label Switching (MPLS) IP forwarding specific parameters. This mode is entered from the Context Configuration Mode.

Mode

Exec > Global Configuration > Context Configuration > MPLS-IP Configuration
configure > context context_name > mpls-ip

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-mpls)#

⚠️ **Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**

Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Use this command to return to the parent configuration mode.
**protocol ldp**

Creates or removes the MPLS label distribution protocol (LDP) configuration, or configures an existing protocol and enters the MPLS-LDP Configuration Mode in the current context. This command configures the protocol parameters for MPLS LDP.

**Product**
- GGSN
- P-GW
- SAEGW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > MPLS-IP Configuration

```bash
configure > context context_name > mpls-ip
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-mpls)#
```

**Syntax**

```
[ no ] protocol ldp
```

```
no
```

Removes the configured MPLS-LDP mode from MPLS-IP Configuration mode.

**Usage**

Use this command to create/ or remove the MPLS LDP configuration, or configure an existing protocol. If required mode already exists it enters the MPLS-LDP Configuration Mode in the current context. Entering this command results in the following prompt:

```
[context_name]host_name(config-ldp)#
```

The commands configured in this mode are defined in the *MPLS-LDP Configuration Mode Commands* chapter.

**Example**

The following command creates and enters the MPLS-LDP Protocol mode:

```
protocol ldp
```
Chapter 220
MPLS-LDP Configuration Mode Commands

The MPLS-LDP Configuration Mode is used to configure Label Distribution Protocol (LDP) specific parameters for MPLS-IP forwarding.

Mode

Exec > Global Configuration > Context Configuration > MPLS-IP Configuration > MPLS-LDP Configuration

configure > context context_name > mpls-ip > protocol ldp

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ldp)#

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
advertise-labels

Configures the Label Advertisement parameters.

Product
GGSN
P-GW
SAEGW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > MPLS-IP Configuration > MPLS-LDP Configuration
configure > context context_name > mpls-ip > protocol ldp

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ldp)#

Syntax
[ no ] advertise-labels { explicit-null | implicit-null }

default advertise-labels

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Disables the label advertisement parameters.</td>
</tr>
</tbody>
</table>

**default**
Advertises the labels from the label space allocated for LDP protocol.

**explicit-null**
Advertises the Explicit NULL label for all the prefixes.

**implicit-null**
Advertises the Implicit NULL label for all the prefixes.

Usage
Use this to configure advertisement of the Implicit NULL or Explicit NULL label for all the prefixes advertised by the system in this context.

Example
The following command configures the MPLS-IP forwarding to advertise the Explicit NULL label for all the prefixes:

```
advertise-labels explicit-null
```

The following command configures the MPLS-IP forwarding to advertise the Implicit NULL label for all the prefixes:

```
advertise-labels implicit-null
```
advertise-labels implicit-null
discovery

Configures the Label Distribution Protocol (LDP) neighbor discovery parameters.

Product

GGSN
P-GW
SAEGW

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > Context Configuration > MPLS-IP Configuration > MPLS-LDP Configuration

configure > context context_name > mpls-ip > protocol ldp

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ldp)#

Syntax

```
discovery { hello { hello-interval integer_value | hold-interval integer_value } | transport-address ipv4_addr } | default discovery hello

no discovery transport-address
```

---

default

Sets the LDP discovery hello interval at 5 seconds and hold interval at 15 seconds.

---

no

Disables the LDP neighbor discovery.

---

`hello { hello-interval integer_value | hold-interval integer_value }`

Configures the LDP Hello parameters.

- `hello-interval` configures the frequency of sending the Discovery Hello packets in seconds. `integer_value` is an integer from 5 through 21845.
- Default: 5

- `hold-interval` configures the Discovery Hold time interval in seconds. `integer_value` is an integer from 15 through 65535.
- Default: 15

---

`transport-address ipv4_addr`

Configures the LDP transport address as an IPv4 address entered in dotted-decimal notation. Transport address is the same as the LDP router ID.
Usage
This is an optional command that is used to configure LDP peer discovery parameters. The LDP discovery hold-interval is always set to three times the LDP discovery hello-interval. Transport address is the address used for the TCP session over which LDP is running. If the transport address is not configured, the LDP router-id is used as transport address. Any update to transport address will take effect only if LDP is disabled and re-enabled. The “default” option sets the hello intervals to the default values.

Example
The following command sequence configures the LDP peer discovery parameters:

```
  discovery hello hello-interval 10
  discovery hello hold-interval 30
  discovery transport-address 10.2.3.4
```
enable

Enables the Label Distribution Protocol (LDP).

**Product**

- GGSN
- P-GW
- SAEGW

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > MPLS-IP Configuration > MPLS-LDP Configuration

```bash
configure > context context_name > mpls-ip > protocol ldp
```

Entering the above command sequence results in the following prompt:

```
[context_name] host_name(config-ldp)#
```

**Syntax**

```
[ no ] enable
```

- **no**
  
  Disables the LDP protocol.

**Usage**

This command is used to enable or disable the LDP protocol. By default the LDP protocol is disabled.

**Example**

Use the following command to enable the LDP protocol:

```
enable
```
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Use this command to return to the parent configuration mode.
**router-id**

Configures the Label Distribution Protocol Router ID.

**Product**
GGSN
P-GW
SAEGW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > MPLS-IP Configuration > MPLS-LDP Configuration

```
configure > context context_name > mpls-ip > protocol ldp
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-idp)#
```

**Syntax**

```
router-id ipv4_addr
no router-id
```

- **no**
  - Disables the router ID.

- **ipv4_addr**
  - Must be an IPv4 address entered in dotted-decimal notation.

**Usage**

This command is used to configure the LDP router-id. This is an optional parameter. If the ID is not configured, the largest operational loopback address is selected as the LDP router ID. If LDP has started, any change will take effect only after disabling and enabling LDP.

**Example**

The following command sequence configures an LDP router ID:

```
router-id 10.2.3.4
```
### session

Configures the LDP session parameters.

#### Product
- GGSN
- P-GW
- SAEGW

#### Privilege
- Security Administrator, Administrator

#### Mode
**Exec > Global Configuration > Context Configuration > MPLS-IP Configuration > MPLS-LDP Configuration**

```bash
configure > context context_name > mpls-ip > protocol ldp
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ldp)#
```

#### Syntax

```text
session timers { hold-interval integer_value | keepalive-interval integer_value }
```

```text
default session timers
```

- **default**
  
  Configures the default values for hold-interval parameter at 45 and keepalive-interval parameter at 15.

- **timers**
  
  Configures the LDP session keepalive parameters.

  ```text
  hold-interval integer_value
  ```

  Configures the session hold time interval in seconds.  
  `integer_value` is an integer from 45 through 65535.  
  Default: 45

  ```text
  keepalive-interval integer_value
  ```

  Configures the frequency of sending keepalive packets in seconds.  
  `integer_value` is an integer from 15 through 21845.  
  Default: 15

#### Usage

This optional command is used to configure LDP session timers. LDP session hold-interval is always set to three times the LDP session keepalive-interval. The “default” option sets the session keepalive and hold intervals to the default values.

#### Example

The following command sequence configures the LDP session parameters:
session timers keepalive-interval 30
session timers hold-interval 45
default session timers
Chapter 221
MRME Service Configuration Mode Commands

The MRME Service Configuration Mode provides commands to enable a trusted WLAN network to provide access to the Evolved Packet Core (EPC) using a AAA peer functionality.

Exec > Global Configuration > Context Configuration > MRME Service Configuration
configure > context context_name > mrme-service mrme_service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-mrme-service)#

Important: Available commands or keywords/variables vary based on platform type, product version, and installed license(s).
attribute

This command allows you to include SSID and Calling-Station-Id AVP values as part of DER messages over STa Interfaces.

Product
SaMOG

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > MRME Service Configuration

configure > context context_name > mrme-service mrme_service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-mrme-service)#

Syntax

attribute sta { anid { ssid | ssid-wlan-prefix | wlan-string } | calling-station-id { imsi | ue-mac } }

default attribute sta { anid | calling-station-id }

default

Sets the configuration to its default value.

Default calling-station-id: imsi
Default anid: wlan-string

anid { ssid | ssid-wlan-prefix | wlan-string }

Specifies to include the information from the ANID AVP in the DER message.

ssid: Include the SSID information from the ANID AVP.
ssid-wlan-prefix: Include the SSID WLAN prefix information from the ANID AVP.
wlan-string: Include the WLAN string information from the ANID AVP.

calling-station-id { imsi | ue-mac }

Specifies to include the calling station ID in the DER message.

imsi: Include the IMSI information.
ue-mac: Include the UE MAC information.

Usage

Use this command to include the received SSID and Calling-StationId-Id values in the ANID/Calling-StationId-Id AVP as part of DER messages over STa Interfaces.

Example

The following command includes ue-mac information from the calling-station-id in the DER message.

attribute sta calling-station-id ue-mac
bind

This command allows you to configure an IPv4 address to be used as the connection point for establishing SAMOG sessions for handling authentication and accounting messages.

**Product**
SaMOG

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > MRME Service Configuration
configure > context context_name > mrme-service mrme_service_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-mrme-service)#
```

**Syntax**

```
bind address ipv4_address [ auth-port auth_port_number ] [ acct-port acct_port_number ] [ max-subscribers max_subscriber_number ]
```

**no bind**

```
no
```

Removes a previously configured binding.

```
address ipv4_address
```

**Important:** Currently, MRME supports IPv4 address only.

Specifies the IP address of an interface to be used as the connection point for establishing SAMOG sessions. `ipv4_address` must be an IPv4 address expressed in dotted-decimal notation.

**Important:** To define more than one NAS IP address per context, in Global Configuration Mode use the `aaa large-configuration` command.

```
auth-port auth_port_number
```

Specifies the authentication port number of the interface where authentication requests are received. The system binds the default authentication port to 1812. In addition to the authentication port, the accounting port and maximum subscriber limit can also be configured optionally. `auth_port_number` must be an integer from 1 through 65535.

```
acct-port acct_port_number
```

Specified the accounting port number of the interface where accounting requests are received. The system binds the default accounting port to 1813.
In addition to the accounting port, the maximum subscriber limit can also be configured optionally. 
acct_port_number must be an integer from 1 through 65535.

max-subscribers max_subscriber_number

Specifies the maximum number of subscriber sessions allowed.
max_subscriber_number must be an integer from 0 through 4,000,000.

Usage
Use this command to configure the IPv4 address to be used as the connection point for establishing SAMOG sessions for handling authentication and accounting messages.

Example
The following command binds the service with an IP address of 196.10.2.3 with a accounting port number of 58 and maximum subscriber limit of 1000.

bind address 196.10.2.3 acct-port 58 max-subscribers 1000
**disconnect**

This command allows you to specify the delay duration before which the call is disconnected.

**Product**
SaMOG

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > MRME Service Configuration

```
configure > context context_name > mrme-service mrme_service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-mrme-service)#
```

**Syntax**

```
disconnect { delay-time seconds | wait-time seconds }

[ default ] disconnect { delay-time | wait-time }
```

**default**

Configures this command to its default setting.

- **delay-time** default: 30 seconds
- **wait-time** default: 10 seconds

**delay-time seconds**

Specifies to configure the timer to retain the session on receiving an Accounting Stop, and for roaming scenarios, session continuity on receiving an Accounting Start.

`seconds` must be an integer from 1 through 60.

**wait-time seconds**

Specifies to configure the timer to wait for accounting start message from the new WLC after processing the accounting stop message from the old WLC.

`seconds` must be an integer of 10 through 300.

**Usage**

Specifies to configure the timer to wait for accounting stop message after triggering a Disconnect Req Message to WLC for an SAMOG session.

**Example**

The following command sets the disconnect wait time to 60 seconds.

```
disconnect wait-time 60
```
dns-pgw

This command allows you to configure the source context in which the DNS client is configured, or enable/disable PGW selection based on topology and load-balancing of PGWs, based on weights from DNS.

**Product**
SaMOG

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > MRME Service Configuration
configure > context context_name > mrme-service mrme_service_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-mrme-service)#
```

**Syntax**

```
dns-pgw { context context_name | selection { topology [ weight ] | weight } } { default | no } dns-pgw { context | selection { topology [ weight ] | weight } }
```

- **default**
  Returns the command to its default value.
  - **default dns-pgw context**: MRME will fetch the dns-client configuration from the current context.
  - **default dns-pgw selection topology**: MRME will perform PGW selection based on the topology.

- **no**
  If previously configured, deletes the dns-pgw configuration.

- **context context_name**
  Specifies to configure the source context in which the DNS client is configured.
  - **context_name** must be an alphanumeric string of 1 through 79 characters.

- **selection { topology [ weight ] | weight }**
  Specifies to enable/disable PGW selection based on topology and load-balancing of PGWs based on weights from DNS.

**Usage**

Use this command to configure the source context in which the DNS client is configured, or enable/disable PGW selection based on topology and load-balancing of PGWs, based on weights from DNS.

In case of topology-based selection, when the DNS procedure outputs a list of PGW hostnames for the APN FQDN, MRME performs the longest suffix match and selects the PGW which is topologically closest to the MRME/subscriber. In case of weight-based selection, if there are multiple entries with the same priority in the list of PGW hostnames for the APN FQDN in the output from the DNS procedure, calls are distributed to...
the PGWs according to the weight field in RRs. The weight field specifies a relative weight for entries with the same priority.

**Example**

This command will configure the source context in which the DNS client is configured to “mrmectx”.

```
dns-pgw context mrmectx
```
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**

Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Use this command to return to the parent configuration mode.
**fqdn**

This command allows you to configure the MRME fully qualified domain name (FQDN) to match the longest suffix during dynamic allocation.

**Product**
SaMOG

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > MRME Service Configuration

configure > context context_name > mrme-service mrme_service_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-mrme-service)#
```

**Syntax**

```
fqdn fqdn_name

{ default | no } fqdn
```

- **default**
  Returns the command to the default setting of “null”.

- **no**
  Removes the configured FQDN from the MRME service configuration.

- **fqdn_name**
  Specifies the MRME FQDN name that will be used for the longest suffix match during dynamic allocation. `fqdn_name` must be an alphanumeric string of 1 to 255 characters.

**Usage**

Use this command to configure the MRME FQDN under MRME service to match the longest suffix during dynamic allocation.

**Example**

The following command sets an MRME FQDN value of “topon.eth.mrme.north.blore.3gppnetwork.org”.

```
fqdn topon.eth.mrme.north.blore.3gppnetwork.org
```
radius

This command allows you to specify the IP address and shared secret of the RADIUS accounting and authentication client from which RADIUS accounting and authentication requests are received.

Product
SaMOG

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > MRME Service Configuration

configure > context context_name > mrme-service mrme_service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-mrme-service)#

Syntax

radius client ipv4_address[/mask] { [ encrypted ] key key [ [ disconnect-message [ dest-port port_number ] ] ] [ acct-onoff { [ aaa-context aaa_context_name ] [ aaa-group aaa_group_name ] [ clear-sessions ] } ] } }

no radius client ipv4_address[/mask]

no
Removes a previously coonfigured RADIUS client.

ipv4_address[/mask]

Specifies the IP address, and optional subnet mask of the RADIUS client from which RADIUS accounting and authentication requests are received.

ipv4_address[/mask] must be an IPv4 address expressed in dotted-decimal notation.

[ encrypted ] key key

•encrypted: Specifies that the shared key between the RADIUS client and this service is encrypted.

•key key: Specifies the shared key between the RADIUS client and this service.

key with encryption must be an alphanumeric string of 1 through 288 characters, and without encryption an alphanumeric string of 1 through 127 characters. Note that key is case sensitive.

disconnect-message [ dest-port port_number ]

Specifies to send RADIUS disconnect messages to the configured RADIUS accounting client in call failure scenarios.

•dest-port port_number: Specifies a port number to which the disconnect message must be sent.

port_number must be an integer from 1 through 65535.
MRME Service Configuration Mode Commands

radius

acct-onoff { [ aaa-context context_name ] [ aaa-group group_name ] [ clear-sessions ] }

**Important:** The acct-onoff keyword is currently not supported in this release.

**Usage**

Use this command to specify the IP address and shared secret of the RADIUS accounting and authentication client from which RADIUS accounting and authentication requests are received.

**Example**

The following command configures the service to communicate with a RADIUS client with an IP address of 190.21.33.40 and an encrypted shared secret of key1234Ax3Z, and clear the session when accounting on/off messages are received:

```
radius client 190.21.33.40 encrypted key 123 4Ax3Z acct-onoff clear-sessions
```
setup-timeout

This command is currently not supported in this release.
Chapter 222
Network Service Entity - Peer NSEI Configuration Mode Commands

The Network Service Entity (NSE) - Peer NSEI configuration mode configures the Frame Relay parameters for the peer NSE. This mode is a sub-mode of the Global Configuration mode. This sub-mode provides the commands and parameters to define the management functionality for the Gb interface between a BSS and an SGSN over a 2.5G GPRS Frame Relay network connection.

Mode

Exec > Global Configuration > Network Service Entity - Frame Relay Peer NSEI Configuration

configure > network-service-entity peer-nsei nsei_number frame-relay

Entering the above command sequence results in the following prompt:

[local]host_name(nse-fr-peer-nsei-nse_id)#

⚠️ Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
bssgp-timer

This command has been deprecated.
Exits the current configuration mode and returns to the Exec mode.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**
```
end
```

**Usage**
Return to the Exec mode.
exit

Exits the current configuration mode and returns to the previous configuration mode.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**
exit

**Usage**
Return to the global configuration mode.
ns-reset-mode

The command configures automatic NS-Reset for a specific Frame Relay peer NSE (network service entity).

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Network Service Entity - Frame Relay Peer NSEI Configuration

`configure > network-service-entity peer-nsei nsei_number frame-relay`

Entering the above command sequence results in the following prompt:

```
[local]host_name(nse-fr-peer-nsei-nse_id)#
```

**Syntax**

```
ns-reset-mode { active | passive }
```

**default ns-reset-mode**

```
default
 Resets the configuration to the passive mode.

active
Configures active mode so that the SGSN is enabled to initiate NS-Reset without manual intervention.

passive
Configures passive mode which means the SGSN continues *not* to initiate NS-Reset. This is the default mode.
```

**Usage**

Use this command to configure the SGSN for active mode regarding the peer NSE, so that the SGSN will initiate:
- NS-Reset when NSVC-DLCI binding is done.
- NS-Reset when the link goes down and then comes back.
- NS-Unblock upon receipt of NS-Reset-Ack message.

Active mode is useful in the following scenarios:
- if the SGSN detects LMI down but the BSC does not detect any link failure so does not send NS-Reset.
- if the NS layer can go down and the SGSN will mark the link as ‘Blocked-Dead’. If the link comes up later, the NS layer state for that link will remain in the Blocked state.

**Example**

Configure active mode to perform NS-Reset when the link goes down and comes back up:
ns-reset-mode active
**NS-VC**

This command creates a network service virtual circuit (NSVC) for this frame relay NSE and enters the configuration sub-mode to define the NSVC parameters. These parameters are described in the NSVC Configuration Mode chapter elsewhere in this CLI Reference Guide.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Network Service Entity - Frame Relay Peer NSEI Configuration

**Syntax**

```
[ no ] ns-vc id ns-vc_id
```

- **no**
  - Removes the specified NSVC configuration.

- **id ns-vc_id**
  - This keyword defines the NSVC configuration identifier.
  - `ns-vc_id`: Must be an integer from 0 to 65535

**Usage**
Access the NSVC configuration mode.

**Example**

Gain access to the NSVC configuration mode to change the 4th instance.

```
ns-vc id 4
```
Chapter 223
Network Service Entity- IP Local Configuration Mode Commands

The Network Service Entity (NSE) - IP Local configuration mode is a sub-mode of the Global Configuration mode. This sub-mode configures the local endpoint for NS/IP with the commands and parameters to define the management functionality for the Gb interface between a BSS and an SGSN over a 2.5G GPRS IP network connection.

Mode
Exec > Global Configuration > Network Service Entity - IP Configuration
configure > network-service-entity ip-local

Entering the above command sequence results in the following prompt:

[local]host_name(nse-ip-local)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
**all-nsvc-failure-action**

Configure how the SGSN handles the NSE when all NSVCs go down.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Network Service Entity - IP Configuration

```
configure > network-service-entity ip-local
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(nse-ip-local)#
```

**Syntax**

```
all-nsvc-failure-action clear-nse
```

```
default all-nsvc-failure-action
```

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>By default, the NSE is not cleared if all NSVCs go down.</td>
</tr>
<tr>
<td>clear-nse</td>
<td>Instructs the SGSN to SGSN to clear NSEs if all NSVCs to the BSC are down. This CLI clears the info only in cases where all the NSVC of NSE go down due to ALIVE time out.</td>
</tr>
</tbody>
</table>

**Usage**

Enable the SGSN to clear NSE information when all NSVCs go down.

**Example**

Use the following command to configure the SGSN to clear NSEs when all NSVCs go down.

```
all-nsvc-failure-action clear-nse
```
associate

This command supports the association of DSCP template at network-service-entity ip local level.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Network Service Entity - IP Configuration
configure > network-service-entity ip-local

Enter the above command sequence results in the following prompt:

[local]host_name(nse-ip-local)#

Syntax

associate dscp-template downlink [<template-name>]

no associate dscp-template downlink

Syntax

no

Removes the associate services needed for all IP nses.

dscp-template

Configures DCSP for all IP nses.

downlink [<template-name>]

Specifies the DSCP template used for the downlink packets.

Usage

Configuring this command allows the SGSN to send the configured DSCP value to:

- All the GPRS nodal messages.
- All the subscriber specific messages, when dscp template association at gprs-service level and nsei level are absent.

The DSCP template can be defined in sgsn global.

By default, SGSN will apply best effort DSCP value (that is, “0”).

Note:

- Atleast one nsvl should be configured, before configuring the DSCP marking at “network-service-entity ip-local” level.
- After the removal of last nsvl, DSCP template association is removed from “network-service-entity ip-local”.

Example
associate

The following example associates a DSCP template at network-service-entity ip local level.

```
associate dscp-template downlink  DSCP
```
bssgp-timer

This command has been deprecated.
end

Exits the current configuration mode and returns to the Exec mode.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Return to the Exec mode.
exit

Exits the current configuration mode and returns to the global configuration mode.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Returns to the global configuration mode.
max-ns-retransmissions

This command configures the maximum number of transmission retries counter.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Network Service Entity - IP Configuration
`configure > network-service-entity ip-local`
Entering the above command sequence results in the following prompt:
`[local]host_name(nse-ip-local)#`

**Syntax**
```plaintext
[ default ] max-ns-retransmissions { alive count | sns-proc count }
```

- **default**
  Resets the specified counter configuration to the default value.

- **alive count**
  Sets the maximum number of alive retries.
  `count`: Must be an integer between 0 and 10. Default is 3.

- **sns-proc count**
  Sets the maximum number of retries for the SNS procedure
  `count`: Must be an integer between 0 and 5. Default is 3.

**Usage**
Sets the maximum for NS transmission retries.

**Example**
```
max-ns-retransmission alive 4
```
**ns-timer**

This command sets the network service (NS) counters for the SNS procedure and testing.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Network Service Entity - IP Configuration  
`configure > network-service-entity ip-local`

Entering the above command sequence results in the following prompt:

```
[local] host_name(nse-ip-local)#
```

**Syntax**

```
ns-timer { sns-guard timeout_val | sns-prov timeout_val | test timeout_val }

default ns-timer { sns-guard | sns-prov | test }
```

---

**default**

Resets the selected timer configuration to its default value.

---

**sns-guard timeout_val**

Sets the SNS-guard timer which is used in the auto-learn procedure to clean-up learnt BSC/NSE information.  
`timeout_val`: Enter an integer from 1 to 300. Default is 60.

---

**sns-prov timeout_val**

Sets the SNS procedure timeout value in seconds.  
`timeout_val`: Enter an integer from 1 to 10. Default is 5.

---

**test timeout_val**

Sets the test procedure timeout value in seconds.  
`timeout_val`: Enter an integer from 1 to 60. Default is 30 seconds.

---

**Usage**

Set NS timers to help manage the NSE-IP connection.

---

**Example**

The following example sets the test timer to 4 seconds:

```
ns-timer test 4
```
**nsvc-failure-action**

This command enables and disables the sending of an NS-STATUS message with cause ‘ip-test fail’ when NSVC goes down.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Network Service Entity - IP Configuration

```configure > network-service-entity ip-local```

Entering the above command sequence results in the following prompt:

```
[local] host_name(nse-ip-local)#
```

**Syntax**

```nsvc-failure-action send-ns-status```

```default nsvc-failure-action```

```default```
Sets the command configuration to its default value. The default action is not to send an NS-STATUS message. This is applicable only to NSVCs that are auto-learned and not configured.

```send-ns-status```
Enables the sending of the NS-STATUS message.

**Usage**

Use this command to enable or disable sending an NS-STATUS messages when an NSVC goes down.

**Example**

Enable sending of the message:

```nsvc-failure-action send-ns-status```
nsvl

This command creates and instance of a network service virtual link (NSVL) and enters the NSVL configuration mode.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Network Service Entity - IP Configuration
configure > network-service-entity ip-local

Entering the above command sequence results in the following prompt:

[local]host_name(nse-ip-local)#

Syntax

[ no ] nsvl instance nsvl_id

no
Removes the identified NSVL definition from the configuration.

instance nsvl_id
Identifies a specific NSVL configuration instance.
nsvl_id: Must be an integer from 0 to 3.

Usage
Access the NSVL configuration mode.

Example
Enter the NSVL configuration sub-mode to modify the configuration for NSVL instance 2:

nsvl instance 2
peer-network-service-entity

This command has been replaced by the Network Service Entity - Peer NSEI Frame Relay configuration mode.
retry-count

This command has been replaced by the `max-ns-retransmissions` command.
timer

This command has been replaced by the ns-timer command.
Chapter 224
Network Service Virtual Connection Configuration Mode Commands

The Network Service Virtual Connection (NSVC) configuration mode is a sub-mode of the Network Service Entity (NSE) - Peer NSEI (for Frame Relay) configuration mode. The NSVC sub-mode creates a configuration instance for a specific NSVC, within the Gb interface, between a BSS and an SGSN in a 2.5G GPRSFrame Relay network connection.

Exec > Global Configuration > Network Service Entity - Frame Relay Peer NSEI Configuration > NSVC Configuration

configure > network-service-entity peer-nsei peer_nsei framerelay > ns-vc nsvc_id

Entering the above command sequence results in the following prompt:

[local] host_name(nse-fr-peer-nsei-nse_id-nsvci-nsvc_instance)#

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
end

Exits the current configuration mode and returns to the Exec mode.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Return to the Exec mode.
exit

Exits the current configuration mode and returns to the previous configuration mode.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Returns to the network service entity - frame relay configuration mode.
Chapter 225  
Network Service Virtual Link Configuration Mode Commands

The Network Service Virtual Link configuration mode is a sub-mode of the Network Service Entity - IP configuration mode. This sub-mode provides the commands and parameters to define the NSVL of the Gb interface between a BSS and an SGSN in a 2.5G GPRS IP network connection.

**Mode**

Exec > Global Configuration > Network Service Entity - IP Configuration > NSVL Configuration  
`configure > network-service-entity ip > nsvl instance nsvl_id`

Entering the above command sequence results in the following prompt:

```
[local]host_name(nse-ip-local-nsvl-nsvl_instance)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**
```
end
```

**Usage**
Return to the Exec mode.
exit

Exits the current configuration mode and returns to the previous configuration mode.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**
Return to the network service entity - IP configuration mode.
nsvl-address

This command configures the IP address of the NSVL end-point.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Network Service Entity - IP Configuration > NSVL Configuration

configure > network-service-entity ip > nsvl instance nsvl_id

Entering the above command sequence results in the following prompt:

[local]host_name(nse-ip-local-nsvl-nsvl_instance)#

Syntax

nsvl-address ip-address ip_address context ctxt_name port port_num

| ip-address | ip_address | Identifies the address of the NSVL.
| context | ctxt_name | Must be specified using the standard IPv4 dotted decimal notation or colon notation for IPv6.
| port | port_num | Identifies the specific context associated with this NSVL address.
| port_num | Must be an integer from 1 to 65535.
| | | Specifies the UDP port to associate with the NSVL end-point.

Usage
Use this command to configure the IP address, context name and port number for the NSVL end-point.

Example

nsvl-address ip-address 1.1.1.1 context sgsn2 port 3735
weight

This command configures the signaling or data weight for NSVL.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Network Service Entity - IP Configuration > NSVL Configuration

configure > network-service-entity ip > nsvl instance nsvl_id

Entering the above command sequence results in the following prompt:

[local]host_name(nse-ip-local-nsvl-nsvl_instance)#

Syntax

weight { data data_weight | signaling signaling_weight }

---

data data_weight

Defines the data weight for the NSVL.

data_weight: Must be an integer from 0 to 255. Default is 1.

---

signaling signaling_weight

Defines the signaling weight for the NSVL.

signaling_weight: Must be an integer from 0 to 255. Default is 1.

---

Usage

Configure the weight of the signaling or data for the NSVL.

Example

weight data 234
Chapter 226
NTP Configuration Mode Commands

The NTP Configuration Mode is used to manage the Network Time Protocol (NTP) options for the entire system.

Mode

Exec > Global Configuration > NTP Configuration
configure > ntp

Entering the above command sequence results in the following prompt:

[local]host_name(config-ntp) #

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
**enable**

Enables the use of the Network Time Protocol (NTP) for synchronizing the system clock. By default, NTP is not enabled externally and should be configured when the system is initially installed. When enabled, the active ASR 5000 SMC or ASR 5500 MIO will synchronize with external sources. If not enabled, the active SMC or MIO will use its local clock as a time source. In the event of an NTP server or network outage, an already running SMC or MIO will continue to use NTP to maintain time accuracy, but in a holdover mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > NTP Configuration

```bash
configure > ntp
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-ntp)#
```

**Syntax**

```bash
enable [ context ]
```

- **context**
  Default: local
  Specifies the context for which NTP is to be enabled as an alphanumeric string of 1 through 79 characters.

**Important:** NTP must be configured for use in the *local* context only. Use of other contexts will cause issues.

**Usage**

Sets the NTP server to be used for the system. Only one NTP server may be active at any given time.

The system uses NTP to synchronize internal clocks on the chassis to external time sources (typically GPS NTP sources, or other Stratum 2 or 3 servers, switches or routers).

All cards with CPUs synchronize to the active SMC or MIO internally. This occurs even if an external NTP server is not configured. In the event of a SMC or MIO switchover, all other cards will start synchronizing with the newly active SMC or MIO automatically.

If any NTP server is enabled, the chassis system clock will be synchronized to the active NTP server which covers all contexts for timing synchronization.

Refer to the *System Administration Guide* for additional information on configuring NTP.

**Example**

The following command enables use of NTP for the *local* context.

```bash
enable
```
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
exit

**Usage**
Use this command to return to the parent configuration mode.
server

Configures a Network Time Protocol (NTP) server for use by the local NTP client in synchronizing the system clock.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > NTP Configuration

configure > ntp

Entering the above command sequence results in the following prompt:

[local]host_name(config-ntp)#

Syntax

server ip_address [ prefer ] [ version number ] [ minpoll poll_period ] [ maxpoll poll_period ]

no server ip_address

no

Indicates the server specified is to be removed from the list of NTP servers for clock synchronization.

ip_address

Specifies the IP address of the NTP server to be used for clock synchronization in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

NTP should be configured for at least three external NTP servers. With three or more servers, outliers and broken or misconfigured servers can be detected and excluded. Generally, the more servers the better (within reason).

prefer

Indicates the NTP server specified to be the preferred server. Only one server can be set to preferred. The preferred server is the first one contacted for clock synchronization.

Important: Use of the prefer keyword is not recommended.

Important: Do not change the version, minpoll or maxpoll keyword settings unless instructed to do so by Cisco TAC.
version number

Specifies the network timing protocol version to use for server communications as an integer from 1 to 4. Default: 4 (RFC 5905)

minpoll poll_period

Specifies the minimum polling interval (in seconds) for NTP messages as a power of \(2^{\text{poll_period}}\) is the exponent (power of) expressed as an integer from 6 through 17. For example, if you specify the number 6, the value is \(2^6\) and the resultant poll period is 64 seconds. Default: 6

maxpoll poll_period

Specifies the maximum polling interval (in seconds) for NTP messages as a power of \(2^{\text{poll_period}}\) is the exponent (power of) expressed as an integer from 6 through 17. For example, if you specify the number 10, the value is \(2^{10}\) and the resultant poll period is 1024 seconds. Default: 10

Usage

Configure the NTP servers in response to network changes. Refer to the System Administration Guide for important information on configuring NTP servers with local sources, and using a load balancer to communicate with external NTP servers.

Important: Adding, removing, or modifying an NTP server configuration entry causes the NTP client to restart itself and resynchronize with all configured NTP servers.

Example

The following command adds the NTP server with address 10.2.3.4 to the list of NTP servers.

```
server 10.2.3.4
```
Chapter 227
Operator Policy Configuration Mode

Operator Policy configuration mode associates APNs, APN profiles, IMEI ranges, IMEI profiles, an APN remap table and a call control profile to an operator policy. These profiles and tables are created and defined within their own configuration modes to generate sets of rules and instructions that can be reused and assigned to multiple policies.

The Operator Policy Configuration Mode is used to create and manage operator policies for MME, S-GW, SAEGW, and SGSN configurations.

- A maximum of 1,000 operator policies can be defined, including the “default” operator policy.
- A maximum of 128 APN profiles can be associated with a single operator policy.
- A maximum of 128 IMEI profiles can be associated with a single operator policy (SGSN-only).
- Only one APN remap table can be associated with a single operator policy.
- Only one call control profile can be associated with a single operator policy.

Using the Operator Policy feature allows the operator to fine-tune any desired restrictions or limitations needed to control call handling per subscriber or for a group of callers across IMSI ranges.

**Mode**

```
Exec > Global Configuration > Operator Policy Configuration
configure > operator-policy policy_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-opr-policy-policy_name)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
**apn**

This command identifies an APN (access point name) and associates it with an APN profile (created separately in the APN Profile Configuration mode).

**Product**

MME
SAEGW
S-GW
SGSN

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Operator Policy Configuration

configure > operator-policy policy_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-opr-policy-policy_name)#

**Syntax**

apn { default-apn-profile apn_profile_name | network-identifier apn_net_id [ apn-profile apn_profile_name ] | operator-identifier apn_op_id apn-profile apn_profile_name }

no apn { default-apn-profile | network-identifier apn_net_id | operator-identifier apn_op_id }

no

Disables the specified APN to APN Profile correspondence.

**default-apn-profile apn_profile_name**

Enables the use of a default APN profile comprised of default values for all parameters. this profile will be used when none of the configured APNs match the APN in the incoming Request.

`apn_profile_name` must be an alphanumeric string of 1 through 64 characters.

**apn-profile apn_profile_name**

`apn_profile_name` must be an alphanumeric string of 1 through 64 characters.

**network-identifier apn_net_id**

Links the specified APN network ID with the specified APN profile.

`apn_net_id` must be an alphanumeric string of 1 through 63 characters, including dots (.) and dashes (-).

: MME or SGSN only. This optional keyword configures the MME or SGSN to apply congestion control actions for this specific APN. Refer to the `drop` and `reject` commands within the [SGSN] Congestion Action Profile Configuration Mode for more information on configuring APN-based congestion control.
operator-identifier apn_op_id

Links the specified APN operator ID with the specified APN profile.

`apn_op_id`: must be an alphanumeric string of 1 through 18 characters, including dots (.). The string must be in the following format, where # represents a digit: MNC###.MCC###.GPRS.

Usage

Use this command, to associate APNs with APN profiles. This command can be repeated to associate multiple APNs with profiles.

Example

Associate the APN profile named `apnprof1` to APN network ID `starflash.com`:

```
apn apnprof1 network-identifier starflash.com
```

Associate congestion control with APN network ID `starflash.com`:

```
apn network-identifier starflash.com congestion-control
```
associate

Associate an APN remap table and a call control profile with the operator policy.

Product

- MME
- SAEGW
- S-GW
- SGSN

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > Operator Policy Configuration

```
configure > operator-policy policy_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-opr-policy-policy_name)#
```

Syntax

```
associate { apn-remap-table table_id | call-control-profile profile_id }
```

```
no associate { apn-remap-table | call-control-profile }
```

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Removes the association definition from the policy configuration.</td>
</tr>
<tr>
<td>apn-remap-table table_id</td>
<td>Identifies the APN remap table to be associated with the operator policy. table_id must be an alphanumeric string of 1 through 65 characters.</td>
</tr>
<tr>
<td>call-control-profile profile_id</td>
<td>Identifies a call control profile to be associated with the operator policy. profile_id must be an alphanumeric string of 1 through 64 characters.</td>
</tr>
</tbody>
</table>

Usage

Use this command to associate an APN remap table and/or a call control profile with this Operator Policy. The APN remap table and the call control profile contain the definitions that instruct the SGSN or MME how to handle calls. Only one of each of these can be associated with an operator policy.

Example

Associate the stardust.net_APNremap1 APN remap table with this operator policy:

```
associate apn-remap-table stardust.net_APNremap1
```
description

Associates a description with or names an operator policy.

Product

MME
SAEGW
S-GW
SGSN

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > Operator Policy Configuration

configure > operator-policy policy_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-opr-policy-policy_name)#

Syntax

description description

no description

---

description

Enter an alphanumeric string of 1 through 100 characters. If the string includes spaces, punctuation, and case-sensitive letters, it must be bracketed with double quotation marks (“ “).

---

no

Removes the existing description from this operator policy.

Usage

Identity this particularly operator policy using descriptive text.

Example

description “sgsn1 operator policy carrier1”
end

Exits the current configuration mode and returns to the Exec mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**

Use this command to return to the Exec mode.
**exit**

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
```
exit
```

**Usage**
Use this command to return to the parent configuration mode.
**imei**

Defines a range of IMEI (International Mobile Equipment Identity) numbers and associates an IMEI profile with the range definition.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Operator Policy Configuration

```bash
configure > operator-policy policy_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-opr-policy-policy_name)#
```

**Syntax**

```bash
imei range IMEI_number to IMEI_number { imei-profile profile_name | sv ## imei-profile profile_name }
```

```bash
no imei range IMEI_number to IMEI_number sv ##
```

**no**

Removes the IMEI definition from the policy configuration.

```bash
range IMEI_number to IMEI_number
```

Defines the beginning and end of a range of IMEI numbers.

**IMEI_number** must be a numerical string of up to 14 digits.

```bash
sv ##
```

Identifies the software version to fine-tune the IMEI definition. This keyword should only be included if the IMEISV is retrievable.

**##** must be a 2-digit integer.

```bash
imei-profile profile_name
```

Identifies the IMEI profile that defines the actions appropriate to the devices identified within the specified range.

**profile_name** must be an alphanumeric string of 1 through 64 characters.

**Usage**

This command defines the IMEI ranges that will be used by the operator policy to determine if the device is appropriately selected for actions defined in the specified IMEI profile.

**Example**

All devices with an IMEI of 123123* requesting Attach shall be subject to actions in the blacklist_profile1.
imei range 1231230 to 1231239 imei-profile name blacklist_profile1
Chapter 228
ORBEM Configuration Mode Commands

The ORBEM Configuration Mode is used to manage the Object Request Broker Element Manager (ORBEM) server options for the current context.

Mode

Exec > Global Configuration > ORBEM Configuration

configure > orbem

Entering the above command sequence results in the following prompt:

[local]host_name(config-orbem)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
activate

Activates/deactivates a Common Object Request Broker Architecture (CORBA) client for the ORBEM interface.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > ORBEM Configuration

configure > orbem

Entering the above command sequence results in the following prompt:

[local]host_name(config-orbem)#

**Syntax**

```
active client id
no active client id
```

**Usage**

Indicates the client specified is to be deactivated. When omitted, the client is activated.

```
no
```

Specifies the client to be activated. *name* must refer to a previously configured client expressed as an alphanumeric string of 1 through 10 characters.

```
id name
```

**Example**

Activates CORBA clients after they have been configured or deactivated by the system or by configuration.

```
active client wem
no active client wem
```
client

Configures/removes a CORBA client from the ORB element manager system interface.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > ORBEM Configuration

configure > orbem

Entering the above command sequence results in the following prompt:

[local]host_name(config-orbem)#

Syntax

client id name [ encrypted ] password pwd

no client id name

no
Indicates the client specified is to be removed from the configuration.

id name
Specifies the client to be configured. *name* must be an alphanumeric string of 1 through 10 characters.

encrypted
Indicates password specified is encrypted.
The *encrypted* keyword is intended only for use by the chassis while saving configuration scripts. The system displays the *encrypted* keyword in the configuration file as a flag that the variable following the *password* keyword is the encrypted version of the plain text password. Only the encrypted password is saved as part of the configuration file.

password pwd
Specifies the password for the CORBA client. *pwd* must be an alphanumeric string of 1 through 35 characters.

Usage
ORBEM clients must be configured prior to being activated.

Example
The following commands set the password for client *wem* specifying a plain text password and an encrypted password as well.

    client id wem password wem1001
    client id wem encrypted password f54gj801sd
The following deletes `wem` from the configuration.

```
no client id wem
```
default

Restores the system default values for the option specified.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > ORBEM Configuration
configure > orbem

Entering the above command sequence results in the following prompt:

[local]host_name(config-ormb)#

Syntax

default { event-notif-iop-port | event-notif-service filter | event-notif-siop-port | iop-port | iop-address | max-attempt | session-timeout | siop-port }

event-notif-iop-port
Restores the port number for the inter-ORB event notifications to the system default: 7778.

event-notif-service filter
Restores the ORB Notification Service filter to its default behavior of sending all “error” level and higher events, and “info” level events for the orbs facility, CLI command logs, and license change logs.

event-notif-siop-port
Restores the port to use for secure socket layer inter-ORB event communication to the system default: 7777.

iop-port
Restores the port number for inter-ORB communications to the system default: 14132.

iop-address
Restores the IP address for inter-ORB communications to the system default: IP address of current context.

max-attempt
Restores the maximum number of failed login attempts before which the client is deactivated to the system default: 3 attempts.

session-timeout
Restores the amount of idle time (no activity) before a session is terminated to the system default: 300 seconds.
**siop-port**

Restores the secure socket layer I/O port for inter-ORB events to the system default: 14131.

**Usage**

Restore the ORB element manager options to a well known values, the system defaults.

**Example**

```
default event-notif-iiop-port

default max-attempt
```
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
event-notif-iiop-port

Configures the port number for Internet inter-ORB event notifications.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > ORBEM Configuration
    configure > orbem
Entering the above command sequence results in the following prompt:

[local]host_name(config-orbem)#

Syntax

```
event-notif-iiop-port number
```

number
Default: 7778
Specifies the port number to use as an integer from 1 through 65535.

Usage
Explicitly set the port number when the default port number is not the desired port value for integrating multiple products together for standardized inter-ORB communications.
Event notification port configured is only used if the Internet inter-ORB transport is enabled via the iiop-transport command with the event notification service being enabled as well.

Example

```
event-notif-iiop-port 25466
```
**event-notif-service**

Enables or disables the ORB Notification Service and allows the configuration of filters dictating which event notifications are sent.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > ORBEM Configuration
configure > orbem

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-orbem)#
```

**Syntax**

```
[ no ] event-notif-service [ filter { event-id event_id [ to final_event_id ] | facility event_facility level event_level } ]
```

- **no**
  - Disables the event notification service.

- **filter**
  - Specifies a filter that determines for which events the system sends notifications.

  ```
event-id  event_id [ to final_event_id ]
```

  - Specifies an event filter based on event identification (event ID) number.
  - `event_id` is a specific event ID to filter or is the initial event ID in range if the `to` keyword is used.
  - In 14.1 and earlier releases, `event_id` is an integer from 1 through 202699.
  - In 15.0 and later releases, `event_id` is an integer from 1 through 204999.
  - `to` allows the specification of a range of event IDs to filter. When used, `final_event_id` specifies the last event ID in the range to be filtered. It can be configured to an integer from 1 through 204999, but must be a value greater than the initial event ID.

- **facility**
  - Specifies an event filter based on facility type and notification severity level.
  - `event_facility` specifies the facility type and can be any one of the following:
    - `a10`: A10 interface facility
    - `a11`: A11 interface facility
    - `a11mgr`: A11 Manager facility
    - `aaa-client`: Authentication, Authorization and Accounting (AAA) client facility
    - `aaamgr`: AAA manager logging facility
    - `aaaproxy`: AAA Proxy facility
• **aal2**: ATM Adaptation Layer 2 (AAL2) protocol logging facility
• **acl-log**: Access Control List (ACL) logging facility
• **acsctrl**: Active Charging Service (ACS) Controller facility
• **acsmgr**: ACS Manager facility
• **afctrl**: Fabric Controller facility [ASR 5500 only]
• **afmgr**: Fabric Manager logging facility [ASR 5500 only]
• **alarmctrl**: Alarm Controller facility
• **alcap**: Access Link Control Application Part (ALCAP) protocol logging facility
• **alcapmgr**: ALCAP manager logging facility
• **all**: All facilities
• **asngwmgr**: Access Service Network (ASN) Gateway Manager facility
• **asnpcmgr**: ASN Paging Controller Manager facility
• **bfd**: Bidirectional Forwarding Detection (BFD) protocol logging facility
• **bgp**: Border Gateway Protocol (BGP) facility
• **bindmux**: IPCF BindMux-Demux Manager logging facility
• **bngmgr**: Broadband Network Gateway (BNG) Demux Manager logging facility
• **bssap+**: Base Station Sub-system Application Part+ protocol facility for the login interface between the SGSN and the MSC/VLR (2.5G and 3G)
• **bssgp**: Base Station Sub-system GPRS Protocol logging facility handles exchange information between the SGSN and the BSS (2.5G only)
• **callhome**: Call Home application logging facility
• **cap**: CAMEL Application Part (CAP) logging facility for protocol used in prepaid applications (2.5G and 3G)
• **cbsmgr**: Cell Broadcasting Service (CBS) logging facility [HNBGW]
• **cdf**: Charging Data Function (CDF) logging facility
• **cgw**: Converged Access Gateway (CGW) logging facility
• **cli**: Command Line Interface (CLI) logging facility
• **cmp**: Certificate Management Protocol (IPSec) logging facility
• **connectedapps**: SecGW ASR 9000 oneP communication protocol
• **connproxy**: Controller Proxy logging facility
• **credit-control**: Credit Control (CC) facility
• **cscf**: IMS/MMD Call Session Control Function (CSCF)
• **cscfcpgmgr**: CSCFCPGRMGR logging facility
• **cscfmgr**: SIP CSCF Manager facility
• **cscfnpdb**: CSCF Number Portability Database (NPDB) logging facility
• **cscfrtcp**: IMS/MMD CSCF RTCP log facility
• **cscfrtp**: IMS/MMD CSCF RTP log facility
• **cscfttmgr**: SIP CSCF Tunnel and Transport Manager facility
• **csp**: Card/Slot/Port controller facility
• **css**: Content Service Selection (CSS) facility
• **css-sig**: CSS RADIUS Signaling facility
• **cx-diameter**: Cx Diameter Messages facility [CSCF <--> HSS]
• **dcardctr**: IPSec Daughter Card Controller logging facility
• **dcardmgr**: IPSec Daughter Card Manager logging facility
• **demuxmgr**: Demux Manager API facility
• **dgmbmgr**: Diameter Gmb Application Manager logging facility
• **dhcp**: Dynamic Host Configuration Protocol (DHCP) logging facility
• **dhcpv6**: DHCPv6
• **dhost**: Distributed Host logging facility
• **diabase**: Diabase messages facility
• **diameter**: Diameter endpoint logging facility
• **diameter-acct**: Diameter Accounting
• **diameter-auth**: Diameter Authentication
• **diameter-dns**: Diameter DNS subsystem
• **diameter-eecs**: ACS Diameter signaling facility
• **diameter-hdd**: Diameter Horizontal Directional Drilling (HDD) Interface facility
• **diameter-svc**: Diameter Service
• **diamproxy**: DiamProxy logging facility
• **dpath**: IPSec Data Path facility
• **drvctr**: Driver Controller facility
• **doulosuemgr**: Doulos (IMS-IPSec-Tool) user equipment manager
• **eap-diameter**: Extensible Authentication Protocol (EAP) IP Security facility
• **eap-ipsec**: Extensible Authentication Protocol (EAP) IPSec facility
• **eap-sta-s6a-s13-s6b-diameter**: EAP/STA/S6A/S13/S6B Diameter messages facility
• **ecs-css**: ACSMGR <--> Session Manager Signalling Interface facility
• **egtpc**: eGTP-C logging facility
• **egtpmgr**: enhanced GPRS Tunneling Protocol (eGTP) manager logging facility
• **egtpu**: eGTP-U logging facility
• **epdg**: evolved Packet Data (ePDG) gateway logging facility
• **event-notif**: Event Notification Interface logging facility
• **evlog**: Event log facility
• **famgr**: Foreign Agent manager logging facility
• **firewall**: Firewall logging facility
• **fng**: Femto Network Gateway (FNG) logging facility
• **gbmgr**: SGSN Gb Interface Manager facility
• **gmm:**
  • For 2.5G: Logs the GPRS Mobility Management (GMM) layer (above LLC layer)
  • For 3G: Logs the access application layer (above the RANAP layer)

• **gprs-app**: GPRS Application logging facility

• **gprs/ns**: GPRS Network Service Protocol (layer between SGSN and the BSS) logging facility

• **gq-rx-tx-diameter**: Gq/Rx/Tx Diameter messages facility

• **gss-gcdr**: GTPP Storage Server GCDR facility

• **gtp**: GTP-C protocol logging facility

• **gtpcmgr**: GTP-C protocol manager logging facility

• **gtp**: GTP-prime protocol logging facility

• **gtpu**: GTP-U protocol logging facility

• **gtpumgr**: GTP-U Demux manager

• **gx-ty-diameter**: Gx/Ty Diameter messages facility

• **gy-diameter**: Gy Diameter messages facility

• **h248prt**: H.248 port manager facility

• **hamgr**: Home Agent manager logging facility

• **hat**: High Availability Task (HAT) process facility

• **hdctrl**: HD Controller logging facility

• **henbapp**: Home Evolved NodeB (HENB) App facility

• **henbgw**: HENB-GW facility

• **henbgw-pws**: HENB-GW Public Warning System logging facility

• **henbgw-sctp-acs**: HENB-GW access Stream Control Transmission Protocol (SCTP) facility

• **henbgw-sctp-nw**: HENBGW network SCTP facility

• **henbgwdemux**: HENB-GW Demux facility

• **henbgwmgr**: HENB-GW Manager facility

• **hnb-gw**: HNB-GW (3G Femto GW) logging facility

• **hnbmgr**: HNB-GW Demux Manager logging facility

• **hss-peer-service**: Home Subscriber Server (HSS) Peer Service facility

• **igmp**: Internet Group Management Protocol (IGMP)

• **ikev2**: Internet Key Exchange version 2 (IKEv2)

• **ims-authorizatn**: IP Multimedia Subsystem (IMS) Authorization Service facility

• **ims-sh**: HSS Diameter Sh Interface Service facility

• **imsimgr**: SGSN IMSI Manager facility

• **imsue**: IMS User Equipment (IMSUE) facility

• **ip-arp**: IP Address Resolution Protocol facility

• **ip-interface**: IP interface facility

• **ip-route**: IP route facility
• **ipms**: Intelligent Packet Monitoring System (IPMS) logging facility
• **ipne**: IP Network Enabler (IPNE) facility
• **ipsec**: IP Security logging facility
• **ipsg**: IP Service Gateway interface logging facility
• **ipsmgrr**: IP Services Gateway facility
• **ipsp**: IP Pool Sharing Protocol logging facility
• **kvstore**: Key/Value Store (KVSTORE) Store facility
• **l2tp-control**: Layer 2 Tunneling Precool (L2TP) control logging facility
• **l2tp-data**: L2TP data logging facility
• **l2tpdemux**: L2TP Demux Manager logging facility
• **l2tpmgr**: L2TP Manager logging facility
• **lagmgr**: Link Aggregation Group (LAG) manager logging facility
• **lcs**: Location Services (LCS) logging facility
• **ldap**: Lightweight Directory Access Protocol (LDAP) messages logging facility
• **li**: Refer to the *Lawful Intercept Interface Reference* for a description of this command.
• **linkmgr**: SGSN/BSS SS7 Link Manager logging facility (2.5G only)
• **llc**: Logical Link Control (LLC) Protocol logging facility; for SGSN: logs the LLC layer between the GMM and the BSSGP layers for logical links between the MS and the SGSN
• **local-policy**: Local Policy Service facility
• **location-service**: Location Services facility
• **m3ua**: M3UA Protocol logging facility
• **magmgr**: Mobile Access Gateway manager logging facility
• **map**: Mobile Application Part (MAP) protocol logging facility
• **megadiamgr**: MegaDiameter Manager (SLF Service) logging facility
• **mme-app**: Mobility Management Entity (MME) Application logging facility
• **mme-misc**: MME miscellaneous logging facility
• **mmedemux**: MME Demux Manager logging facility
• **mmemgr**: MME Manager facility
• **mmgr**: Master Manager logging facility
• **mobile-ip**: Mobile IP processes
• **mobile-ip-data**: Mobile IP data facility
• **mobile-ipv6**: Mobile IPv6 logging facility
• **mpls**: Multiprotocol Label Switching (MPLS) protocol logging facility
• **mrme**: Multi Radio Mobility Entity (MRME) logging facility
• **mseg-app**: Mobile Services Edge Gateway (MSEG) application logging facility (This option is not supported in this release.)
• **mseg-gtpc**: MSEG GTP-C application logging facility (This option is not supported in this release.)
• **mseg-gtpu**: MSEG GTP-U application logging facility (This option is not supported in this release.)
• **msegmgr**: MSEG Demux Manager logging facility (This option is not supported in this release.)
• **mtp2**: Message Transfer Part 2 (MTP2) Service logging facility
• **mtp3**: Message Transfer Part 3 (MTP3) Protocol logging facility
• **multicast-proxy**: Multicast Proxy logging facility
• **nas**: Non-Access Stratum (NAS) protocol logging facility [MME 4G]
• **netwstrg**: Network Storage facility
• **npuctrl**: Network Processor Unit Control facility
• **npudrv**: Network Processor Unit Driver facility [ASR 5500 only]
• **npumgr**: Network Processor Unit Manager facility
• **npumgr-acl**: NPUMGR ACL logging facility
• **npumgr-drvt**: NPUMGR DRV logging facility
• **npumgr-flow**: NPUMGR FLOW logging facility
• **npumgr-fwd**: NPUMGR FWD logging facility
• **npumgr-init**: NPUMGR INIT logging facility
• **npumgr-lc**: NPUMGR LC logging facility
• **npumgr-port**: NPUMGR PORT logging facility
• **npumgr-recovery**: NPUMGR RECOVERY logging facility
• **npumgr-rri**: NPUMGR RRI (Reverse Route Injection) logging facility
• **npumgr-vpn**: NPUMGR VPN logging facility
• **npusim**: NPUSIM logging facility [ASR 5500 only]
• **ntfy-intf**: Notification Interface logging facility [Release 12.0 and earlier versions only]
• **ocsp**: Online Certificate Status Protocol logging facility.
• **orbs**: Object Request Broker System logging facility
• **ospf**: OSPF protocol logging facility
• **ospfv3**: OSPFv3 protocol logging facility
• **p2p**: Peer-to-Peer Detection logging facility
• **pagingmgr**: PAGINGMGR logging facility
• **pccmgr**: Intelligent Policy Control Function (IPCF) Policy Charging and Control (PCC) Manager library
• **pdg**: Packet Data Gateway (PDG) logging facility
• **pdgmgr**: PDG Demux Manager logging facility
• **pdif**: Packet Data Interworking Function (PDIF) logging facility
• **pgw**: Packet Data Network Gateway (PGW) logging facility
• **pmm-app**: Packet Mobility Management (PMM) application logging facility
• **ppp**: Point-To-Point Protocol (PPP) link and packet facilities
• **pppoed**: PPP over Ethernet logging facility
ORBEM Configuration Mode Commands

- **push**: VPNMGR CDR push logging facility
- **radius-act**: RADIUS accounting logging facility
- **radius-auth**: RADIUS authentication logging facility
- **radius-coa**: RADIUS change of authorization and radius disconnect
- **ranap**: Radio Access Network Application Part (RANAP) Protocol facility logging info flow between SGSN and RNS (3G)
- **rct**: Recovery Control Task logging facility
- **rdt**: Redirect Task logging facility
- **resmgr**: Resource Manager logging facility
- **rf-diameter**: Diameter Rf interface messages facility
- **rip**: Routing Information Protocol (RIP) logging facility [RIP is not supported at this time.]
- **rlf**: Rate Limiting Function (RLF) logging facility
- **rohc**: Robust Header Compression (RoHC) facility
- **rsvp**: Reservation Protocol logging facility
- **rua**: RANAP User Adaptation (RUA) [3G Femto GW - RUA messages] logging facility
- **s1ap**: S1 Application Protocol (S1AP) Protocol logging facility
- **sabp**: Service Area Broadcast Protocol (SABP) logging facility
- **saegw**: System Architecture Evolution (SAE) Gateway facility
- **scfp**: Signalling Connection Control Part (SCCP) Protocol logging (connection-oriented messages between RANAP and TCAP layers).
- **sct**: Shared Configuration Task logging facility
- **sctp**: Stream Control Transmission Protocol (SCTP) Protocol logging facility
- **sef_ecs**: Severely Errored Frames (SEF) APIs printing facility
- **sess-gr**: SM GR facility
- **sessctrl**: Session Controller logging facility
- **sessmgr**: Session Manager logging facility
- **sesstrec**: session trace logging facility
- **sft**: Switch Fabric Task logging facility
- **sgs**: SGs interface protocol logging facility
- **sgsn-app**: SGSN-APP logging various SGSN “glue” interfaces (for example, between PMM, MAP, GPRS-FSM, SMS).
- **sgsn-failures**: SGSN call failures (attach/activate rejects) logging facility (2.5G)
- **sgsn-gtpc**: SGSN GTP-C Protocol logging control messages between the SGSN and the GGSN
- **sgsn-gtpu**: SGSN GTP-U Protocol logging user data messages between the SGSN and GGSN
- **sgsn-mbms-bearer**: SGSN Multimedia Broadcast/Multicast Service (MBMS) Bearer app (SMGR) logging facility
- **sgsn-misc**: Used by stack manager to log binding and removing between layers
- **sgsn-system**: SGSN System Components logging facility (used infrequently)
• **sgsn-test**: SGSN Tests logging facility; used infrequently
• **sgtpcmgr**: SGSN GTP-C Manager logging information exchange through SGTPC and the GGSN
• **sgw**: Serving Gateway facility
• **sh-diameter**: Sh Diameter messages facility
• **sitmain**: System Initialization Task main logging facility
• **sm-app**: SM Protocol logging facility
• **sms**: Short Message Service (SMS) logging messages between the MS and the SMSC
• **sndep**: Sub Network Dependent Convergence Protocol (SNDCP) logging facility
• **snmp**: SNMP logging facility
• **sprmgr**: IPCF Subscriber Policy Register (SPR) manager logging facility
• **srdb**: Static Rating Database
• **srp**: Service Redundancy Protocol (SRP) logging facility
• **sscfnni**: Service-Specific Coordination Function for Signaling at the Network Node Interface (SSCF-NNI) logging facility
• **sscop**: Service-Specific Connection-Oriented Protocol (SSCOP) logging facility
• **ssh-ipse**: Secure Shell (SSH) IP Security logging facility
• **ssl**: Secure Socket Layer (SSL) message logging facility
• **stat**: Statistics logging facility
• **supserv**: Supplementary Services logging facility [H.323]
• **system**: System logging facility
• **tacacsplus**: TACACS+ Protocol logging facility
• **tcap**: TCAP Protocol logging facility
• **testctrl**: Test Controller logging facility
• **testmgr**: Test Manager logging facility
• **threshold**: threshold logging facility
• **ttg**: Tunnel Termination Gateway (TTG) logging facility
• **tucl**: TCP/UDP Convergence Layer (TUCL) logging facility
• **udr**: User Data Record (UDR) facility (used with the Charging Service)
• **user-data**: User data logging facility
• **user-l3tunnel**: User Layer 3 tunnel logging facility
• **usertcp-stack**: User TCP Stack
• **vim**: Voice Instant Messaging (VIM) logging facility
• **vinfo**: VINFO logging facility
• **vmgctrl**: Virtual Media Gateway (VMG) controller facility
• **vmgctrl**: VMG Content Manager facility
• **vpn**: Virtual Private Network logging facility
• **wimax-data**: WiMAX DATA
- `wimax-r6`: WiMAX R6

### event_level

specifies the severity level of the event notification to filter and can be configured to one of the following:

- `critical`: display critical events
- `error`: display error events and all events with a higher severity level
- `warning`: display warning events and all events with a higher severity level
- `unusual`: display unusual events and all events with a higher severity level
- `info`: display info events and all events with a higher severity level
- `trace`: display trace events and all events with a higher severity level
- `debug`: display all events

### Usage

This command is used to enable or disable the ORB Notification Service. Additionally, it can be used to configure filters dictating which events are sent. This service is disabled by default. Filters can be configured for a specific event identification number (event ID), a range of event IDs, or specific severity levels for events for particular facilities. When no filters are configured and the service is enabled, the ORB Notification Service sends all “error” level and higher events, and “info” level events for the orbs facility, CLI command logs, and license change logs. Multiple instance of this command can be executed to configure multiple filters.

### Example

The following command enables the ORB Notification service:

```
   event-notif-service
```

The following command disables the ORB Notification service:

```
   no event-notif-service
```

The following command configures a filter for the ORB Notification Service allowing only event IDs 800 through 805 to be sent:

```
   event-notif-service filter event-id 800 to 805
```

The following command configures a filter for the ORB Notification Service allowing only `critical` level notifications for all facilities:

```
   event-notif-service filter facility all level critical
```
event-notif-siop-port

Configures the port to use for secure socket layer (SSL) inter-ORB event communication.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > ORBEM Configuration

```bash
configure > orbem
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ORBEM)#
```

**Syntax**

```
event-notif-siop-port number
```

*number*

Default: 7777

Specifies the port number to use as an integer from 1 through 65535.

**Usage**

Explicitly set the port number when the default port number is not the desired port value for integrating multiple products together for inter-ORB communications using SSL.

**Example**

```
event-notif-siop-port 25466
```
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Use this command to return to the parent configuration mode.
**iiop-port**

Configures the port number for Internet Inter-ORB Protocol (IIOP) communications.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > ORBEM Configuration

`configure > orbem`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ORBEM)#
```

**Syntax**

```
[ no ] iiop-port number
```

- **no**
  
  Disables the IIOP port.

- **number**
  
  Default: 14132
  
  Specifies the port number to use as an integer from 1 through 65535.

**Usage**

Explicitly set the port number when the default port number is not the desired port value for integrating multiple products together for standardized inter-ORB communications.

Internet inter-ORB port is only used if IIOP transport is enabled via the `iiop-transport` command.

**Example**

```
iiop-port 25466
```
**iiop-transport**

Enables/disables use of the Internet Inter-ORB Protocol (IIOP) for management across the network.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > ORBEM Configuration

`configure > orbem`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-orbem)#
```

**Syntax**

```
iiop-transport

no iiop-transport
```

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no iiop-transport</td>
<td>Disables internet inter-ORB protocol communication across the network.</td>
</tr>
</tbody>
</table>

**Usage**

Enables the transport of IIOP messages to support remote management across the network.

The default is IIOP transport disabled.

**Example**

The following commands enable and disable the ORB-based management across the network, respectively.

```
iiop-transport

no iiop-transport
```
**iop-address**

Sets the IP address used by the ORBEM Server to advertise service.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > ORBEM Configuration

```bash
configure > orbem
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-orbem)#
```

**Syntax**

```
iop-address  ip_address
```

`ip_address`

Specifies the IP address to use for inter-ORB communications for the current context. `ip_address` must be specified using IPv4 dotted-decimal notation.

**Usage**

Change the inter-ORB IP address when the IP address of the current context should not be used. The IP address of the local context may not be appropriate when the ORB configuration across nodes would cause conflicts with the IP addresses.

The default inter-ORB IP address is the IP address of the current context.

**Example**

```
iop-address 10.2.3.4
```
**max-attempt**

Configures the maximum number of failed login attempts after which the client is deactivated.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > ORBEM Configuration

`configure > orbem`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-orbem)#
```

**Syntax**

```
max-attempt count
```

`count`

Default: 3 attempts

Specifies the number of failed login attempts prior to deactivating a client. The value must be an integer from 1 through 10.

**Usage**

Adjust the maximum number of attempts to a smaller value to increase the security level of the system.

**Example**

```
max-attempt 3
```
session-timeout

Configures the amount of idle time (no activity) before a client session is terminated.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > ORBEM Configuration

configure > orbem

Entering the above command sequence results in the following prompt:

[local]host_name(config-orbem)#

Syntax

```
session-timeout seconds
```

seconds

Default: 300 seconds
Specifies the number of seconds of idle time before a client session is terminated. The value must be an integer from 1 through 86400.

Usage

Reduce the session timeout when the maximum number of sessions allowed is frequently being reached. Setting this to a lower value will help release idle sessions faster to allow use by other clients.

Example

```
session-timeout 1800
```
siop-port

Configures the SSL I/O port for inter-ORB events.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > ORBEM Configuration
configure > orbem

Entering the above command sequence results in the following prompt:

[local]host_name(config-orbem)#

Syntax

siop-port number

number

Default: 14131
Specifies the port number to use as an integer from 1 through 65535.

Usage
Explicitly set the port number when the default port number is not the desired port value for integrating multiple products together for inter-ORB communications.

Example

siop-port 25466
ssl-auth-policy

Configures the SSL peer authentication policy used by the ORBEM server.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > ORBEM Configuration
configure > orbem
Entering the above command sequence results in the following prompt:

[local] host_name(config-orbem)#

Syntax

ssl-auth-policy { auth-none | auth-once | auth-once-fail | auth-peer | auth-peer-fail }

auth-none | auth-once | auth-once-fail | auth-peer | auth-peer-fail

Default: auth-none
auth-none: ORBEM server does not authenticate the peer
auth-once: ORBEM server authenticates the peer once (no fail)
auth-once-fail: ORBEM server authenticates the peer once (fail if no certificate)
auth-peer: ORBEM server authenticates the peer every time (no fail)
auth-peer-fail: ORBEM server authenticates the peer every time (fail if no certificate)

Usage
Use to configure the peer authentication policy used by the SSL transport of ORBEM.

Example
The following command sets the policy to authenticate the peer once without failure.

ssl-auth-policy auth-once
ssl-certificate

Defines the certificate to be used by the SSL transport of ORBEM.

Product

All

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > ORBEM Configuration
configure > orbem

Entering the above command sequence results in the following prompt:

[local]host_name(config-orbem)#

Syntax

ssl-certificate { string certificate | file url }

string certificate

Specifies an ORBEM SSL certificate. certificate is an alphanumeric string of up to 4096 characters.

file url

Default: /usr/ssl/certs/orbscert.pem
Specifies an ORBEM SSL certificate file and location. url is an alphanumeric string of up to 1024 characters.

Usage

Use to configure the certificate to be used by the SSL transport of ORBEM. Note that if the file option is used, the certificate content is read from the url and converted into a quoted string.

Example

The following command defines the certificate cert3.pem file as being located in the /usr/ssl/certs directory:

ssl-certificate file /usr/ssl/certs/cert3.pem

The following command defines the certificate string (the string shown is abbreviated):

ssl-certificate string

"-----BEGIN CERTIFICATE-----
MIIELDCCA5WgAwIBAgIBATANBgkqhkiG9w0BAQQFADCBsTELMAkGA1UEBhMCVVMx
FjAUBgNVBAgTDU1hc3NhY2h1c2V0dHMxETAfM2Rld2tzYnVyeTeMBwG
A1UEChMVU3RhcmVudCB0ZXRxZ3b3JrcyBJbmMuMSIwIAYDVQQLExlFbGVtZW50IEdv
b3JiZW1AbnVsaW5raW5jLmNvbTAgMaMwJSd0TVFsZnVzaW9uQ0EwDQYJKoZIhvcNAQEF
b3JiZW1AbnVsaW5raW5jLmNvbTAeFw0wMjA5MDYxMjE5MTNaFw0yMjA5MDExMjE5
-----END CERTIFICATE-----"
ssl
certificate

MTNaMIGxMQswCQYDVQQGEwJVUzEWMBQGA1UECBMNTWFzc2FjaHVzZXR0czESMBAG
A1UdDgQWBBSpuGGMTwgaq8H+e70ZPIFHVZjiWDCB3gYDVR0jBIHWMIHTgBRkV
Bzy
4zW5Gv0pXcwT07PtzCm53qGb6SBtDCBsTELMAkGA1UEBhMCVVMyFjAU
BgNVBAgT
DU1hc3NhY2h1c2V0dHMxEjAQBgNVAcTCVQRld2tzYnVyeTEeMBwGA1UECh
MVU3Rh
cmVudCBOZXRx3b3JrcyBbmMzIAYDVQLExLFbGtZW50IE1hbmFnZWZlbnQg
U3lz
MVQ4wDAYDVQQDEwVPUKJFT
TeiMCAGCSqGSIb3DQEJARYb3JiZW1AbnV
aw5raW5raW5jZW1AbnV

-----END CERTIFICATE-----

Cisco ASR 5x00 Command Line Interface Reference
ssl-private-key

Configures the SSL private key used by the ORBEM server.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > ORBEM Configuration
configure > orbem

Entering the above command sequence results in the following prompt:

[local]host_name(config-ORBEM)#

Syntax

ssl-private-key { string key | file url }

string key
Specifies an ORBEM SSL private key. key is an alphanumeric string of up to 4096 characters.

file url
Default: /usr/ssl/certs/orbscert.pem
Specifies the ORBEM SSL private key file location. url is an alphanumeric string of up to 1024 characters.

Usage

Use to configure the private key for the SSL transport of ORBEM. Note that if file option is used, the private key is read from the url and converted into a quoted string.

Example

The following command defines the private-key cert3.pem file as being located in the /usr/ssl/certs directory:

ssl-private-key file /usr/ssl/certs/cert3.pem

The following command defines the private-key string (the string shown is abbreviated):

ssl-private-key string

"-----BEGIN RSA PRIVATE KEY-----
MIICXQIBAAKBgQC6Dh79iaK/zzG/Kwme2XS6G8/n3/+sac6huxI1WNgammyY9ZKZp
XTjHUjS92vn0UUM4tFjN4XoqveSiqy3IqUhnVKS3+0L7s9beanQUuR9MdLyd9Ho
7qh720wpN4isqN7yFGloqGsLQjhs8z6ZT0ZUhyusY0rE6yHTV23n6HKNtQIDAQAB
9br1iVWvy/N23WXwZliH+el7BiFhqlSd/0wJBAEEOOGH/vJse/YdHeYjIT76lcoG
Tq6ldbXdoLDRGUF2AqdboJ7wVCOJQO34XbBtmWfTkqz48M6u3/5kDFH8CQGAI
-----END RSA PRIVATE KEY-----"
XObwPFRztvkXprZfh7IekxAIuoHiT1JsEKSIIPzEqDY2rmoWDghOvPETO+5zWEQk\n\nTXzLaRgbly9MKnXSt8CQQCeBfT7VndEfiG9VWyPzeL4vx4ZiUMZQ6FJdXo7Xq9x\n\nmzX8hgcfdg3tahlNt35gL/DjUY7d14+MgLrRf3Udbk9\n
-----END RSA PRIVATE KEY-----\n"
Chapter 229
OSPF Configuration Mode Commands

The OSPF Configuration sub-mode is used to configure the Open Shortest Path First (OSPF) routing protocol. This mode includes commands that configure OSPF routing parameters.

Mode

Exec > Global Configuration > Context Configuration > OSPF Configuration

configure > context context_name > router ospf

Entering the above command sequence results in the following prompt:

[local]host_name(config-ospf)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
area authentication

Enables authentication for the specified OSPF area.

Product
PDSN
HA
GGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > OSPF Configuration
configure > context context_name > router ospf

Entering the above command sequence results in the following prompt:

[local]host_name(config-ospf)#

Syntax

[ no ] area { ipaddress | decimal_value } authentication { message-digest }

- no
  Disables authentication for the specified area.

- ipaddress
  Specifies the IP address of the area where authentication will be enabled in IPv4 dotted-decimal notation.

- decimal-value
  Specifies the identification number of the area where authentication will be enabled. This must be an integer from 0 through 4294967295.

- authentication
  Sets the OSPF authentication type to use the simple authentication method.

- message-digest
  Sets the OSPF authentication type to use the message digest 5 (MD5) authentication method.

Usage
Use this command to enable authentication of OSPF areas.

Example
The following command enables authentication for an OSPF area defined by the IP address 192.168.100.10 and the OSPF authentication type to MD5:

    area 192.168.100.10 authentication message-digest
area default-cost

Configures the default cost for an area.

Product
PDSN
HA
GGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > OSPF Configuration
configure > context context_name > router ospf

Entering the above command sequence results in the following prompt:

[local]host_name(config-ospf)#

Syntax
[ no ] area { ipaddress | decimal_value } default-cost cost_value

no
Deletes the default cost for the area.

ipaddress
Specifies the IP address of the area in IPv4 dotted-decimal notation.

decimal-value
Specifies the identification number of the area as an integer from 0 through 4294967295.

cost_value
Sets the default cost to be configured for the specified area as an integer from 0 through 16777215.

Usage
Use this command to configure the default cost for an OSPF area.

Example
The following command sets the default cost for an OSPF area defined by the IP address 192.168.100.10 to 300:

area 192.168.100.10 default-cost 300
area nssa

Defines an area as an NSSA (Not So Stubby Area) and configures OSPF parameters for it.

**Product**

PDSN
HA
GGSN

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > OSPF Configuration

```
configure > context context_name > router ospf
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ospf)#
```

**Syntax**

```
[ no ] area { ipaddress | decimal_value } nssa [ default-information-originate ] [ no-redistribution ] [ no-summary ] [ translate-always ] [ translate-candidate ] [ translate-never ]
```

**ipaddress**

Specifies the IP address of the NSSA in IPv4 dotted-decimal notation.

**decimal-value**

Specifies the identification number of the NSSA area as an integer from 0 through 4294967295.

**default-information-originate**

Originates default information to the NSSA area.

**no-redistribution**

Does not redistribute external routes to the NSSA area.

**no-summary**

Does not inject inter-area routes into NSSA.

**translate-always**

Configures the NSSA-ABR (Area Border Router) to always translate

**translate-candidate**

Configure NSSA-ABR for translate election. (This is enabled by default.)
translate-never

Configure NSSA-ABR to never translate.

Usage

Use this command to define NSSA areas.

Example

The following command defines the area designated by the IP address 192.168.100.10 as an NSSA area:

```
area 192.168.100.10 nssa
```
area stub

Defines an area as an OSPF stub area.

Product
- PDSN
- HA
- GGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > OSPF Configuration

configure > context context_name > router ospf

Entering the above command sequence results in the following prompt:

[local]host_name(config-ospf)#

Syntax

[ no ] area { ipaddress | decimal_value } stub [ no-summary ]

ipaddress
Specifies the IP address of the stub area in IPv4 dotted-decimal notation.

decimal-value
Specifies the identification number of the stub area as an integer from 0 through 4294967295.

no-summary
Disables (stops) the ABR (Area Border Router) from sending summary link state advertisements (LSAs) into the stub area.

Usage
Use this command to define an OSPF area as a stub area.

Example
The following command defines the OSPF area defined by the IP address 192.168.100.10 as a stub area:

area 192.168.100.10 stub
area virtual-link

Configures a virtual link between an area that cannot be physically connected to the network backbone and an area that is physically connected to the network backbone.

**Product**

PDSN  
HA  
GGSN

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > OSPF Configuration  
`configure > context context_name > router ospf`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ospf)#
```

**Syntax**

```
[ no ] area { ipaddress | decimal_value } virtual-link router_id_address
```

- **no**  
  Disables area virtual-link.

- **ipaddress**  
  Specifies the IP address of the transit area in IPv4 dotted-decimal notation.

- **decimal-value**  
  Specifies the identification number of the transit area as an integer from 0 through 4294967295.

- **router_id_address**  
  Specifies the router id of the ABR to be linked to in IPv4 dotted-decimal notation.

**Usage**

Use this command to create a virtual link between an area that is connected to the network backbone and an area that cannot be connected to the network backbone.

**Example**

The following command creates a virtual link between the OSPF areas defined by the IP address 192.168.100.10 and the IP address 192.168.200.20:

```
area 192.168.100.10 virtual-link 192.168.200.20
```
area virtual link authentication

Configures the OSPF authentication method to be used by the virtual link between an area that cannot be physically connected to the network backbone and an area that is physically connected to the network backbone.

**Product**
PDSN
HA
GGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > OSPF Configuration

```
configure > context context_name > router ospf
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ospf)#
```

**Syntax**

```
[ no ] area { ipaddress | decimal_value } virtual-link router_id_address authentication { message-digest | null | text }
```

- **no**
  Disables area virtual link authentication.

- **ipaddress**
  Specifies the IP address of the transit area in IPv4 dotted-decimal notation.

- **decimal-value**
  Specifies the identification number of the transit area as an integer from 0 through 4294967295.

- **router_id_address**
  Specifies the router id of the ABR to be linked to in IPv4 dotted-decimal notation.

- **authentication**
  Sets the OSPF authentication type to use the simple authentication method.

- **message-digest**
  Sets the OSPF authentication type to use the message digest (MD) authentication method.

- **null**
  Set the OSPF authentication type to use no authentication, thus disabling either MD or clear text methods.
area virtual link authentication

text
Set the OSPF authentication type to use the clear text authentication method.

Usage
Use this command to set the authentication method for a virtual link between an area that is connected to the network backbone and an area that cannot be connected to the network backbone.

Example
The following command sets the authentication method for a virtual link between the OSPF areas defined by the IP address 192.168.100.10 and the IP address 192.168.200.20 to use no authentication:

```text
area 192.168.100.10 virtual-link 192.168.200.20 null
```
area virtual-link authentication-key

Configures the authentication password for the virtual link between an area that cannot be physically connected to the network backbone and an area that is physically connected to the network backbone.

**Product**
- PDSN
- HA
- GGSN

**Privilege**
- Security Administrator, Administrator

**Mode**

- Exec > Global Configuration > Context Configuration > OSPF Configuration
- configure > context context_name > router ospf

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-ospf)#
```

**Syntax**

```
area { ipaddress | decimal_value } virtual-link router_id_address authentication-key { encrypted password | encrypted_authentication_key | password authentication_key }

no area { ipaddress | decimal_value } virtual-link router_id_address authentication-key
```

**no**

Disables the area virtual link authentication key.

**ipaddress**

Specifies the IP address of the transit area in IPv4 dotted-decimal notation.

**decimal-value**

Specifies the identification number of the transit area as an integer from 0 through 4294967295.

**router_id_address**

Specifies the router id of the ABR to be linked to in IPv4 dotted-decimal notation.

**encrypted password**

`encrypted_authentication_key` is an alphanumeric string of 1 through 523 characters. Use this if you are pasting a previously encrypted authentication key into the CLI command.

**password authentication_key**

The password to use for authentication. `authentication_key` is an alphanumeric string of 1 through 16 characters that denotes the authentication password. This variable is entered in clear text format.
Usage

Use this command to specify the authentication password for a virtual link between an area that is connected to the network backbone and an area that cannot be connected to the network backbone.

Example

The following command creates an authentication password of 123456 for a virtual link between the OSPF areas defined by the IP address 192.168.100.10 and the IP address 192.168.200.20:

```
area 192.168.100.10 virtual-link 192.168.200.20 authentication-key password 123456
```
area virtual link intervals

Configures the interval or delay type, and the delay time in seconds, for the virtual link between an area that cannot be physically connected to the network backbone and an area that is physically connected to the network backbone.

**Product**
- PDSN
- HA
- GGSN

**Privilege**
- Security Administrator, Administrator

**Mode**
```
Exec > Global Configuration > Context Configuration > OSPF Configuration
```
```
configure > context context_name > router ospf
```

Entering the above command sequence results in the following prompt:
```
[local]host_name(config-ospf)>
```

**Syntax**
```
[ no ] area { ipaddress | decimal_value } virtual-link router_id_address [ dead-interval value ] [ hello-interval value ] [ retransmit-interval value ] [ transmit-delay value ]
```

- **no**
  - Disables the area virtual link intervals.

- **ipaddress**
  - Specifies the IP address of the area in IPv4 dotted-decimal notation.

- **decimal-value**
  - Specifies the identification number of the transit area as an integer from 0 through 4294967295.

- **router_id_address**
  - Specifies the router id of the ABR to be linked to in IPv4 dotted-decimal notation.

- **dead-interval value**
  - Specifies The interval (in seconds) that the router should wait, during which time no packets are received and after the router considers a neighboring router to be off-line. value must be an integer from 1 through 65535.

- **hello-interval value**
  - Specifies the interval (in seconds) before sending a hello packet. value must be an integer from 1 through 65535.
retransmit-interval value

Specifies the interval (in seconds) that router should wait before retransmitting a packet. value must be an integer from 1 through 3600.

transmit-delay value

Specifies the interval (in seconds) that the router should wait before transmitting a packet. value must be an integer from 1 through 3600.

Usage

Use this command to set the intervals or delay types for a virtual link between an area that is connected to the network backbone and an area that cannot be connected to the network backbone.

Example

The following command sets the retransmit interval for a virtual link between the OSPF areas defined by the IP address 192.168.100.10 and the IP address 192.168.200.20 to 60 seconds:

```
area 192.168.100.10 virtual-link 192.168.200.20 retransmit-interval 60
```
area virtual link message-digest-key

Enables the use of MD5-based OSPF authentication for the virtual link between an area that cannot be physically connected to the network backbone and an area that is physically connected to the network backbone.

Product
PDSN
HA
GGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > OSPF Configuration
configure > context context_name > router ospf

Entering the above command sequence results in the following prompt:

[local] host_name(config-ospf) #

Syntax
area { ipaddress | decimal_value } virtual-link router_id_address message-digest-key
key_id md5 { encrypted password encrypted_authentication_key | password
authentication_key }

no area { ipaddress | decimal_value } virtual-link router_id_address message-digest-key
key_id

no
Disables the area virtual link message digest key.

ipaddress
Specifies the IP address of the transit area in IPv4 dotted-decimal notation.

decimal-value
Specifies the identification number of the transit area as an integer from 0 through 4294967295.

router_id_address
Specifies the router id of the ABR to be linked to in IPV4 dotted-decimal notation.

message-digest-key key_id
Specifies the key identifier number. key_id must be an integer from 1 through 255.

encrypted password
Specifies the use of an encrypted password. encrypted_authentication_key is an alphanumeric string of 1 through 523 characters.
Used this if you are pasting a previously encrypted authentication key into the CLI command.
password authentication_key

Specifies the password to use for authentication. authentication_key is an alphanumeric string from 1 through 16 characters that is entered in clear text format.

Usage

Use this command to enable the use of MD5-based OSPF authentication for a virtual link between an area that is connected to the network backbone and an area that cannot be connected to the network backbone.

Example

The following command enables the use of MD5-based OSPF authentication for a virtual link between the OSPF areas defined by the IP address 192.168.100.10 and the IP address 192.168.200.20, sets the MD5 Key ID to 25, and the password to 123456:

```
area 192.168.100.10 virtual-link 192.168.200.20 message-digest-key 25 md5 password 123456
```
**bfd-all-interfaces**

Enables or disables Bidirectional Forwarding Detection (BFD) on all OSPF interfaces.

**Product**
- PDSN
- HA
- GGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > OSPF Configuration
```plaintext
configure > context context_name > router ospf
```
Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ospf)#
```

**Syntax**
```
[no] bfd-all-interfaces
```

- **no**
  Disables BFD capability on all interfaces.

- **Usage**
  Use this command to configure BFD on all OSPF interfaces. See the *System Administration Guide* for additional information on how to configure BFD.

- **Example**
  The following command configures BFD on all OSPF interfaces:

```
bfd-all-interfaces
```
capability graceful-restart

Configures graceful-restart. By default, this capability is set to enabled.

**Product**
- PDSN
- HA
- GGSN

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration > Context Configuration > OSPF Configuration
- `configure > context context_name > router ospf`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ospf)#
```

**Syntax**

```
[ no | default ] capability graceful-restart
```

- **no**
  - Disables the graceful-restart capability.

- **default**
  - Enables the graceful-restart capability if it has been disabled.

**Usage**

Use this command to configure graceful-restart.

**Example**

The following command configures graceful-restart:

```
capability graceful-restart
```
default-information originate

Creates a default external route into an OSPF routing domain.

Product
- PDSN
- HA
- GGSN

Privilege
- Security Administrator, Administrator

Mode
- Exec > Global Configuration > Context Configuration > OSPF Configuration
  
  configure > context context_name > router ospf

Entering the above command sequence results in the following prompt:

[local]host_name(config-ospf)#

Syntax

default-information originate

default-information originate [ always ] [ metric metric_value ] [ metric-type { 1 | 2 } ] [ route-map route_map_name ]

no default-information originate

no

Disables the default external route.

- **always**
  - Always advertise the route regardless of whether or not the software has a default route.

- **metric metric_value**
  - Sets the OSPF metric used in creating the default route as an integer from 1 through 16777214.

- **metric-type { 1 | 2 }**
  - Sets the default route metric type.
  - 1: Sets the OSPF external link type for default routes to Type 1.
  - 2: Sets the OSPF external link type for default routes to Type 2.

- **route-map route_map_name**
  - Specifies the name of the default route-map to be use as an alphanumeric string of 1 through 79 characters.

Usage

Use this command to set the default external route into an OSPF routing domain.
The following command sets the default external route to originate from the route map named `rmap1`:

```
default-information originate route-map rmap1
```
default-metric

Configures the default metric value for the OSPF routing protocol. All OSPF interfaces have a cost, which is a routing metric that is used in the link-state calculation. Routes with lower total path metrics are preferred over those with higher path metrics. When several equal-cost routes to a destination exist, traffic is distributed equally among them. The default metric is a global parameter that specifies the cost applied to all OSPF routes by default.

Product
- PDSN
- HA
- GGSN

Privilege
Security Administrator, Administrator

Mode
- Exec > Global Configuration > Context Configuration > OSPF Configuration
- configure > context context_name > router ospf

Entering the above command sequence results in the following prompt:

[local]host_name(config-ospf)#

Syntax

```plaintext
default-metric metric_value

no default-metric
```

**metric-value**

Sets the metric value expressed as an integer from 1 through 16777214. Default: 26385.

**no**

Enables or disables the default metric value for OSPF.

Usage

Use this command to set the default metric for routes.

Example

The following command sets the default metric to 235:

```
default-metric 235```
distance

Configures the OSPF route administrative distances for all OSPF route types or based on specific route type. Administrative distance is the measure used by Cisco routers to select the best path when there are two or more different routes to the same destination from two different routing protocols. Administrative distance defines the reliability of a routing protocol. Each routing protocol is prioritized in order of most to least reliable (believable) using an administrative distance value. A lower numerical value is preferred.

**Product**
- PDSN
- HA
- GGSN

**Privilege**
- Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > OSPF Configuration

```
configure > context context_name > router ospf
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ospf)#
```

**Syntax**

```
[ no ] distance { distance_value | ospf { [ external distance_value ] [ inter-area distance_value ] [ intra-area distance_value ] } }
```

- **no**
  Disables the OSPF route administrative distances for all OSPF route types.

- **distance_value**
  Specifies the OSPF route administrative distances as an integer from 1 to 255. The default distance value is 110.

- **ospf { [ external distance_value ] [ inter-area distance_value ] [ intra-area distance_value ] }**
  Set the distance value for the specified route type.
  - **external distance_value**: Set the OSPF route administrative distance for routes from other routing domains, learned by redistribution. This must be an integer from 1 through 255. The default is 110.
  - **inter-area distance_value**: sets the OSPF route administrative distance for routes from one routing area to another. This must be an integer from 1 through 255. The default is 110.
  - **intra-area distance_value**: sets the OSPF route administrative distance for all routes within an area. This must be an integer from 1 through 255. The default is 110.

- **no**
  Enables or disables the specified option.
**Usage**

Use this command to set the administrative distance for OSPF routes.

**Example**

The following command sets the administrative distance for all OSPF route types to 30:

```
distance 30
```
**distribute-list**

Enables or disables the filtering of networks in outgoing routing updates.

**Product**
- PDSN
- HA
- GGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > OSPF Configuration

```bash
configure > context context_name > router ospf
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ospf)#
```

**Syntax**

```
[ no ] distribute-list route_access_list out { connected | rip | static }
```

- **no**
  Disables the filtering of networks in outgoing routing updates.

- **route_access_list**
  Specifies the name of the OSPF route access list to use for filtering as an alphanumeric string of 1 through 63 characters.

- **connected**
  Filters connected routes.

- **rip**
  Filters RIP routes. (RIP is not supported at this time.)

- **static**
  Filters static routes.

- **no**
  Disables the specified option.

**Usage**

Use this command to enable the filtering of outgoing route updates by using the specified route access list.

**Example**

Use this command to enable the filtering of outgoing route updates by using the specified route access list.
The following command uses the route access list named *ral1* to filter outgoing routing updates for all connected routes:

```
distribute-list ral1 out connected
```
**end**

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**

Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Use this command to return to the parent configuration mode.
ip vrf

Configures the Virtual Routing and Forwarding (VRF) instances for OSPF routing protocol.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > OSPF Configuration

configure > context context_name > router ospf

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ospf)#
```

**Syntax**

```
[ no ] ip vrf vrf_name
```

- **no**
  
  Disables the VRF instances and removes the configured VRF context association for OSPF routing.

- **vrf vrf_name**

  Configures Virtual Routing & Forwarding (VRF) parameters.
  
  *vrf_name* is name of a preconfigured VRF context configured in Context Configuration Mode via the `ip vrf` command. It is an alphanumeric string of 1 through 63 characters.

**Usage**

Use this command to configure the IP VRF forwarding also to associate the preconfigured VRF context with the specific tunnel interface.

This command creates and enters the OSPF VRF Configuration Mode if required to configure the VRF context instances for OSPF routing.

**Example**

The following command enables preconfigured VRF context instance *ospf_vrf1* for OSPF routing and enters the OSPF VRF Configuration mode:

```
ip vrf ospf_vrf1
```
neighbor

Configures OSPF routers that interconnect to non-broadcast networks.

**Product**
- PDSN
- HA
- GGSN

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration > Context Configuration > OSPF Configuration

```
configure > context context_name > router ospf
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ospf)#
```

**Syntax**

```
[ no ] neighbor ip_address [ poll-interval poll_interval_value ] [ priority priority_value ]
```

**no**

Disables OSPF routers that interconnect to non-broadcast networks.

---

**ip_address**

Specifies the interface IP address of the OSPF neighbor expressed using IPv4 dotted-decimal notation.

**poll-interval poll_interval_value**

Default: 120
Sets the number of seconds in the dead neighbor polling interval as an integer from 1 through 65535.

**priority priority_value**

Default: 0
Sets the 8-bit number that represents the router priority value of the non-broadcast neighbor associated with the specified IP address. This must be an integer from 0 through 255. This keyword does not apply to point-to-multipoint interfaces.

**Usage**

Use this command to configure OSPF routers that connect to non-broadcast networks.

**Example**

The following command specifies an OSPF router neighbor with the IP address of `192.168.100.10`:

```
neighbor 192.168.100.10
```
network area

Enables OSPF on an interface and defines the OSPF area for that network.

Product

- PDSN
- HA
- GGSN

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > Context Configuration > OSPF Configuration

configure > context context_name > router ospf

Entering the above command sequence results in the following prompt:

[local]host_name(config-ospf)#

Syntax

[ no ] network network_ip_address / network_mask area { area_id | area_ip_address }

- no
  Enables OSPF on an interface and defines the OSPF area for that network.

- network_ip_address/network_mask
  Specifies the network address and mask as well as the interface on which OSPF will be enabled. network_ip_address is entered in IPv4 dotted-decimal notation, followed by the “/” and the mask (CIDR).

- area_id
  Specifies the OSPF area identification number for the specified network as an integer from 0 through 4294967295.

- area_ip_address
  Specifies the IP address of the OSPF area for this network. This must be entered in IPv4 dotted-decimal notation.

Usage

Use this command to specify the IP address of the network interface that the OSPF router will use.

Example

The following command specified that the OSPF router will use the interface at IP address 192.168.1.0 with a netmask of 24:

    network 192.168.1.0/24
ospf graceful-restart

Configures OSPF graceful-restart settings.

Product

- PDSN
- HA
- GGSN

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > Context Configuration > OSPF Configuration

configure > context context_name > router ospf

Entering the above command sequence results in the following prompt:

[local]host_name(config-ospf)#

Syntax

ospf graceful-restart { grace-period grace_period | helper { never | policy { only-reload | only-upgrade } } |

<table>
<thead>
<tr>
<th>grace-period grace-period</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the OSPF graceful restart grace period (in seconds) as an integer from 1 through 1800. Default grace period is 60 seconds.</td>
</tr>
</tbody>
</table>

| helper { never | policy { only-reload | only-upgrade } } |
|---------------------------------------------------------|
| Helps configure OSPF helper settings. |
| never: Do not allow helper mode. |
| policy { only-reload | only-upgrade }): Allows ospf graceful-restart helper mode. |
| only-reload: Allows ospf graceful-restart helper mode only for a reload. |
| only-upgrade: Allows ospf graceful-restart helper mode only for an upgrade. |
| Default is ospf graceful-restart grace-period. |

Usage

Use this command to configure graceful-restart specific settings.

Example

The following command sets the graceful restart grace period to 60 seconds:

ospf graceful-restart grace-period 60

ospf graceful-restart helper policy only-reload

ospf graceful-restart helper policy only-upgrade
**ospf router-id**

This command configures the router ID for the OSPF process.

**Product**
- PDSN
- HA
- GGSN

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration > Context Configuration > OSPF Configuration
- `configure > context context_name > router ospf`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ospf)#
```

**Syntax**

```
[ no ] ospf router-id ip_address
```

- `no`
  - Disables the router ID for the OSPF process.

- `router-id ip_address`
  - Specifies the router ID for the OSPF process. `ip_address` is entered using IPv4 dotted-decimal notation.

**Usage**

Use this command to set the router ID for the current OSPF router process.

**Example**

The following command sets the router ID to `192.168.200.1`:

```
ospf router-id 192.168.200.1
```
**passive-interface**

Enables or disables the suppression of OSPF routing updates on the specified interface.

**Product**
- PDSN
- HA
- GGSN

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration > Context Configuration > OSPF Configuration
- `configure > context context_name > router ospf`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ospf)#
```

**Syntax**

```
[ no ] passive-interface interface_name
```

- **no**
  - Disables the name assigned to a logical interface within the specific context.

- **interface_name**
  - Specifies the name assigned to a logical interface within the specific context as an alphanumeric string of 1 through 79 characters.

**Usage**

Use this command to suppress router updates on an interface in the current context.

**Example**

The following command suppresses OSPF routing updates on the interface named `Intfcl`:

```
passive-interface Intfcl
```
**redistribute**

Redistributes routes from other protocols to OSPF neighbors using the OSPF protocol.

**Product**
- PDSN
- HA
- GGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > OSPF Configuration
configure > context context_name > router ospf

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ospf)#
```

**Syntax**

```
redistribute { connected | rip | static } [ metric metric_value ] [ metric-type { 1 | 2 } ] [ route-map route_map_name ]
```

```
no redistribute { connected | rip | static }
```

**no**
Disables the redistributed routes.

**connected**
Redistributes connected routes.

**rip**
Specifies that RIP routes will be redistributed. (RIP is not supported at this time.)

**static**
Redistributes static routes.

**metric metric_value**
Sets the OSPF metric used in the redistributed route. This must be an integer from 1 through 16777214.

**metric-type { 1 | 2 }**
Default: 2
Sets route metric type that is applied to redistributed routes.
1: Sets the OSPF external link type for routes to Type 1.
2: Sets the OSPF external link type for routes to Type 2.
route-map route_map_name

Filter routes through the specified route map before redistribution. route_map_name specifies the name of the route-map to use as an alphanumeric string of 1 through 79 characters.

**Usage**

Use this command to define what routing protocols should have their routes redistributed into OSPF.

**Example**

The following command defines that BGP routes should be redistributed:

```
redistribute connected
```
refresh timer

Adjusts settings for the OSPF refresh timer.

Product
PDSN
HA
GGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > OSPF Configuration
configure > context context_name > router ospf

Entering the above command sequence results in the following prompt:
[local]host_name(config-ospf)#

Syntax

[ no ] refresh timer value

no
Disables the refresh timer.

value
Default: 10
Specifies the minimum amount of time (in seconds) to wait before refreshing a Link-state Advertisement (LSA). This must be an integer from 10 through 1800.

Usage
Use this command to define the amount of time to wait before refreshing an LSA.

Example
The following command sets the refresh timer to 90 seconds:

    refresh timer 90
router-id

Configures the router ID for the OSPF process.

Product
- PDSN
- HA
- GGSN

Privilege
- Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > OSPF Configuration

configure > context context_name > router ospf

Entering the above command sequence results in the following prompt:

[local]host_name(config-ospf)#

Syntax

[ no ] router-id ip_address

no
Disables the router ID for the OSPF process.

ip_address
Specifies the router ID for the OSPF process in IPv4 dotted-decimal notation.

Usage
Use this command to set the router ID for the current OSPF router process.

Example
The following command sets the router ID to 192.168.200.1:

    router-id 192.168.200.1
timers spf

Sets the Shortest Path First (SPF) timers.

Product

PDSN
HA
GGSN

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > Context Configuration > OSPF Configuration

configure > context context_name > router ospf

Entering the above command sequence results in the following prompt:

[local]host_name(config-ospf)#

Syntax

```
timers spf delay_value hold_time_value
no timers spf
```

**no**

Disables SPF timers.

```
delay_value
```

Default: 5

Specifies the delay time (in seconds) between receiving changes to an SPF calculation. This must be an integer from 0 through 4294967295.

```
hold_time_value
```

Default: 10

Specifies the hold time (in seconds) between consecutive SPF calculations. This must be an integer from 0 through 4294967295.

Usage

Use this command to set the SPF delay and hold timers for the current OSPF router process.

Example

The following command sets the delay timer to 15 and the hold timer to 15:

```
timers spf 15 15
```
Chapter 230
OSPFv3 Configuration Mode Commands

The OSPFv3 Configuration sub-mode is used to configure the OSPFv3 routing protocol. This mode includes commands that configure OSPFv3 routing parameters.

**Mode**

Exec > Global Configuration > Context Configuration > OSPFv3 Configuration

```bash
configure > context context_name > router ospfv3
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-ospfv3) #
```

⚠️ **Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
area

Configures an Open Shortest Path First Version 3 (OSPFv3) area and enables authentication for that area.

Product

- PDSN
- HA
- GGSN

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > Context Configuration > OSPFv3 Configuration

```bash
configure > context context_name > router ospfv3
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ospfv3)#
```

Syntax

```bash
[ no | area { decimal_value | ipv4address } default-cost default_integer_value | stub [ no-summary ] | virtual-link virtuallink_neighbour_Ipv4_address [ dead-interval virtuallink_dead_interval ] [ hello-interval virtuallink_hello_interval ] [ retransmit-interval virtuallink_retransmit_interval ] [ transmit-delay virtuallink_transmit_delay ]
```

- `[ no | area { decimal_value | ipv4address } default-cost default_integer_value | stub [ no-summary ] | virtual-link virtuallink_neighbour_Ipv4_address [ dead-interval virtuallink_dead_interval ] [ hello-interval virtuallink_hello_interval ] [ retransmit-interval virtuallink_retransmit_interval ] [ transmit-delay virtuallink_transmit_delay ]

Disables authentication for the specified area.

```bash
decimal_value | ipv4address
```

- `decimal_value` specifies the identification number of the area where authentication will be enabled as an integer from 0 through 4294967295.
- `ipv4address`: Specifies the IP address of the area where authentication will be enabled in IPv4 dotted-decimal notation.

```bash
default-cost default_integer_value
```

Sets the OSPFV3 authentication area’s default cost as an integer from 1 through 16777215.

```bash
stub [ no-summary ]
```

Sets the OSPFV3 stub area. Only Router-LSAs, Network-LSAs, Inter-area Prefix-LSAs, Intra-area Prefix-LSAs and Link-LSAs are allowed in a Stub area.

```bash
no-summary
```

Does not inject inter-area routes into stub area.

```bash
virtual-link virtuallink_neighbour_Ipv4_address
```

Configures a virtual link to the authentication area.

```bash
virtuallink_neighbour_Ipv4_address
```

Is the IPv4 address for the virtual link of the authenticated area in dotted-decimal notation.

The following interval timers can be set for the virtual link:
OSPFv3 Configuration Mode Commands

- **dead-interval virtuallink_dead_interval**: Sets the virtual link dead-interval (in seconds) as an integer from 1 through 65535.
- **hello-interval virtuallink_hello_interval**: Sets the virtual link hello interval (in seconds) as an integer from 1 through 65535.
- **retransmit-interval virtuallink_retransmit_interval**: Sets the virtual link retransmit interval (in seconds) as an integer from 1 through 3600.
- **transmit-delay virtuallink_transmit_delay**: Sets the virtual link transmit delay (in seconds) as an integer from 1 through 3600.

**Usage**

Use this command to establish OSPFv3 areas and enable authentication.

**Example**

The following command enables authentication for an OSPFv3 area defined by the IP address 192.168.100.10 with default cost of 256

```
area 192.168.100.10 default-cost 256
```
default-metric

Configures the default metric value for routes redistributed from another protocol into Open Shortest Path First Version 3 (OSPFv3).

**Product**
- PDSN
- HA
- GGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > OSPFv3 Configuration
configure > context context_name > router ospfv3

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-ospfv3)#
```

**Syntax**

```
[ no ] default-metric default_metric_integer_value
```

- **no**
  - Disables the default metric.

```
default_metric_integer_value
```

- Specifies the default metric as an integer from 1 through 16777214.

**Usage**
Use this command to configure OSPFv3 default metric.

**Example**
The following command configures OSPFv3 default metric to 256

```
default-metric 256
```
**end**

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
```
end
```

**Usage**
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
exit
```

Usage

Use this command to return to the parent configuration mode.
passive Interface

Configures an OSPFv3 passive interface as passive. If a network interface is configured as passive, it will not receive or send any OSPFv3 packets.

Product
PDSN
HA
GGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > OSPFv3 Configuration
configure > context context_name > router ospfv3

Entering the above command sequence results in the following prompt:

[local]host_name(config-ospfv3)#

Syntax

[ no ] passive-interface passive_interface_name

no
Disables the passive interface.

passive-interface passive_interface_name
Sets the named interface to be a passive interface as an alphanumeric string of 1 through 79 characters.

Usage

Use this command to configure an OPSFv3 passive interface in this context.

Example

The following command configures an OSPFv3 passive interface.

passive-interface OSPF-if1
**redistribute**

Redistributes routes from other protocols to OSPFv3 neighbors using the OSPFv3 protocol.

**Product**
- PDSN
- HA
- GGSN

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration > Context Configuration > OSPFv3 Configuration
- `configure > context context_name > router ospfv3`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ospfv3)#
```

**Syntax**

```
[ no ] redistribute { connected | static }

redistribute connected [ metric metric_value [ metric-type external_metric_type ] [ route-map route_map_name ] ] [ metric-type external_metric_type [ route-map route_map_name ] ] [ route-map route_map_name ]

static [ metric metric_value [ metric-type external_metric_type ] [ route-map route_map_name ] ] [ metric-type external_metric_type [ route-map route_map_name ] ] [ route-map route_map_name ]
```

- **no**
  Disables the route redistribution.

- **connected**
  Redistributes connected routes.

- **static**
  Redistributes static routes.

- **metric metric_value**
  Specifies the OSPFv3 default metric value as an integer from 0 through 16777214.

- **metric-type external_metric_type**
  Specifies the OSPFv3 external metric type as the integer 1 or 2

- **route-map route_map_name**
  Specifies a route map as an alphanumerical string of 1 through 79 characters.
Usage
Use this command to configure OSPFv3 redistribution of connected or static routes.

Example
The following command configures OSPFv3 redistribution of connected routes.

```
redistribute connected metric 45 metric-type 1 route-map rt
```
router-id

Sets the OSPFv3 router ID for the Open Shortest Path First Version 3 (OSPFv3) routing process.

**Product**
- PDSN
- HA
- GGSN

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration > Context Configuration > OSPFv3 Configuration
- `configure > context context_name > router ospfv3`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ospfv3)#
```

**Syntax**

```
[ no ] router-id router_id_ipaddress
```

- **no**
  - Disables the router-id.

- **router_id_ipaddress**
  - Specifies the router-id an IPv4 address in dotted-decimal notation.

**Usage**

Use this command to configure OPSF v3 router id to the given IPv4 address.

**Example**

The following command configures OSPFv3 router id to the given IPv4 address.

```
router-id 11.22.22.21
```
**timers spf**

Sets OSPFv3 the delay in the time between the detection of a topology change and when the SPF algorithm actually runs.

**Product**
- PDSN
- HA
- GGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > OSPFv3 Configuration

```
configure > context context_name > router ospfv3
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ospfv3)#
```

**Syntax**

```
[ no ] timers spf spf_delay_timer_value
```

- **no**
  Disables the SPF delay timer.

- **spf spf_delay_timer_value**
  Sets the Shortest Path First (SPF) delay timer (in milliseconds) as an integer from 0 through 4294967295.

**Usage**

Use this command to configure the OSPFv3 SPF delay timer.

**Example**

The following command sets OSPFv3 SPF timer.

```
timers spf 256
```
Chapter 231
OSPF VRF Configuration Mode Commands

The OSPF VRF Configuration sub-mode is used to configure the virtual routing and forwarding (VRF) context instances for OSPF routing protocol. This mode includes commands that configure VRF instance for OSPF routing parameters.

Mode

Exec > Global Configuration > Context Configuration > OSPF Configuration > OSPF VRF Configuration

configure > context context_name > router ospf > ip vrf vrf_name

Entering the above command sequence results in the following prompt:

[local] host_name(config-ospf-vrf) #

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
area

Configures various parameters, including authentication, area identification, virtual link ID, and delay/interval values for the specified OSPF area using a specific VRF instance.

Product

PDSN
HA
GGSN

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > Context Configuration > OSPF Configuration > OSPF VRF Configuration

configure > context context_name > router ospf > ip vrf vrf_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-ospf-vrf)#

Syntax

[no] area {decimal_value | ip_address} {authentication [message-digest] | default-cost cost_value | nssa [default-information-originate] [no-redistribution] [no-summary] [translate-always] [translate-candidate] [translate-never] | stub [no-summary] | virtual-link router_ip_address [authentication {message-digest | null | text}] [authentication-key {encrypted password encrypted_string | password password_string}] [message-digest-key key_id md5 [encrypted password encrypted_string | password password_string]] [dead-interval] [hello-interval] [retransmit-interval] [transmit-delay]

no

Disables or removes configured parameters for the specified OSPF area using a specific VRF instance.

ip_address

Specifies the IP address of the area where authentication will be enabled in IPv4 dotted-decimal notation.

decimal_value

Specifies the identification number of the area where parameters to be configured as an integer from 0 through 4294967295.

authentication

Sets the OSPF authentication type to use the simple authentication method.

message-digest

Sets the OSPF authentication type to use the message digest 5 (MD5) authentication method.

default-cost cost_value

Sets the default cost for an OSPF area. cost_value must be an integer from 0 through 16777215.
**nssa [default-information-originate] [no-redistribution no-summary] [translate-always] [translate-candidate] [translate-never]**

Configures and defines an area as an NSSA (Not So Stubby Area) and configures OSPF parameters for it.

- **default-information-originate**: Configures the OSPF VRF instances to originate default information to the NSSA area.
- **no-redistribution**: Configures the OSPF VRF instance to not to redistribute external routes to the NSSA area.
- **no-summary**: Configures the OSPF VRF instance to not to inject the inter-area routes into NSSA.
- **translate-always**: Configures the NSSA-ABR (Area Border Router) always to translate. By default this is disabled.
- **translate-candidate**: Configures the NSSA-ABR always to translate election. By default this is enabled.
- **translate-never**: Configures the NSSA-ABR never to translate. By default this is disabled.

**stub [no-summary]**

Specifies an OSPF area as an stub area configures the NSSA-ABR never to translate. By default this is disabled.
- **no-summary**: Disables (stops) the ABR from sending summary LSAs into the stub area.

**virtual-link router_id**

Specifies the router identifier which provides a virtual link between an area that cannot be physically connected to the network backbone and an area that is physically connected to the network backbone.
- **router_id**: Must be an IP address in IPv4 dotted-decimal notation of the ABR to be linked to.

**authentication {message-digest | null | text}**

Configures the OSPF authentication method to be used by the virtual link between an area that cannot be physically connected to the network backbone and an area that is physically connected to the network backbone.
- **message-digest**: Set the OSPF authentication type to use the message digest (MD) authentication method.
- **null**: Set the OSPF authentication type to use no authentication, thus disabling either MD or clear text methods.
- **text**: Set the OSPF authentication type to use the clear text authentication method.

**authentication-key**

Configures the authentication password for the virtual link between an area that cannot be physically connected to the network backbone and an area that is physically connected to the network backbone.

**message-digest-key key_id**

Specifies the MD key identifier number for virtual link connection. `key_id` must be an integer from 1 through 255.

**md5**

Sets the message digest to MD5 for virtual link connection.

**[encrypted] password passwd_string**

Specifies the password required for virtual link connection authentications. The keyword `password` is optional and if specified `passwd_string` must be an alphanumeric string of 1 through 63 characters. The password specified must be in an encrypted format if the optional keyword `encrypted` was specified.
The **encrypted** keyword is intended only for use by the system while saving configuration scripts. The system displays the **encrypted** keyword in the configuration file as a flag that the variable following the **password** keyword is the encrypted version of the plain text password. Only the encrypted password is saved as part of the configuration file. **encrypted_string** is an alphanumeric string of 1 through 523 characters.

---

### dead-interval value

Specifies the dead interval (in seconds) that the router should wait, during which time no packets are received and after the router considers a neighboring router to be off-line. **value** must be an integer from 1 through 65535.

---

### hello-interval value

Specifies the hello interval (in seconds) before sending a hello packet. **value** must be an integer from 1 through 65535.

---

### retransmit-interval value

Specifies the delay between retransmission (in seconds) that router should wait before retransmitting a packet. **value** must be an integer from 1 through 3600.

---

### transmit-delay value

Specifies the interval (in seconds) that the router should wait before transmitting a packet. **value** must be an integer from 1 through 3600.

---

### Usage

Use this command to configure/set the various network/connection/authentication parameters of OSPF areas using specific VRF instance.

### Example

The following command enables authentication for an OSPF area defined by the IP address 192.168.100.10 and the OSPF authentication type to MD5:

```
area 192.168.100.10 authentication message-digest
```

The following command defines the area designated by the IP address 192.168.100.10 as an NSSA area where translation of NSSA candidate is enabled by default:

```
area 192.168.100.10 nssa
```

The following command defines the OSPF area defined by the IP address 192.168.100.10 as a stub area:

```
area 192.168.100.10 stub
```

The following command creates a virtual link between the OSPF areas defined by the IP address 192.168.100.10 and the IP address 192.168.200.20:

```
area 192.168.100.10 virtual-link 192.168.200.20
```

The following command sets the authentication method for a virtual link between the OSPF areas defined by the IP address 192.168.100.10 and the IP address 192.168.200.20 to use no authentication:

```
area 192.168.100.10 virtual-link 192.168.200.20 null
```
The following command creates an authentication password of 123456 for a virtual link between the OSPF areas defined by the IP address 192.168.100.10 and the IP address 192.168.200.20:

```bash
area 192.168.100.10 virtual-link 192.168.200.20 authentication-key password 123456
```

The following command enables the use of MD5-based OSPF authentication for a virtual link between the OSPF areas defined by the IP address 192.168.100.10 and the IP address 192.168.200.20, sets the MD5 Key ID to 25, and the password to 123456:

```bash
area 192.168.100.10 virtual-link 192.168.200.20 message-digest-key 25 md5 password 123456
```

The following command sets the retransmit interval for a virtual link between the OSPF areas defined by the IP address 192.168.100.10 and the IP address 192.168.200.20 to 60 seconds:

```bash
area 192.168.100.10 virtual-link 192.168.200.20 retransmit-interval 60
```
default-information originate

Creates a default external route into an OSPF routing domain.

**Product**
- PDSN
- HA
- GGSN

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration > Context Configuration > OSPF Configuration > OSPF VRF Configuration

```
configure > context context_name > router ospf > ip vrf vrf_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ospf-vrf)#
```

**Syntax**

```
default-information originate

default-information originate [ always ] [ metric metric_value ] [ metric-type { 1 | 2 } ] [ route-map route_map_name ]
```

```
no default-information originate
```

- **no**
  
  Disables the default external route.

- **always**
  
  Always advertise the route regardless of whether or not the software has a default route.

- **metric metric_value**
  
  Sets the OSPF metric used in creating the default route as an integer from 1 through 16777214.

- **metric-type { 1 | 2 }**
  
  Sets the default route metric type.
  1: Sets the OSPF external link type for default routes to Type 1.
  2: Sets the OSPF external link type for default routes to Type 2.

- **route-map route_map_name**
  
  Specifies the name of the default route-map to be use as an alphanumeric string of 1 through 79 characters.

**Usage**

Use this command to set the default external route into an OSPF routing domain.
Example

The following command sets the default external route to originate from the route map named `rmap1`:

```
default-information originate route-map rmap1
```
**default metric**

Configures the default metric value for the OSPF routing protocol.

**Product**
- PDSN
- HA
- GGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > OSPF Configuration > OSPF VRF Configuration
```
configure > context context_name > router ospf > ip vrf vrf_name
```

Entering the above command sequence results in the following prompt:
```
[local]host_name(config-ospf-vrf)#
```

**Syntax**

```
default-metric metric_value
default-metric
```

Sets the metric value expressed as an integer from 1 through 16777214. The default metric value setting is 26385.

```
no
```

Enables or disables the default metric value for OSPF.

**Usage**
Use this command to set the default metric for routes.

**Example**
The following command sets the default metric to 235:
```
default-metric 235
```
distance

Configures the OSPF route administrative distances for all OSPF route types or based on specific route type. Administrative distance is the measure used by Cisco routers to select the best path when there are two or more different routes to the same destination from two different routing protocols. Administrative distance defines the reliability of a routing protocol. Each routing protocol is prioritized in order of most to least reliable (believable) using an administrative distance value. A lower numerical value is preferred.

Product
PDSN
HA
GGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > OSPF Configuration > OSPF VRF Configuration
configure > context context_name > router ospf > ip vrf vrf_name

Entering the above command sequence results in the following prompt:
[local]host_name(config-ospf-vrf)#

Syntax

\[ no \] distance \{ distance_value | ospf \{ [ external distance_value ] [ inter-area distance_value ] [ intra-area distance_value ] \} \}

no
Disables the OSPF route administrative distances for all OSPF route types.

distance_value
Specifies the OSPF route administrative distances as an integer from 1 to 255. The default distance value is 110.

ospf \{ [ external distance_value ] [ inter-area distance_value ] [ intra-area distance_value ] \}
Set the distance value for the specified route type.
external distance_value: Set the OSPF route administrative distance for routes from other routing domains, learned by redistribution. This must be an integer from 1 through 255. The default is 110.
inter-area distance_value: sets the OSPF route administrative distance for routes from one routing area to another. This must be an integer from 1 through 255. The default is 110.
intra-area distance_value: sets the OSPF route administrative distance for all routes within an area. This must be an integer from 1 through 255. The default is 110.

no
Enables or disables the specified option.
**Usage**

Use this command to set the administrative distance for OSPF routes.

**Example**

The following command sets the administrative distance for all OSPF route types to **30**:

```
   distance 30
```
**distribute-list**

Enables or disables the filtering of networks in outgoing routing updates.

**Product**

PDSN  
HA  
GGSN  

**Privilege**

Security Administrator, Administrator  

**Mode**

Exec > Global Configuration > Context Configuration > OSPF Configuration > OSPF VRF Configuration  
`configure > context context_name > router ospf > ip vrf vrf_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ospf-vrf)#
```

**Syntax**

```
[ no ] distribute-list route_access_list out { connected | rip | static }
```

- **no**  
  Disables the filtering of networks in outgoing routing updates.

- **route_access_list**  
  Specifies the name of the OSPF route access list to use for filtering as an alphanumeric string of 1 through 63 characters.

- **connected**  
  Filters connected routes.

- **rip**  
  Filters RIP routes. (RIP is not supported at this time.)

- **static**  
  Filters static routes.

- **no**  
  Disables the specified option.

**Usage**

Use this command to enable the filtering of outgoing route updates by using the specified route access list.

**Example**


The following command uses the route access list named `ral1` to filter outgoing routing updates for all connected routes:

```
distribute-list ral1 out connected
```
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
dec
```

**Usage**

Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Use this command to return to the parent configuration mode.
neighbor

Configures OSPF routers that interconnect to non-broadcast networks.

Product
PDSN
HA
GGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > OSPF Configuration > OSPF VRF Configuration

configure > context context_name > router ospf > ip vrf vrf_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-ospf-vrf)#

Syntax

no neighbor ip_address [ poll-interval poll_interval_value ] [ priority priority_value ]

no
Disables OSPF routers that interconnect to non-broadcast networks.

ip_address
Specifies the interface IP address of the OSPF neighbor expressed using IPv4 dotted-decimal notation.

poll-interval poll_interval_value
Default: 120
Sets the number of seconds in the dead neighbor polling interval as an integer from 1 through 65535

priority priority_value
Default: 0
Sets the 8-bit number that represents the router priority value of the non-broadcast neighbor associated with the specified IP address. This must be an integer from 0 through 255. This keyword does not apply to point-to-multipoint interfaces.

Usage
Use this command to configure OSPF routers that connect to non-broadcast networks.

Example

The following command specifies an OSPF router neighbor with the IP address of 192.168.100.10:

neighbor 192.168.100.10
**network area**

Enables OSPF on an interface and defines the OSPF area for that network.

**Product**
- PDSN
- HA
- GGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > OSPF Configuration > OSPF VRF Configuration

```
configure > context context_name > router ospf > ip vrf vrf_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ospf-vrf)#
```

**Syntax**

```
[ no ] network network_ip_address / network_mask area { area_id | area_ip_address }
```

- **no**
  Disables OSPF on an interface and defines the OSPF area for that network.

- **network_ip_address/network_mask**
  Specifies the network address and mask as well as the interface on which OSPF will be enabled.
  *network_ip_address* entered in IPv4 dotted-decimal notation, followed by the “/” and the mask (CIDR).

- **area_id**
  Specifies the OSPF area identification number for the specified network as an integer from 0 through 4294967295.

- **area_ip_address**
  Specifies the IP address of the OSPF area for this network. This must be entered in IPv4 dotted-decimal notation.

**Usage**

Use this command to specify the IP address of the network interface that the OSPF router will use.

**Example**

The following command specified that the OSPF router will use the interface at IP address 192.168.1.0 with a netmask of 24:

```
network 192.168.1.0/24
```
**ospf router-id**

Configures the router ID for the OSPF process.

**Product**
- PDSN
- HA
- GGSN

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration > Context Configuration > OSPF Configuration > OSPF VRF Configuration
- `configure > context context_name > router ospf > ip vrf vrf_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ospf-vrf)#
```

**Syntax**

```
ospf router-id ip_address
no ospf router-id ip_address
```

- `no`
  - Disables `ospf router-id`.
- `ip_address`
  - Specifies the router ID for the OSPF process as an IP address entered using IPv4 dotted-decimal notation

**Usage**

Use this command to set the router ID for the current OSPF router process.

**Example**

The following command sets the router ID to 192.168.200.1:

```
ospf router-id 192.168.200.1
```
passive-interface

Enables or disables the suppression of OSPF routing updates on the specified interface.

Product
PDSN
HA
GGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > OSPF Configuration > OSPF VRF Configuration
configure > context context_name > router ospf > ip vrf vrf_name

Entering the above command sequence results in the following prompt:
[local]host_name(config-ospf-vrf)#

Syntax

[ no ] passive-interface interface_name

no
Disables the name assigned to a logical interface within the specific context.

interface_name
Specifies the name assigned to a logical interface within the specific context as an alphanumeric string of 1 through 79 characters.

Usage
Use this command to suppress router updates on an interface in the current context.

Example
The following command suppresses OSPF routing updates on the interface named Intfcl:

    passive-interface Intfcl
**redistribute**

Redistributes routes from other protocols to OSPF neighbors using the OSPF protocol.

**Product**
- PDSN
- HA
- GGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > OSPF Configuration > OSPF VRF Configuration

```
configure > context context_name > router ospf > ip vrf vrf_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ospf-vrf)>
```

**Syntax**

```
redistribute { connected | rip | static } [ metric metric_value ] [ metric-type { 1 | 2 } ] [ route-map route_map_name ]
```

**no redistribute { connected | rip | static }**

- **no**
  Disables the redistributed routes.

- **connected**
  Redistributes connected routes.

- **rip**
  Specifies that RIP routes will be redistributed. (RIP is not supported at this time.)

- **static**
  Redistributes static routes.

- **metric metric_value**
  Sets the OSPF metric used in the redistributed route. This must be an integer from 1 through 16777214.

- **metric-type { 1 | 2 }**
  Default: 2
  Sets route metric type that is applied to redistributed routes.
  1: Sets the OSPF external link type for routes to Type 1.
  2: Sets the OSPF external link type for routes to Type 2.
route-map route_map_name

Filter routes through the specified route map before redistribution. `route_map_name` specifies the name of the route-map to use as an alphanumeric string of 1 through 79 characters.

Usage

Use this command to define what routing protocols should have their routes redistributed into OSPF.

Example

The following command defines that BGP routes should be redistributed:

```
redistribute connected
```
refresh timer

Adjusts settings for the OSPF refresh timer.

Product
PDSN
HA
GGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > OSPF Configuration > OSPF VRF Configuration
configure > context context_name > router ospf > ip vrf vrf_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-ospf-vrf)#

Syntax

[ no ] refresh timer value

| no          | Disables the refresh timer. |
| value       | Default: 10                  |
|             | Specifies the minimum amount of time (in seconds) to wait before refreshing a Link-state Advertisement (LSA). This must be an integer from 10 through 1800. |

Usage
Use this command to define the amount of time to wait before refreshing an LSA.

Example
The following command sets the refresh timer to 90 seconds:

    refresh timer 90
**router-id**

Configures the router ID for the OSPF process.

**Product**
- PDSN
- HA
- GGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > OSPF Configuration > OSPF VRF Configuration

```
configure > context context_name > router ospf > ip vrf vrf_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ospf-vrf)#
```

**Syntax**

```
[ no ] router-id ip_address
```

- **no**
  Disables the router ID for the OSPF process.

- **ip_address**
  Specifies the router ID for the OSPF process in IPv4 dotted-decimal notation.

**Usage**

Use this command to set the router ID for the current OSPF router process.

**Example**

The following command sets the router ID to `192.168.200.1`:

```
router-id 192.168.200.1
```
timers spf

Sets the Shortest Path First (SPF) timers.

**Product**
PDSN
HA
GGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > OSPF Configuration > OSPF VRF Configuration

```
configure > context context_name > router ospf > ip vrf vrf_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ospf-vrf)#
```

**Syntax**

```
timers spf delay_value hold_time_value
```

```
no timers spf
```

**Usage**
Use this command to set the SPF delay and hold timers for the current OSPF router process.

**Example**
The following command sets the delay timer to 15 and the hold timer to 15:

```
timers spf 15 15
```
Chapter 232
Out-Address Configuration Mode Commands

The Out-Address configuration mode provides the commands to configure the outbound parameters for the SCCP entities as part of the gtt-address-map configuration.

Mode

Exec > Global Configuration > GTT Address-Map Configuration > Out-Address Configuration

```
configure > gtt address-map map_id > out-address address_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-gtt-addrmmap-outaddr-out_address)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
end

Exits the configuration mode and returns to the Exec mode.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Change the mode back to the Exec mode.
exit

Exits the configuration mode and returns to the Global configuration mode.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**
```
exit
```

**Usage**
Return to the Global configuration mode.
gt-address

Configures the SCCP short address.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > GTT Address-Map Configuration > Out-Address Configuration

configure > gtt address-map map_id > out-address address_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-gtt-addrmap-outaddr-out_address)#

Syntax

gt-address gt_address

    gt_address
    A string of 1 to 15 digits to define the GT-address

Usage
Define the GT-address

Example

gt-address 010405525397
**gt-format**

The GT-format provides four formats that can be used during GTT.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > GTT Address-Map Configuration > Out-Address Configuration

```bash
configure > gtt address-map map_id > out-address address_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-gtt-addrmapp-outaddr-out_address)#
```

**Syntax**

```bash
gt-format format_num
```

- **format_num**
  1: Selects GT-format 1 options which include `nature-of-address` and `odd/even`. Once selected, the system enters GT-Format1 configuration mode.
  2: Selects GT-format2 options which include `translation-type`. Once selected, the system enters GT-Format2 configuration mode.
  3: Selects GT-format3 options which include `encoding-scheme`, `numbering-plan3` and `translation-type`. Once selected, the system enters GT-Format1 configuration mode.
  4: Selects GT-format4 options which include `encoding-scheme`, `nature-of-address`, `numbering-plan`, and `translation-type`. Once selected, the system enters GT-Format4 configuration mode.

**Usage**
Select the a GT-format that include encoding-scheme as part of the GTT process.

**Example**

```bash
gt-format 3
```
ni-indicator

Configures the National and International indicator to use during the GTT process.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > GTT Address-Map Configuration > Out-Address Configuration

```
configure > gtt address-map map_id > out-address address_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-gtt-addrmap-outaddr-out_address)#
```

**Syntax**

```
ni-indicator ni_ind
```

- **ni_ind**

  Select one of the following as the appropriate type of national indicator for the address structure:
  - *national*
  - *international*

**Usage**

Select the international indicator to be used for out-going addresses.

**Example**

```
ni-indicator international
```
point-code

Selects and configures the SS7-type point code for use with the out-going address.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > GTT Address-Map Configuration > Out-Address Configuration

```bash
configure > gtt address-map map_id > out-address address_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-gtt-addrmdep-outaddr-out_address)#
```

**Syntax**

```
point-code pt_code
```

<table>
<thead>
<tr>
<th>pt_code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter 1 to 11 digits in the point code format predefined during variant selection of GTT association.</td>
</tr>
</tbody>
</table>

**Usage**
Define an ITU point code to be used for out-going address processing.

**Example**

```bash
point-code 6.255.6
```
routing-indicator

Selects the type of routing and the indicator to be included in the out-going message.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > GTT Address-Map Configuration > Out-Address Configuration

`configure > gtt address-map map_id > out-address address_name`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-gtt-addrrmap-outaddr-out_address)#
```

**Syntax**

```
routing-indicator routing_ind
```

<table>
<thead>
<tr>
<th>routing_ind</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>gt</td>
<td>Inserts an indicator that identifies routing based on global title.</td>
</tr>
<tr>
<td>ssn</td>
<td>Inserts an indicator that identifies routing based on the subsystem number.</td>
</tr>
</tbody>
</table>

**Usage**
Select global title as the appropriate routing indicator.

**Example**
```
routing-indicator gt
```
ssf

Selects the subservice field as factor in the out-going address processing. ssf sets the network indicator in the subservice field for SS7 Message Signal Units (MSUs). The indicator carried in the message’s routing information typically identifies the structure of the point code as a message from within a nation or as a message coming from outside the national - international.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > GTT Address-Map Configuration > Out-Address Configuration

configure > gtt address-map map_id > out-address address_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-gtt-addrmapping-outaddr-out_address)#

Syntax

ssf sub_svc_fld

sub_svc_fld

Select one of the following options:

• international: The network indicator identifies the message as international with a point code structure that does not match the national point code structure,

• national: The network indicator identifies the messages as having a national point code structure.

• reserved: Provides an alternate network indicator for national messages.

• spare: Provides an alternate network indicator for international messages.

Usage

Select the international NI for inclusion in out-going address subservice fields.

Example

ssf international
**ssn**

Selects the subsystem number to be included in the out-going message.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > GTT Address-Map Configuration > Out-Address Configuration

```bash
configure > gtt address-map map_id > out-address address_name
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-gtt-addrmap-outaddr-out_address)#
```

**Syntax**

```bash
ssn sub_sys_num
```

<table>
<thead>
<tr>
<th>sub_sys_num</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter an integer from 1 to 255.</td>
</tr>
</tbody>
</table>

**Usage**

Use subsystem number 44 in the out-going address.

**Example**

```bash
ssn 44
```
Chapter 233
PCC-Action-Set Configuration Mode Commands

The PCC-Action-Set Configuration Mode provides the parameters to indicate the policy and charging as well as event generation related decisions that will get activated when the corresponding PCC-Condition-Group is evaluated to TRUE within a profile. A maximum of 32 actions can be configured in an instance of PCC-Action-Set.

**Important:** This configuration mode is supported from StarOS Release 12.1 onward.

Mode

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Action-Set Configuration

```
configure > context context_name > pcc-service service_name > action-set action_set_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-action-set)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
af-media-type

This command is used to set the action to be taken when specific media type is received from Application Function (AF) over Rx interface.

Product
IPCF

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Action-Set Configuration

configure > context context_name > pcc-service service_name > action-set action_set_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pcc-action-set)#

Syntax

[ no ] af-media-type {application | audio | control | data | message | other | text | video} {qos-profile qos_profile_value} {gate-status {disabled | enabled | enabled-downlink | enabled-uplink}} | {gate-status {disabled | enabled | enabled-downlink | enabled-uplink} [qos-profile qos_profile_value]} | [monitoring-key mon_key_id]

no
Removes the configured action set for different type of AF media in a PCC-Action-Set configuration instance for PCC-Service configuration.

application
Sets the AF media type to ‘application’ data traffic for various action configuration under PCC-Action-Set configuration instance for PCC-Service configuration.

audio
Sets the AF media type to ‘audio’ data traffic for various action configuration under PCC-Action-Set configuration instance for PCC-Service configuration.

control
Sets the AF media type to ‘control’ signal for various action configuration under PCC-Action-Set configuration instance for PCC-Service configuration.

data
Sets the AF media type to ‘data’ for various action configuration under PCC-Action-Set configuration instance for PCC-Service configuration.

message
Sets the AF media type to ‘message’ data for various action configuration under PCC-Action-Set configuration instance for PCC-Service configuration.
other
Sets the AF media type to ‘other’, out of AF media type configured here, for various action configuration under PCC-Action-Set configuration instance for PCC-Service configuration.

text
Sets the AF media type to ‘text’ for various action configured under PCC-Action-Set configuration instance for PCC-Service configuration.

video
Sets the AF media type to ‘video’ for various action configured under PCC-Action-Set configuration instance for PCC-Service configuration.

qos-profile qos_profile_value
Associate the pre-defined PCC-QoS-Profile for specific AF media type for various action configured for PCC-Service configuration.
qos_profile_value is name of the pre-defined PCC-QoS-Profile in PCC-Service Configuration instance.

gate-status {disabled | enabled | enabled-downlink | enabled-uplink}
Default: Enabled
Associate the status of Gate for specific AF media type for various action configured for PCC-Service configuration.
disabled: disables the Gate status in downlink and uplink direction for specific type of AF media type along optionally with PCC-QoS-Profile in PCC-Service Configuration instance.
enabled: Enables the Gate status in downlink and uplink direction for specific type of AF media type along optionally with PCC-QoS-Profile in PCC-Service Configuration instance. This is the default status of Gate.
enabled-downlink: Enables the Gate status in downlink direction for specific type of AF media type along optionally with PCC-QoS-Profile in PCC-Service Configuration instance.
enabled-uplink: Enables the Gate status in uplink direction for specific type of AF media type along optionally with PCC-QoS-Profile in PCC-Service Configuration instance.

monitoring-key mon_key_id
Specifies the Monitoring Key identifier to be associated with AF-Media-type under PCC-Action-Set configuration instance for PCC-Service configuration.
mon_key_id must be a preconfigured monitoring key having integer between 1 through 65535.

Usage
Use this command to set the action to be taken when specific media type is received from Application Function (AF) over Rx interface.
It also associates the pre-defined PCC-QoS-Profile and Gate function and monitoring key with specific media type.

Example
The following command sets the AF media type to ‘video’ with PCC-QoS-Profile named video_qos1 with gate status enabled in downlink and uplink traffic for various action configured under PCC-Action-Set configuration instance for PCC-Service configuration:

af-media-type video qos-profile video_qos1 gate-status enabled
associate monitoring-key

This command associates a Monitoring Key id with a PCC-Usage-Monitor in PCC-Action-Set configuration for PCC-Service instance.

Product
IPCF

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Action-Set Configuration

configure > context context_name > pcc-service service_name > action-set action_set_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pcc-action-set)#

Syntax

[no] associate monitoring-key mon_key_id usage-monitor usage_mon_name

no
Removes the associated Monitoring Key id configuration along with the association to PCC-Usage-Monitor from a PCC-Action-Set configuration instance for PCC-Service configuration.

mon_key_id
Specifies the Monitoring Key identifier to be associated with PCC-Usage-Monitor under PCC-Action-Set configuration instance for PCC-Service configuration.

mon_key_id must be an integer between 1 through 65535.

usage-monitor usage_mon_name

Specifies the PCC-Usage-Monitor associated with Monitoring Key mon_key_id under PCC-Action-Set configuration instance for PCC-Service configuration.

usage_mon_name is a pre-configured PCC-Usage-Monitor instance in PCC-Service Profile Configuration for PCC-Service configuration.

Usage

Use this command to associate a Monitoring Key with a PCC-Usage-Monitor in PCC-Action-Set configuration for PCC-Service instance.

There is a Many-To-Many relationship between Usage-Monitor and Monitoring-Key. Operator can change this relationship using required command.

When usage is reported to IPCF for a particular Monitoring Key, the usage is added to all the Usage Monitoring to which the Monitoring Key is associated.

Operator can break the relationship between Monitoring Key and Usage Monitor by dissociate monitoring-key command.

Example

The following command associates Monitoring Key id 102 with pre-defined PCC-Usage-Monitor named usage_mon1 under PCC-Action-Set configuration instance for PCC-Service configuration:
associate monitoring-key 102 usage-monitor usage_mon1
authorize

This command sets an action to change the various authorization parameters used for the IP-CAN session under PCC-Action-Set configuration instance for PCC-Service configuration.

**Product**
IPCF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Action-Set Configuration

configure > context context_name > pcc-service service_name > action-set action_set_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pcc-action-set)#

**Syntax**

```
[no] authorize {apn-mbr | default-eps-bearer | qci qci_value} qos-profile qos_prof_name
```

- **no**
  Removes the configured action for QoS Profile authorization parameters from PCC-Action-Set configuration instance for PCC-Service configuration.

- **apn-mbr**
  Sets the action for QoS authorization of Maximum Bit Rate (MBR) at APN through a pre-configured QoS profile name `qos_prof_name` which is to use for the authorization at different level in an PCC-Service instance.
  This keyword is applicable only to EPS access type. MBR Download and MBR Upload values of the QoS profile is used with this authorization.

- **default-eps-bearer**
  Sets the action QoS authorization of the Default EPS bearer in an EPS access network through a pre-configured QoS profile name `qos_prof_name` which is to use for the authorization at different level in an PCC-Service instance.
  This keyword is applicable only to EPS access type. QoS Class Identifier (QCI) and Allocation and Retention Priority (ARP) values of the QoS profile is used with this authorization.

- **qci qci_value**
  Sets the action QoS authorization per QCI in case of PCEF binding through a pre-configured QoS profile name `qos_prof_name` which is to use for the authorization at different level in an PCC-Service instance.
  `qci_value` must be an integer value between 1 through 255.

**Important:** This keyword is applicable only in case of PCEF binding. QCI defined in QoS profile is not used when this keyword is active, so this keyword is repeated per QCI that has to be authorized by IPCF. For each QCI authorization Maximum Bit Rate Upload/Download (MBR DL/MBR UL) or Guaranteed Bit Rate Upload/Download (GBR DL/MBR UL) and ARP values of the QoS profile is used with this authorization.
authorize qos-profile qos_prof_name

This keyword associates the action configured for authorization with a pre-configured PCC-QoS-Profile named qos_prof_name and uses configured values from specific PCC-QoS-Profile during authorization. qos_prof_name specifies the pre-configured QoS profile name which is to use for the authorization at different level in an PCC-Service instance.

Usage

Use this command to define an action for the authorization parameters in PCC-QoS-Profile which is to be used under PCC-Action-Set configuration instance for PCC-Service configuration.

Example

Following command sets the action for QoS authorization for APN MBR with PCC-QoS-Profile apn_qos_prof1 under PCC-Action-Set configuration instance for PCC-Service configuration.

authorize apn-mbr qos-profile apn_qos_profile apn_qos_prof1
dissociate monitoring-key

This command dissociates a Monitoring Key id with a PCC-Usage-Monitor in PCC-Action-Set configuration for PCC-Service instance.

**Product**

IPCF

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Action-Set Configuration

configure > context context_name > pcc-service service_name > action-set action_set_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-action-set)#
```

**Syntax**

```
[no] dissociate monitoring-key mon_key_id usage-monitor usage_mon_name
```

- **[no]**
  - Removes the dissociated Monitoring Key id configuration from a PCC-Action-Set configuration instance for PCC-Service configuration.

- **mon_key_id**
  - Specifies the Monitoring Key identifier to be dissociated with PCC-Usage-Monitor under PCC-Action-Set configuration instance for PCC-Service configuration.
  - `mon_key_id` must be an integer between 1 through 65535.

- **usage-monitor usage_mon_name**
  - Specifies the PCC-Usage-Monitor need to be dissociated with Monitoring Key `mon_key_id` under PCC-Action-Set configuration instance for PCC-Service configuration.
  - `usage_mon_name` is a pre-configured PCC-Usage-Monitor instance in PCC-Service Profile Configuration for PCC-Service configuration.

**Usage**

Use this command to dissociate a Monitoring Key with a PCC-Usage-Monitor in PCC-Action-Set configuration for PCC-Service instance.

There is a Many-To-Many relationship between Usage-Monitor and Monitoring-Key. Operator can change this relationship using required commands.

When usage is reported to IPCF for a particular Monitoring Key, the usage is added to all the Usage Monitoring to which the Monitoring Key is associated.

Operator can reassociate the relationship between Monitoring Key and Usage Monitor by `associate monitoring-key` command.

**Example**

The following command dissociates a associated pair of Monitoring Key id 102 and PCC-Usage-Monitor named `usage_mon1` under PCC-Action-Set configuration instance for PCC-Service configuration:
dissociate monitoring-key 102 usage-monitor usage_mon1
dynamic-rule-install

This command sets an action to install a PCC Dynamic rule for the specified PCC-Data-service in PCC-Action-Set configuration for PCC-Service instance.

Product
IPCF

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Action-Set Configuration

configure > context context_name > pcc-service service_name > action-set action_set_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pcc-action-set)#

Syntax

[no] dynamic-rule-install data-service data_svc_name [qos-profile qos_prof_name]
[precedence preced_value] [monitoring-key mon_key_id [rating-group rating_grp_id] [gate-status [disabled | enabled | enabled-downlink | enabled-uplink]] [defer-by interval delayed_dur] [metering-method {both-duration-volume | duration | volume}] [reporting-level {service-identifier-level | rating-group-level}] [failure-policy { continue | terminate }]

no

Removes the Dynamic Rule install action configured for specific PCC-Data-Service from a PCC-Action-Set configuration instance for PCC-Service configuration.

data-service data_svc_name

Specifies the name of the pre-configured PCC-Data-Service for which Dynamic Rules to be installed under PCC-Action-Set configuration instance for PCC-Service configuration.

data_svc_name is a pre-configured PCC-Data-Service instance in PCC-Service Configuration mode.

metering-method {both-duration-volume | duration | volume}

Specifies the reporting level to be used by PCEF to report the data usage for the related PCC rule in a PCC-Data-service instance on IPCF node.

• both-duration-volume sets the metering method as based on volume of data usage and duration of session, both for offline charging in a PCC-Data-service instance on IPCF node.

• duration sets the metering method as based on duration of session usage for offline charging in a PCC-Data-service instance on IPCF node.

• volume sets the metering method as based on the volume of data usage for offline charging in a PCC-Data-service instance on IPCF node.

If no metering method is defined, the reporting level preconfigured at PCEF is considered.
monitoring-key *mon_key_id*

Specifies the pre-defined Monitoring Key identifier which is to be used in Dynamic Rule for specific PCC-Data-service under PCC-Action-Set configuration instance for PCC-Service configuration.

*mon_key_id* is a pre-defined Monitoring Key identifier in PCC-Service Configuration mode.

precedence *preced_value*

Specifies the precedence value for the Dynamic Rule for specific PCC-Data-service under PCC-Action-Set configuration instance for PCC-Service configuration.

*preced_value* must be an integer between 1 through 65535.

qos-profile *qos_prof_name*

Specifies the name of the pre-configured PCC-QoS-Profile which is to be used in Dynamic Rule for specific PCC-Data-Service under PCC-Action-Set configuration instance for PCC-Service configuration.

*qos_prof_name* is a pre-configured PCC-QoS-Profile instance in PCC-Service Configuration mode.

rating-group *rating_grp_id*

Specifies the pre-defined Rating Group identifier which is to be used in Dynamic Rule for specific PCC-Data-service under PCC-Action-Set configuration instance for PCC-Service configuration.

*rating_grp_id* is a pre-defined Rating Group identifier in PCC-Service Configuration mode.

reporting-level {service-identifier-level | rating-group-level}

Specifies the reporting level to be used by PCEF to report the data usage for the related PCC rule in a PCC-Data-service instance on IPCF node.

  • *service-identifier-level* sets the data usage reporting level to be used by PCEF to report the data usage for the related PCC rule at the Service Identifier level which is configured in a PCC-Data-service instance on IPCF node.

  • *rating-group-level* sets the data usage reporting level to be used by PCEF to report the data usage for the related PCC rule at the Rating Group level which is configured in a PCC-Data-service instance on IPCF node.

If no reporting level is defined, the reporting level preconfigured at PCEF is considered.

gate-status {disabled | enabled | enabled-downlink | enabled-uplink}

Default: Enabled

Sets the Gate-status which is to be used in Dynamic Rule for specific PCC-Data-Service under PCC-Action-Set configuration instance for PCC-Service configuration.

*disabled*: disables the Gate status in downlink and uplink direction which is to be used in Dynamic Rule for specific PCC-Data-Service under PCC-Action-Set configuration instance for PCC-Service configuration.

*enabled*: Enables the Gate status in downlink and uplink direction which is to be used in Dynamic Rule for specific PCC-Data-Service under PCC-Action-Set configuration instance for PCC-Service configuration. This is the default status of Gate.

*enabled-downlink*: Enables the Gate status in downlink direction which is to be used in Dynamic Rule for specific PCC-Data-Service under PCC-Action-Set configuration instance for PCC-Service configuration.

*enabled-uplink*: Enables the Gate status in uplink direction which is to be used in Dynamic Rule for specific PCC-Data-Service under PCC-Action-Set configuration instance for PCC-Service configuration.
**defer-by interval delayed_dur**

This optional keyword supports the time-of-day-based procedures under PCC-Action-Set instance by configuring the relative time delay for dynamic rule installation.

*delayed_dur* configures the relative delay time by which the corresponding dynamic rule installation is deferred. The action is triggered only when the time specified by *delayed_dur* is passed.

*delayed_dur* specifies the delayed interval in *HH MIN SS* format.

Following format is used for *HH MIN SS* in *delayed_dur*:

- **HH** specifies the hour to defer the action trigger and must be an integer between 00 through 23.
- **MIN** specifies the minutes to defer the action trigger and must be an integer between 00 through 59.
- **SS** specifies the seconds to defer the action trigger and must be an integer between 00 through 59.

**failure-policy { continue | terminate }**

Default: Continue

This optional keyword configures the rule failure policy action when failure occurs on PCEF for PCC rules.

- **Continue**: If this option enabled, the IPCF continues even if PCEF reports rule failure through charging rule report. This is the default action.

- **Terminate**: If this option enabled, the IPCF triggers PCC session termination on receiving rule failure through charging rule report.

**Usage**

Use this command to set an action to install a PCC Dynamic rule for the specified PCC-Data-Service in PCC-Action-Set configuration for PCC-Service instance

Operator can override parameters such as, QoS profile, Precedence, Gate-status, Monitoring Key and PCC-Rating-id.

The same command is used to modify already installed PCC Dynamic-rule for the PCC-Data-Service by overriding required parameters only.

Additionally **defer-by interval** keyword is used to configure relative time by which the corresponding dynamic rule installation is deferred.

IPCF handles operation of PCC Rule and activate/deactivate/install/modify/remove the PCC rules at PCEF through this configuration. PCC rule operation may fail on PCEF due to various reasons. In such failure cases PCEF sends back a Charging Rule Report containing name of the failed PCC rule and corresponding failure cause.

The IPCF handles these charging rule report and take appropriate actions based on configuration done through **failure-policy** keyword.

Charging Rule Report comes through CCA or RAA messages in a call flow used for handling the charging-rule-report.

IPCF supports following charging rule failure codes in report:

- Out-of-credit
- Reallocation-of-credit
- Unknown rule name
- Invalid Rating Group
- Invalid Service Identifier
- GW/PCEF Malfunction
• Limited Resources
• Max No. of Bearers Reached
• Unknown Bearer Id
• Missing Bearer Id
• Missing Flow Description
• Resource Allocation Failure
• QoS Validation Failure

Charging rule status can any one of the following in this scenario:
• Active
• Inactive
• Temporarily Inactive

A charging rule report can occur in CCR message multiple times and maximum of 16 charging rule reports per CCR message is supported by IPCF.

**Example**

The following command sets the action for PCC-Data-Service named `temp_data1` for Dynamic Rule install with PCC-QoS-Profile named `temp_qos1` having precedence 22 and Gate-status as **Enabled** under PCC-Action-Set configuration instance for PCC-Service configuration:

```
dynamic-rule-install data-service temp_data1 qos-profile temp_qos1 precedence 22
```
dynamic-rule-uninstall

This command sets an action to uninstall a Dynamic Rule for the specified PCC-Data-Service in PCC-Action-Set configuration for PCC-Service instance.

**Product**
IPCF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Action-Set Configuration

```bash
configure > context context_name > pcc-service service_name > action-set action_set_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-action-set)#
```

**Syntax**

```
[no] dynamic-rule-uninstall data-service data_svc_name [defer-by interval delayed_dur]
```

- **no**
  Removes the Dynamic Rule Uninstall action configured for specific PCC-Data-Service from a PCC-Action-Set configuration instance for PCC-Service configuration.

- **data-service** *data_svc_name*
  Specifies the name of the pre-configured PCC-Data-Service for which Dynamic Rules to be uninstalled under PCC-Action-Set configuration instance for PCC-Service configuration. *data_svc_name* is a pre-configured PCC-Data-Service instance in PCC-Service Configuration mode.

- **defer-by interval** *delayed_dur*
  This optional keyword supports the time-of-day-based procedures under PCC-Action-Set instance by configuring the relative time delay for dynamic rule removal. *delayed_dur* configures the relative delay time by which the corresponding dynamic rule uninstallation is deferred. The action is triggered only when the time specified by *delayed_dur* is passed. *delayed_dur* specifies the delayed interval in HH MIN SS format. Following format is used for HH MIN SS in *delayed_dur*:

  - **HH** specifies the hour to defer the action trigger and must be an integer between 00 through 23.
  - **MIN** specifies the minutes to defer the action trigger and must be an integer between 00 through 59.
  - **SS** specifies the seconds to defer the action trigger and must be an integer between 00 through 59.

**Usage**

Use this command to set an action to uninstall a PCC Dynamic rule for the specified PCC-Data-Service in PCC-Action-Set configuration for PCC-Service instance. Additionally **defer-by interval** keyword is used to configure relative time by which the corresponding dynamic rule uninstallation is deferred.
Example

The following command sets the action of Dynamic Rule uninstall for PCC-Data-Service named temp_data1 under PCC-Action-Set configuration instance for PCC-Service configuration:

```
dynamic-rule-uninstall data-service temp_data1
```
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
```
end
```

**Usage**
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
- All

Privilege
- Security Administrator, Administrator

Syntax

exit

Usage

Use this command to return to the parent configuration mode.
### log-event

This command allows operator to specify a string to be logged at Subscriber Service Controller (SSC) when the corresponding action set is triggered under PCC-Action-Set configuration for PCC-Service instance.

#### Product

IPCF

#### Privilege

Security Administrator, Administrator

#### Mode

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Action-Set Configuration  
`configure > context context_name > pcc-service service_name > action-set action_set_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-action-set)#
```

#### Syntax

```
[no] log-event msg-text message_string
```

- **no**
  
  Removes the notification message configured for specific action under a PCC-Action-Set configuration instance for PCC-Service configuration.

- **msg-text message_string**
  
  Specifies the message notification text string to be logged at the SSC when a particular PCC-Action-Set triggered for PCC-Service instance.  
  `message_string` is a string of alphanumerical characters of 1 through 255 characters

#### Usage

Use this command to allow operator to specify a string to be logged at Subscriber Service Controller (SSC) when the corresponding action set is triggered under PCC-Action-Set configuration for PCC-Service instance.

#### Example

The following command sets the notification message for an action under PCC-Action-Set configuration instance for PCC-Service configuration:

```
log-event msg-text "This Action is Applicable for EPS Session Only."
```
notify-user

This command allows operator to specify a string template-id at SSC under PCC-Action-Set configuration for PCC-Service instance.

**Product**
- IPCF

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Action-Set Configuration
- `configure > context context_name > pcc-service service_name > action-set action_set_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-action-set)#
```

**Syntax**

```
[no] notify-user message-id message_id [parameter value_pair]
```

- **no**
  - Removes the user notification message id configured for specific action under a PCC-Action-Set configuration instance for PCC-Service configuration.

- **message-id message_id**
  - Specifies the message template id stored at SSC to be used for user notification for action under PCC-Action-Set configuration for PCC-Service instance.
  - `message_id` is a string of alphanumerical characters of 1 through 255 characters

- **parameter value_pair**
  - Specifies the parameters in the form of name value pairs separated by comma. A maximum of 16 name value pairs can be defined for action under PCC-Action-Set configuration for PCC-Service instance.
  - The name value pairs is encoded into XML data like other parameters and sent out to SSC for user notification.
  - `value_pair` is a string of alphanumerical characters of 1 through 255 characters which can accommodate up to 16 name value pair separated by comma (,).

**Usage**

Use this command to allow operator to specify a string template-id under PCC-Action-Set configuration for PCC-Service instance.

The template description exists at SSC and when the corresponding action set is hit, the subscriber is notified with the specified template configured via this command.

The action set makes a XML remote procedure call towards SSC. The XML contains information like IMSI, template-id of the SMS/E-mail template and other details like MSISDN, NAI if available. To give more flexibility to the operator, now the this command accepts name value pairs, which are also sent along with the said data.

**Example**
The following command sets the message id “Invalid User.” for user notification message to an action under PCC-Action-Set configuration instance for PCC-Service configuration:

```
notify-user message-id "Invalid User."
```
**offline-charging-server**

This command sets the action to change the offline charging server applicable to an IP-CAN session under PCC-Action-Set configuration instance for PCC-Service configuration.

**Product**

IPCF

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Action-Set Configuration

```
configure > context context_name > pcc-service service_name > action-set action_set_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-action-set)#
```

**Syntax**

```
[no] offline-charging-server primary pri_serv_address [secondary sec_serv_address]
```

- **no**
  
  Removes the action set to change the offline charging server under PCC-Action-Set configuration instance for PCC-Service configuration.

- **primary pri_serv_address**
  
  Identifies the name of the primary offline charging server which is to be used for action to change under PCC-Action-Set configuration instance for PCC-Service configuration.
  
  The `pri_serv_address` must be the address of an offline charging server in Diameter URI format (`FQDN [port][transport][protocol]`).

- **secondary sec_serv_address**
  
  Identifies the name of the secondary offline charging server which is to be used for action to change under PCC-Action-Set configuration instance for PCC-Service configuration.
  
  The `sec_serv_address` must be the address of an offline charging server in Diameter URI format (`FQDN [port][transport][protocol]`).

**Usage**

Use this command to set an action to change the offline charging server applicable to an IP-CAN session under PCC-Action-Set configuration instance for PCC-Service configuration.

**Example**

Following command configures an action change the offline charging server to primary server `aaa://host.abc.com:6666;transport=tcp;protocol=diameter` and secondary server `aaa://host.xyz.com:6666;transport=sctp;protocol=radius` under PCC-Action-Set configuration instance for PCC-Service configuration:
offline-charging-server

offline-charging-server primary
aaa://host.abc.com:6666;transport=tcp;protocol=diameter

offline-charging-server secondary
aaa://host.xyz.com:6666;transport=sctp;protocol=radius
online-charging-server

This command sets the action to change the online charging server applicable to an IP-CAN session under PCC-Action-Set configuration instance for PCC-Service configuration.

**Product**

IPCF

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Action-Set Configuration

configure > context context_name > pcc-service service_name > action-set action_set_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pcc-action-set)#

**Syntax**

[no] online-charging-server primary pri_serv_address [secondary sec_serv_address]

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Removes the action set to change the online charging server under PCC-Action-Set configuration instance for PCC-Service configuration.</td>
</tr>
<tr>
<td>primary</td>
<td>Identifies the name of the primary online charging server which is to be used for action to change under PCC-Action-Set configuration instance for PCC-Service configuration. The pri_serv_address must be the address of an online charging server in Diameter URI format (FQDN [port][transport][protocol]).</td>
</tr>
<tr>
<td>secondary</td>
<td>Identifies the name of the secondary online charging server which is to be used for action to change under PCC-Action-Set configuration instance for PCC-Service configuration. The sec_serv_address must be the address of an online charging server in Diameter URI format (FQDN [port][transport][protocol]).</td>
</tr>
</tbody>
</table>

**Usage**

Use this command to set an action to change the online charging server applicable to an IP-CAN session under PCC-Action-Set configuration instance for PCC-Service configuration.

**Example**

Following command configures an action change the online charging server to primary server aaa://host.abc.com:6666;transport=tcp;protocol=diameter and secondary server aaa://host.xyz.com:6666;transport=sctp;protocol=radius under PCC-Action-Set configuration instance for PCC-Service configuration:
online-charging-server primary
aaa://host.abc.com:6666;transport=tcp;protocol=diameter
secondary
aaa://host.xyz.com:6666;transport=sctp;protocol=radius
request-usage-report monitoring-key

This command configures the action to allow operator to explicitly request usage report for the specified Monitoring Key or all Monitoring Keys under PCC-Action-Set configuration for PCC-Service instance.

**Product**
IPCF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Action-Set Configuration

```configure > context context_name > pcc-service service_name > action-set action_set_name```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-action-set)#
```

**Syntax**

```
[no] request-usage-report monitoring-key {mon_key_id | any}
```

- **no**
  Removes the usage request action configuration for Monitoring Key id from a PCC-Action-Set configuration instance for PCC-Service configuration.

- **mon_key_id**
  Specifies the Monitoring Key identifier for which usage report action is to be set under PCC-Action-Set configuration instance for PCC-Service configuration.
  
  - `mon_key_id` must be an integer between 1 through 65535.

- **any**
  Specifies the Monitoring Key identifier to “ANY” value for which usage report action is to be set under PCC-Action-Set configuration instance for PCC-Service configuration.

**Usage**

Use this command to configure the action to allow operator to explicitly request usage report for the specified Monitoring Key or all Monitoring Keys under PCC-Action-Set configuration for PCC-Service instance.

**Example**

The following command sets an action to request the usage report for Monitoring Key id 102 under PCC-Action-Set configuration instance for PCC-Service configuration:

```
request-usage-report monitoring-key 102
```
rule-activate

This command sets an action to activate a pre-configured Rule in PCC-Action-Set configuration for PCC-Service instance.

Product
IPCF

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Action-Set Configuration
configure > context context_name > pcc-service service_name > action-set action_set_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pcc-action-set)#

Syntax

[no] rule-activate rule_name[defer-by interval delayed_dur]

no
Removes the action to activate a pre-configured Rule from a PCC-Action-Set configuration instance for PCC-Service configuration.

rule_name
Specifies the name of the pre-configured Rule on PCEF for an activation action is set under PCC-Action-Set configuration instance for PCC-Service configuration.
rule_name is a pre-configured Rule in PCEF.

defer-by interval delayed_dur
This optional keyword supports the time-of-day-based procedures under PCC-Action-Set instance by configuring the relative time delay for rule activation. 
delayed_dur configures the relative delay time by which the corresponding rule activation is deferred. The action is triggered only when the time specified by delayed_dur is passed.
delayed_dur specifies the delayed interval in HH MIN SS format.
Following format is used for HH MIN SS in delayed_dur:

- HH specifies the hour to defer the action trigger and must be an integer between 00 through 23.
- MIN specifies the minutes to defer the action trigger and must be an integer between 00 through 59.
- SS specifies the seconds to defer the action trigger and must be an integer between 00 through 59.

Usage
Use this command to set an action to activate a pre-configured Rule in PCC-Action-Set configuration for PCC-Service instance.
Additionally defer-by interval keyword is used to configure relative time by which the corresponding rule activation is deferred.
PCC-Action-Set Configuration Mode Commands

Example

The following command sets an action to activate for Rule \texttt{rule1} under PCC-Action-Set configuration instance for PCC-Service configuration:

\begin{verbatim}
rule-activate rule1
\end{verbatim}
rule-deactivate

This command sets an action to deactivate a pre-configured Rule in PCC-Action-Set configuration for PCC-Service instance.

Product
IPCF

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Action-Set Configuration

configure > context context_name > pcc-service service_name > action-set action_set_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pcc-action-set)#

Syntax

[no] rule-deactivate rule_name [defer-by interval delayed_dur]

no
Removes the action to deactivate a pre-configured Rule from a PCC-Action-Set configuration instance for PCC-Service configuration.

rule_name
Specifies the name of the pre-configured Rule on PCEF for a deactivation action is set under PCC-Action-Set configuration instance for PCC-Service configuration.

rule_name is a pre-configured Rule in PCEF.

defer-by interval delayed_dur
This optional keyword supports the time-of-day-based procedures under PCC-Action-Set instance by configuring the relative time delay for rule deactivation.

delayed_dur configures the relative delay time by which the corresponding rule deactivation is deferred. The action is triggered only when the time specified by delayed_dur is passed.

delayed_dur specifies the delayed interval in HH MIN SS format.

Following format is used for HH MIN SS in delayed_dur:

• HH specifies the hour to defer the action trigger and must be an integer between 00 through 23.
• MIN specifies the minutes to defer the action trigger and must be an integer between 00 through 59.
• SS specifies the seconds to defer the action trigger and must be an integer between 00 through 59.

Usage
Use this command to set an action to deactivate a pre-configured Rule in PCC-Action-Set configuration for PCC-Service instance.

Additionally defer-by interval keyword is used to configure relative time by which the corresponding rule deactivation is deferred.
Example

The following command sets an action to deactivate for Rule `rule1` under PCC-Action-Set configuration instance for PCC-Service configuration:

```
rule-deactivate rule1
```
rulebase-activate

This command sets an action to activate a pre-configured Rulebase in PCC-Action-Set configuration for PCC-Service instance.

Product
IPCF

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Action-Set Configuration

configure > context context_name > pcc-service service_name > action-set action_set_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pcc-action-set)#

Syntax

[no] rulebase-activate rulebase_name [defer-by interval delayed_dur]

no

Removes the action to activate a pre-configured Rulebase from a PCC-Action-Set configuration instance for PCC-Service configuration.

rulebase_name

Specifies the name of the pre-configured Rulebase on PCEF for an activation action is set under PCC-Action-Set configuration instance for PCC-Service configuration.

rulebase_name is a pre-configured Rulebase in PCEF.

defer-by interval delayed_dur

This optional keyword supports the time-of-day-based procedures under PCC-Action-Set instance by configuring the relative time delay for Rulebase activation.

delayed_dur configures the relative delay time by which the corresponding Rulebase activation is deferred. The action is triggered only when the time specified by delayed_dur is passed.

delayed_dur specifies the delayed interval in HH MIN SS format.

Following format is used for HH MIN SS in delayed_dur:

- HH specifies the hour to defer the action trigger and must be an integer between 00 through 23.
- MIN specifies the minutes to defer the action trigger and must be an integer between 00 through 59.
- SS specifies the seconds to defer the action trigger and must be an integer between 00 through 59.

Usage

Use this command to set an action to activate a pre-configured Rulebase in PCC-Action-Set configuration for PCC-Service instance.

Additionally defer-by interval keyword is used to configure relative time by which the corresponding Rulebase activation is deferred.
Example

The following command sets an action to activate for Rulebase *rulebase1* under PCC-Action-Set configuration instance for PCC-Service configuration:

```
rulebase-activate rulebase1
```
**rulebase-deactivate**

This command sets an action to deactivate a pre-configured Rulebase in PCC-Action-Set configuration for PCC-Service instance.

**Product**
IPCF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Action-Set Configuration

```
configure > context context_name > pcc-service service_name > action-set action_set_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-action-set)#
```

**Syntax**

```
[no] rulebase-deactivate rulebase_name [defer-by interval delayed_dur]
```

- **no**
  Removes the action to deactivate a pre-configured Rulebase from a PCC-Action-Set configuration instance for PCC-Service configuration.

- **rulebase_name**
  Specifies the name of the pre-configured Rulebase on PCEF for a deactivation action is set under PCC-Action-Set configuration instance for PCC-Service configuration.

  *rule_name* is a pre-configured Rulebase in PCEF.

- **defer-by interval delayed_dur**
  This optional keyword supports the time-of-day-based procedures under PCC-Action-Set instance by configuring the relative time delay for Rulebase deactivation.

  *delayed_dur* configures the relative delay time by which the corresponding Rulebase deactivation is deferred. The action is triggered only when the time specified by *delayed_dur* is passed.

  *delayed_dur* specifies the delayed interval in **HH MIN SS** format.

  Following format is used for **HH MIN SS** in *delayed_dur*:

  - **HH** specifies the hour to defer the action trigger and must be an integer between 00 through 23.
  - **MIN** specifies the minutes to defer the action trigger and must be an integer between 00 through 59.
  - **SS** specifies the seconds to defer the action trigger and must be an integer between 00 through 59.

**Usage**

Use this command to set an action to deactivate a pre-configured Rulebase in PCC-Action-Set configuration for PCC-Service instance.

Additionally **defer-by interval** keyword is used to configure relative time by which the corresponding Rulebase deactivation is deferred.
Example

The following command sets an action to deactivate for Rulebase *rulebase1* under PCC-Action-Set configuration instance for PCC-Service configuration:

```
rulebase-deactivate rulebase1
```
service-tag

This command sets an action to activate/deactivate a pre-configured Service Tag rule in PCC-Action-Set configuration for PCC-Service instance.

Product
IPCF

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Action-Set Configuration
configure > context context_name > pcc-service service_name > action-set action_set_name

Entering the above command sequence results in the following prompt:
[context_name]host_name(config-pcc-action-set)#

Syntax

[no] service-tag svc_tag {activate-rule | deactivate-rule}

---

no
Removed the action to activate/deactivate a pre-configured Service Tag rule in PCC-Action-Set configuration for PCC-Service instance.

svc_tag
Specifies the name of the pre-configured Service Tag rule for an activation/deactivation is set under PCC-Action-Set configuration instance for PCC-Service configuration.
svc_tag is a pre-configured Service Tag name.

activate-rule
Specifies that action to be set for Service Tag activation rule under PCC-Action-Set configuration instance for PCC-Service configuration.

deactivate-rule
Specifies that action to be set for Service Tag deactivation rule under PCC-Action-Set configuration instance for PCC-Service configuration.

Usage
Use this command to set an action to activate/deactivate a pre-configured Service Tag rule in PCC-Action-Set configuration for PCC-Service instance.

Example

The following command sets the an activation rule for Service Tag named service_1 under PCC-Action-Set configuration instance for PCC-Service configuration:

    service-tag service_1 activate-rule
**terminate-session**

This command sets an action to terminate a Bearer based on **bearer-id** or unique combination of QCI and ARP received through current CCR message in PCC-Action-Set configuration for PCC-Service instance.

**Product**
IPCF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Action-Set Configuration
configure > context context_name > pcc-service service_name > action-set action_set_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-action-set)#
```

**Syntax**

```
[no] terminate-session
```

- **no**
  Removes the action to terminate a Bearer based on **bearer-id** from a PCC-Action-Set configuration instance for PCC-Service configuration.

**Usage**
Use this command to set an action to terminate a Bearer based on **bearer-id** or unique combination of QCI and ARP received through current CCR message in PCC-Action-Set configuration for PCC-Service instance. Termination of Bearer is possible only in case of PCRF binding and limited to Dynamic rules.

**Important:** This action is only applicable to IP-CAN sessions with access type as GPRS. When terminate Bearer is initiated, IPCF triggers **Bearer Termination Procedure** for the **bearer-id** received through current CCR message.

**Caution:** This command triggers termination of Gx and SPR sub session active under PCC-Service instance.

**Example**
The following command sets an action to terminate a Bearer based on **bearer-id** received through current CCR message under PCC-Action-Set configuration instance for PCC-Service configuration:
```
terminate-session
```
usage-monitor

This command sets an action to allow operator to stop, reset or start the counting for a PCC-Usage-Monitor in PCC-Action-Set configuration for PCC-Service instance.

Product
IPCF

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Action-Set Configuration
configure > context context_name > pcc-service service_name > action-set action_set_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pcc-action-set)#

Syntax

[no] usage-monitor usage_mon_name {reset-counter | start-counter | stop-counter}

no
Removes the action to allow operator to stop, reset or start the counting for a PCC-Usage-Monitor in PCC-Action-Set configuration for PCC-Service instance.

usage_mon_name
Specifies the name of the pre-configured PCC-Usage-Monitor for which counter action is configured under PCC-Action-Set configuration instance for PCC-Service configuration. usage_mon_name is a pre-configured PCC-Usage-Monitor.

reset-counter
 Resets the usage counts for PCC-Usage-Monitor under PCC-Action-Set configuration instance for PCC-Service configuration.

start-counter
 Starts the accumulation of usage counts for PCC-Usage-Monitor under PCC-Action-Set configuration instance for PCC-Service configuration.

stop-counter
 Stops the accumulation of usage counts for PCC-Usage-Monitor under PCC-Action-Set configuration instance for PCC-Service configuration.

Usage
Use this command to set an action to allow operator to stop, reset or start the counting for a usage monitor in PCC-Action-Set configuration for PCC-Service instance.

Example
The following command sets the an action to stop the accumulation of usage counts for PCC-Usage-Monitor named `usage_1` under PCC-Action-Set configuration instance for PCC-Service configuration:

```
usage-monitor usage_1 stop-counter
```
Chapter 234
PCC-AF-Service Configuration Mode Commands

The PCC-AF-Service Configuration mode provides a mechanism to IPCF to manage the external interfaces required for media and application function management. The PCC-AF-Service manages Rx interface which would be based on the dictionary used.

An Application Function (AF) provides Application (layer 7) proxies for client server applications. It also provides enforcement of operator and subscriber QoS, Charging, and Security policies to subscriber session and represents the network element that supports applications that require dynamic policy and/or charging control. In the IMS model, the AF is implemented by the Proxy Call Session Control Function (P-CSCF).

*Important:* This configuration mode is supported from StarOS Release 12.1 onward.

**Mode**

Exec > Global Configuration > Context Configuration > PCC AF Service Configuration

```
configure > context context_name > pcc-af-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-imsapp-service)#
```

*Important:* The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
associate pcc-service

This command is used to associate a pre-configured PCC-Service with a PCC-AF-Service for IPCF configuration.

**Product**
IPCF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PCC AF Service Configuration

configure > context context_name > pcc-af-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-imsapp-service)#

**Syntax**

```
associate pcc-service pcc_svc_name
```

```
[no] associate pcc-service
```

**no**

Removes/disassociate the configured PCC-service from this PCC-AF-Service instance configured for IPCF configuration.

**pcc_svc_name**

Specifies the name of a pre-configured PCC-service configured in Context Configuration mode for IPCF configuration.

The `pcc_svc_name` is name of a predefined PCC-Service instance and must be an alphanumerical string from 1 through 63 characters.

**Usage**

Use this command to associate a pre-configured PCC-Service instance for IPCF configuration.

**Important:** For more information on PCC-Service configuration, refer *PCC-Service Configuration Mode Commands*.

**Example**

Following command binds a PCC-Service named `pcc_svc1` with in a PCC-AF-Service.

```
associate pcc-service pcc_svc1
```

Following command removes an associated PCC-Service named `pcc_svc1` from a PCC-AF-Service.

```
no associate pcc-service pcc_svc1
```
diameter dictionary

This command is used to assign a Diameter dictionary for Rx messaging with a PCC-AF-Service for IPCF configuration.

**Product**
IPCF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PCC AF Service Configuration  
```
configure > context context_name > pcc-af-service service_name
```
Enter the above command sequence results in the following prompt:

```
[context_name]host_name(config-imsapp-service)#
```

**Syntax**

```text
diameter dictionary {r8-standard | standard}

default diameter dictionary
```

**default diameter dictionary**

Sets the Diameter Rx dictionary to default dictionary r8-standard (3GPP Rel. 8 standard) for a PCC-AF-Service instance configured for IPCF configuration.

**r8-standard**

Default: Enabled  
Sets the Diameter Rx dictionary to be used by a PCC-AF-Service instance configured for IPCF configuration over Rx interface to 3GPP Rel. 8 standard.

**standard**

Default: Disabled  
Sets the Diameter Rx dictionary to be used by a PCC-AF-Service instance configured for IPCF configuration over Rx interface to 3GPP Rel. 7 standard.

**Usage**

Use this command to configure the PCC-AF-Service to determine which of the 3GPP dictionary to be used for Rx interface messaging for media and application function management.

**Example**

Following command sets the PCC-AF-Service to use 3GPP Rel. 8 standard dictionary for Rx interface and application function management related messaging in a PCC-AF-Service.

```
default diameter dictionary
```
diameter origin end-point

This command is used to bind/associate a pre-configured Diameter host/realm (AF) over Rx interface with a PCC-AF-Service to be used for subscriber service control and AF profile management.

**Product**
IPCF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PCC AF Service Configuration
configure > context context_name > pcc-af-service service_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-imsapp-service)#
```

**Syntax**

```
diameter origin endpoint dia_endpoint_name

no diameter origin endpoint
```

- **no**
  Removes the associated Diameter Origin Endpoint configuration from PCC-AF-Service instance configured for IPCF configuration.

- **any**
  Sets the PCC-AF-Service instance to use any available AF node over Rx interface for AF support.

- **dia_endpoint_name**
  The dia_endpoint_name is a predefined Diameter origin endpoint node and must be an alphanumerical string from 1 through 63 characters.

**Usage**

Use this command to bind the AF node over Rx interface by associating a pre-configured Diameter Origin Endpoint with a PCC-AF-Service.

The Diameter origin endpoint must be a pre-configured instance in the Context Configuration Mode. For more information on Diameter origin endpoint configuration, refer Diameter Endpoint Configuration Mode Commands chapter.

**Example**

Following command associates a pre-configured Diameter endpoint node configuration named af_pcscfl with a PCC-AF-Service for AF profile management.

```
diameter origin endpoint af_pcscfl
```

Following command removes the pre-associated Diameter endpoint node configuration named af_pcscfl with a PCC-AF-Service.
no diameter origin endpoint
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

exit

Usage
Use this command to return to the parent configuration mode.
Chapter 235
PCC-Condition-Group Configuration Mode Commands

The PCC-Condition-Group Configuration Mode is used to configure the various rating parameters under a logical identifier name in the PCC-Service. A PCC-Condition-Group is a collection of conditions that identify a network or state constraint represented as a logical expression. A maximum of 128 conditions can be configured in one PCC-Condition-Group.

**Important:** This configuration mode is supported from StarOS Release 12.1 onward.

**Mode**

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Condition Group Configuration

```
configure > context context_name > pcc-service service_name > condition group group_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-condition-group)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
af-application-id

This command defines a condition based on the application id of an Application Function service through the Rx interface over which the IPCF receives media information for the application usage in an IP-CAN session.

Product
IPCF

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Condition Group Configuration

configure > context context_name > pcc-service service_name > condition group group_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pcc-condition-group)#

Syntax

[ no ] af-application-id operator value af_app_id

[ no ] af-application-id operator profile-attribute spr_attr_value

[ no ] af-application-id operator subscription-attribute subs_prof_attr_value

no
Removes the specified condition definition.

operator
Specifies how to logically match the AF-Application id.
operator must be one of the following:

- !=: Does not equal
- <: Equals

af_app_id
Specifies the identity string for AF-Application identifier over Rx interface.
af_app_id must be an alphanumeric string of 1 to 256 characters.

profile-attribute spr_attr_value
Specifies the profile attribute value in SPR to match with application id of an Application Function service condition validation in an IP-CAN session.
spr_attr_value must be an alphanumeric string of from 1 through 63 characters.

subscription-attribute subs_prof_attr_value
Specifies the subscriber profile attribute parameter value to match with application id of an Application Function service condition validation in an IP-CAN session.
subs_prof_attr_value must be an alphanumeric string of from 1 through 31 characters.
Usage

Use this command to define a condition based on the application id of an Application Function service through the Rx interface over which the IPCF receives media information for the application usage in an IP-CAN session.

Example

The following command creates a condition definition to analyze the PCC service user traffic for the AF Application id is not equal to pcc_af_1:

```
af-application-id != pcc_af_1
```
af-media-codec

This command defines a condition based on the media Codec used by AF application in an IP-CAN session.

Product
IPCF

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Condition Group
Configuration
configure > context context_name > pcc-service service_name > condition group group_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pcc-condition-group)#

Syntax

[ no ] af-media-codec operator value {g722 | g726 | ilbc | pcma | pcmu}
[ no ] af-media-codec operator profile-attribute spr_attr_value
[ no ] af-media-codec operator subscription-attribute subs_prof_attr_value

no

Removes the specified condition definition.

operator

Specifies how to logically match the AF-media Codec.

operator must be one of the following:

- !=: Does not equal
- ==: Equals

G.722

Specifies the media Codec as G.722 used for user traffic from AF server over Rx interface.

G.722 is a ITU-T standard 7 kHz wideband speech codec operating at 48, 56 and 64 kbit/s.

G.726

Specifies the media codec as G.726 used for user traffic from AF server over Rx interface.

G.726 is an ITU-T ADPCM speech codec standard covering the transmission of voice at rates of 16, 24, 32, and 40 kbit/s.

ilbc

Specifies the media codec as Internet Low Bitrate Codec (iLBC) used for user traffic from AF server over Rx interface.

iLBC is a narrowband speech codec suitable for VoIP applications, streaming audio, archival and messaging.

The encoded blocks encapsulated in Real-time Transport Protocol (RTP) protocol for transport.
pcma
Specifies the media codec as Pulse Code Modulation A-law scaling (PCMA) used for user traffic from AF server over Rx interface.
PCMA is an ITU-T Recommendation G.711 audio data encoding in eight bits per sample, after A-law logarithmic scaling.

pcmu
Specifies the media codec as Pulse Code Modulation mu-law scaling (PCMU) used for user traffic from AF server over Rx interface.
PCMU is an ITU-T Recommendation G.711 audio data encoding in eight bits per sample, after mu-law logarithmic scaling.

profile-attribute spr_attr_value
Specifies the profile attribute value in SPR to match with application media codec of an Application Function service condition validation in an IP-CAN session.
spr_attr_value must be an alphanumeric string of from 1 through 63 characters.

subscription-attribute subs_prof_attr_value
Specifies the subscriber profile attribute parameter value to match with application media codec of an Application Function service condition validation in an IP-CAN session.
subs_prof_attr_value must be an alphanumeric string of from 1 through 31 characters.

Usage
Use this command to define a condition based on the media codecs used by AF service through the Rx interface over which the IPCF receives media information for the application usage in an IP-CAN session.

Example
The following command creates a condition definition to analyze the PCC service user traffic for the AF Media codec is equal to PCMA:

af-media-codec = pcma
af-media-type

This command defines a condition based on the media type used by AF application in an IP-CAN session.

Product
IPCF

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Condition Group Configuration

configure > context context_name > pcc-service service_name > condition group group_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pcc-condition-group)#

Syntax

[ no ] af-media-type operator value {application | audio | control | data | message | other | text | video}

[ no ] af-media-type operator profile-attribute spr_attr_value

[ no ] af-media-type operator subscription-attribute subs_prof_attr_value

no

Removes the specified condition definition.

operator

Specifies how to logically match the media type in user traffic.

operator must be one of the following:

- !=: Does not equal
- ==: Equals

application

Specifies the media type as Application in user traffic from AF server over Rx interface.

audio

Specifies the media type as Audio in user traffic from AF server over Rx interface.

ccontrol

Specifies the media type as Control in user traffic from AF server over Rx interface.

data

Specifies the media type as Data in user traffic from AF server over Rx interface.
message
Specifies the media type as Message in user traffic from AF server over Rx interface.

Text
Specifies the media type as Text in user traffic from AF server over Rx interface.

video
Specifies the media type as Video in user traffic from AF server over Rx interface.

profile-attribute $spr_attr_value$
Specifies the profile attribute value in SPR to match with application media type of an Application Function service condition validation in an IP-CAN session.
$spr_attr_value$ must be an alphanumeric string of from 1 through 63 characters.

subscription-attribute $subs_prof_attr_value$
Specifies the subscriber profile attribute parameter value to match with application media type of an Application Function service condition validation in an IP-CAN session.
subs_prof_attr_value must be an alphanumeric string of from 1 through 31 characters.

Usage
Use this command to define a condition based on the media type used by AF service through the Rx interface over which the IPCF receives media information for the application usage in an IP-CAN session.

Example
The following command creates a condition definition to analyze the PCC service user traffic for the AF Media type is equal to Video:

   af-media-type = video
af-service-urn

This command defines a condition based on the service Uniform Resource Names (URNs) used by AF application in an IP-CAN session.

**Product**
IPCF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Condition Group Configuration

```
configure > context context_name > pcc-service service_name > condition group group_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-condition-group)#
```

**Syntax**

```
[ no ] af-service-urn operator value urn_string
[ no ] af-service-urn operator profile-attribute spr_attr_value
[ no ] af-service-urn operator subscription-attribute subs_prof_attr_value
```

**no**

Removes the specified condition definition.

**operator**

Specifies how to logically match the information in the analyzed field.

- `!==`: Does not equal
- `<=`: Lesser than or equals
- `==`: Equals
- `>=`: Greater than or equals

**urn_string**

Specifies the URN in user traffic from AF server over Rx interface.

- `urn_string` must be an alphanumeric string of 1 through 256 characters.

**profile-attribute spr_attr_value**

Specifies the profile attribute value in SPR to match with URN used by AF service condition validation in an IP-CAN session.

- `spr_attr_value` must be an alphanumeric string of from 1 through 63 characters.
subscription-attribute subs_prof_attr_value

Specifies the subscriber profile attribute parameter value to match with URN used by AF service condition validation in an IP-CAN session.

*subs_prof_attr_value* must be an alphanumeric string of from 1 through 31 characters.

**Usage**

Use this command to define a condition based on the URN used by AF service through the Rx interface over which the IPCF receives media information for the application usage in an IP-CAN session. Uniform Resource Names (URNs) serves as persistent, location-independent resource identifiers and are designed to make it easy to map other namespaces into URN-space.

**Example**

The following command creates a condition definition to analyze the PCC service user traffic for the AF service URN is equal to ietf:rfc:4003:

```
af-service-urn = ietf:rfc:4003
```
an-gw-address

This command defines a condition based on the IP address of Access Node Gateway (AN-GW) on which subscriber is attached in an IP-CAN session.

**Product**
IPCF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Condition Group Configuration

configure > context context_name > pcc-service service_name > condition group group_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pcc-condition-group)#

**Syntax**

```
[ no ] an-gw-address [operator value anw_ip/mask | [in-range | !in-range] range_start_ip to range_end_ip]

[ no ] an-gw-address operator profile-attribute spr_attr_value

[ no ] an-gw-address operator subscription-attribute subs_prof_attr_value
```

**no**
Removes the specified condition definition.

**operator**
Specifies how to logically match the information in the analyzed field. 

`operator` must be one of the following:

- `!=`: Does not equal
- `=`: Equals

**in-range**
Specifies the condition to accept the IP address which are in range as argument to define the Access Node Gateway address which is used by subscriber in IP-CAN session.

**!in-range**
Specifies the condition to accept the IP address which are NOT in range as argument to define the Access Node Gateway address which is used by subscriber in IP-CAN session.

**range_start_ip**
Specifies the starting IP address which is used for defining the range of AN-GW IP addresses which is used by subscriber in IP-CAN session.

`range_start_ip` is an IP address and must be lesser than `end_start_ip` address.
range_end_ip

Specifies the ending IP address which is used for defining the range of AN-GW IP addresses which is used by subscriber in IP-CAN session.
range_end_ip is an IP address and must be greater than end_start_ip address.

angw_ip/mask

Specifies the IP address of the Access Node Gateway which is used by subscriber in IP-CAN session along with IP mask as well.
angw_ip must be an IP address in IPv4 or IPv6 notation.
mask: Specifies the IP address mask bits to determine the number of IP addresses of AN-GW in condition.
mask must be specified using the standard IPv4 dotted decimal notation.

profile-attribute spr_attr_value

Specifies the profile attribute value in SPR to match with AN gateway IP address condition validation in an IP-CAN session.
spr_attr_value must be an alphanumeric string of from 1 through 63 characters.

subscription-attribute subs_prof_attr_value

Specifies the subscriber profile attribute parameter value to match with AN gateway IP address condition validation in an IP-CAN session.
subs_prof_attr_value must be an alphanumeric string of from 1 through 31 characters.

Usage

Use this command to define a condition based on the AN-GW IP address used by subscriber in an IP-CAN session.

Example

The following command creates a condition definition to analyze the condition based on AN-GW IP address 1.2.3.4 in an IP-CAN session:

    an-gw-address = 1.2.3.4
**authorized-qci**

This command defines a condition based on the authorized QoS Class Identifier used in an IP-CAN session.

**Product**

IPCF

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Condition Group Configuration

```
configure > context context_name > pcc-service service_name > condition group group_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-condition-group)#
```

**Syntax**

```
[ no ] authorized-qci operator value qci
[ no ] authorized-qci operator profile-attribute spr_attr_value
[ no ] authorized-qci operator subscription-attribute subs_prof_attr_value
```

- **no**
  - Removes the specified condition definition.

- **operator**
  - Specifies how to logically match the information in the analyzed field.
  - **operator** must be one of the following:
    - !=: Does not equal
    - <=: Lesser than or equal
    - =: Equals
    - >=: Greater than or equal

- **qci**
  - Specifies the authorized QoS class identifier in user traffic for condition validation.
  - **qci** must be an integer between 1 through 255.

- **profile-attribute spr_attr_value**
  - Specifies the profile attribute value in SPR to match with authorized QoS class identifier condition validation in an IP-CAN session.
  - **spr_attr_value** must be an alphanumeric string of from 1 through 63 characters.
subscription-attribute subs_prof_attr_value

Specifies the subscriber profile attribute parameter value to match with authorized QoS class identifier condition validation in an IP-CAN session.

subs_prof_attr_value must be an alphanumeric string of from 1 through 31 characters.

Usage

Use this command to define a condition based on the authorized QCI used by the subscriber in an IP-CAN session.

The condition evaluates to TRUE, if Bearer Control Mode is UE and network (PCEF bearer binding) and IPCF has authorized the specified QCI earlier.

QCI is a number which describes the error rate and delay that are associated with the service. It includes bearer parameters including scheduling weights and queue management thresholds.

Example

The following command creates a condition definition to analyze the PCC service user traffic for the authorized QCI is greater than or equal to 4:

```bash
authorized-qci >= 4
```
**base-station-id**

This command defines a condition based on the various parameters used in base-station id by subscriber in an IP-CAN session between PCEF (PDSN) and IPCF over Gx interface.

**Product**
IPCF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Condition Group Configuration

```bash
configure > context context_name > pcc-service service_name > condition group group_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-condition-group)#
```

**Syntax**

```bash
[no] base-station-id { [sid operator sys_identifier] | range start_range to end_range] } [ nid operator netwrk_identifier ] | range start_range to end_range } [ cellid operator cell_identifier ] | range start_range to end_range ]}
```

- **no**
  Removes the specified condition definition.

**operator**

Specifies how to logically match the information in the analyzed field.

* operator must be one of the following:

- • !=: Does not equal
- • <: Lesser than
- • <=: Lesser than or equals
- • =: Equals
- • >: Greater than
- • >=: Greater than or equals

**sid operator sys_identifier**

Specifies the system identifier in base-station id of subscriber for condition validation in an IP-CAN session.

*sys_identifier* must be an integer between 0 through 65535.

**nid operator netwrk_identifier**

Specifies the network identifier in base-station id, which is used by subscriber, for condition validation in an IP-CAN session.

*netwrk_identifier* must be an integer between 0 through 65535.
**cellid operator cell_identifier**

Specifies the cell identifier in base-station id, which is used by subscriber, for condition validation in an IP-CAN session.

*cell_identifier* must be an integer between 0 through 65535.

**range start_range to end_range**

This optional keyword specifies range of the identifiers (SID, Cell Id, Network Id) to be used for condition validation in an IP-CAN session.

*start_range* is the start value of range having integer between 0 through 65535 and it must be lesser than *end_range*.

*end_range* is the end value of range having integer between 0 through 65535 and it must be greater than *start_range*.

**Usage**

User this command to define a condition based on the parameters used in base-station id of subscriber, which is composition of SID, Cell Id, and/or Network Id, in an IP-CAN session between PCEF (PDSN) and IPCF over Gx interface.

This condition is defined for PCC functionality support to CDMA users over Gx interface.

**Example**

The following command creates a condition definition to analyze the condition based on base-station id of subscriber where SID is 1001 and cell id is in range of 2001 to 2069 in an IP-CAN session between PDSN and IPCF having network id as 3989:

```
base-station-id sid = 1001 nid = 3989 cellid = range 2001 to 2069
```
**bearer-count**

This command defines a condition based on the number of bearers allowed in a subscriber session on IPCF to accept bearer-count in an IP-CAN session.

**Product**

IPCF

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Condition Group Configuration

`configure > context context_name > pcc-service service_name > condition group group_name`

Entering the above command sequence results in the following prompt:

```
[context_name] host_name(config-pcc-condition-group) #
```

**Syntax**

```
[ no ] bearer-count operator value num_bearer
[ no ] bearer-count operator profile-attribute spr_attr_value
[ no ] bearer-count operator subscription-attribute subs_prof_attr_value
```

**no**

Removes the specified condition definition.

**operator**

Specifies how to logically match the information in the analyzed field. `operator` must be one of the following:

- `!=`: Does not equal
- `<=`: Lesser than or equals
- `=`: Equals
- `>=`: Greater than or equals

**num_bearer**

Specifies the number of bearers in user traffic for condition validation. `num_bearer` indicates a condition based on the number of bearer established in a IP-CAN session and must be an integer between 1 through 11.

**profile-attribute spr_attr_value**

Specifies the profile attribute value in SPR to match with number of bearers allowed for a subscriber in an IP-CAN session as condition. `spr_attr_value` must be an alphanumeric string of from 1 through 63 characters.
**subscription-attribute subs_prof_attr_value**

Specifies the subscriber profile attribute parameter value to match with number of bearers allowed for a subscriber in an IP-CAN session as condition.

`subs_prof_attr_value` must be an alphanumerical string of from 1 through 31 characters.

**Usage**

Use this command to define a condition based on the number of bearers allowed for a subscriber in an IP-CAN session.

**Example**

The following command creates a condition definition to analyze the PCC service user traffic for bearers allowed in a subscriber session is equal to 4:

```
bearer-count = 4
```
connectivity-access-network

This command defines a condition based on the access network type used by subscriber in an IP-CAN session.

Product
IPCF

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Condition Group
Configuration

configure > context context_name > pcc-service service_name > condition group group_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pcc-condition-group)#

Syntax

[ no ] connectivity-access-network operator value {3gpp-gprs | 3gpp2 | 3gpp2-eps | docsis | non-3gpp-eps | wimax | xdsl }

[ no ] connectivity-access-network operator profile-attribute spr_attr_value

[ no ] connectivity-access-network operator subscription-attribute subs_prof_attr_value

no

Removes the specified condition definition.

operator

Specifies how to logically match the media type in user traffic.
operator must be one of the following:

- !=: Does not equal
- ==: Equals

3gpp-gprs

Specifies the network access connectivity type as 3GPP-GPRS for user traffic in condition definition.

3gpp2

Specifies the network access connectivity type as 3GPP2 (CDMA) for user traffic in condition definition.

3gpp2-eps

Specifies the network access connectivity type as 3GPP2-EPS for user traffic in condition definition.

docsis

Specifies the network access connectivity type as Data Over Cable Service Interface Specification (DOCSIS) for user traffic in condition definition.
non-3gpp-eps
Specifies the network access connectivity type as non-3GPP-EPS to connect with Gxa based HSGW for user traffic in condition definition.

wimax
Specifies the network access connectivity type as Wi-MAX for user traffic in condition definition.

xdsl
Specifies the network access connectivity type as xDSL (ADSL/SDSL) or user traffic in condition definition.

profile-attribute spr_attr_value
Specifies the profile attribute value in SPR to match with type of connectivity used for network access by subscriber in an IP-CAN session as condition.

subscription-attribute subs_prof_attr_value
Specifies the subscriber profile attribute parameter value to match with type of connectivity used for network access by subscriber in an IP-CAN session as condition.

Usage
Use this command to define a condition based on the type of connectivity used for network access by subscriber in an IP-CAN session.

Example
The following command creates a condition definition to analyze the PCC service user traffic for the network type is equal to Wi-MAX:

```
connectivity-access-network = wimax
```
**end**

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
end
```

**Usage**
Use this command to return to the Exec mode.
**eval-condition-group**

This command defines a condition based on the TRUE or FALSE setting of a configured PCC-Condition-Group for subscriber in an IP-CAN session.

**Product**
IPCF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Condition Group Configuration

```
configure > context context_name > pcc-service service_name > condition group group_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-condition-group)#
```

**Syntax**

```
[no] eval-condition-group cond_grp_name operator {FALSE | TRUE}
```

- **no**
  Removes the specified condition definition.

- **cond_grp_name**
  Specifies the name of the configured PCC-Condition-Group which is used for evaluation with in this PCC-Condition-Group for user traffic.
  `cond_grp_name` must be a pre-configured PCC-Condition-Group in this configuration mode.

- **operator**
  Specifies how to logically match the media type in user traffic.
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `==`: Equals

- **FALSE**
  Sets the evaluation condition for specified PCC-Condition-Group to FALSE.
  With this keyword system rejects all conditions defined in specific PCC-Condition-Group and match the same in user traffic.

- **TRUE**
  Sets the evaluation condition for specified PCC-Condition-Group to TRUE.
  With this keyword system accepts all conditions defined in specific PCC-Condition-Group and match the same in user traffic.
**Usage**

Use this command to define a condition based on the acceptance or rejection of specific pre-configured PCC-Condition-Group for user traffic in an IP-CAN session. This command allows the operator to use configured PCC-Condition-Group in another PCC-Condition-Group as subset of PCC-Condition-Group.

**Important:** A maximum of 3 level of recursion depth is allowed for PCC-Condition-Group evaluation in a PCC-Condition-Group.

**Example**

The following command creates a condition definition to accept the all conditions defined in PCC-Condition-Group named `af_1`:

```
eval-condition-group af_1 = TRUE
```
event-time

This command defines a condition based on the event-trigger time as per the time specified by the named Time definition (Timedef) configured for subscriber session in an IP-CAN session.

Product
IPCF

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Condition Group Configuration

configure > context context_name > pcc-service service_name > condition group group_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pcc-condition-group)#

Syntax

[no] event-time operator timedef_name

---

no

Removes the specified condition definition.

---

operator

Specifies how to logically match the information in the analyzed field.

operator must be one of the following:

- !=: Does not equal
- <=: Lesser than or equals
- ==: Equals
- >=: Greater than or equals

---

timedef_name

Specifies the name of the configured time definition (start and end timer of session) which is used for evaluation with this PCC-Condition-Group for user traffic.

timedef_name must be a pre-configured Time definition in PCC-Service Configuration Mode.

---

Usage

Use this command to define a condition based on the start and end time defined in a Time Definition configuration in PCC-Service Configuration Mode for user traffic in an IP-CAN session.

Event trigger in this command indicates a condition when the event-trigger time was as per the time specified by the named Time Definition.

This command allows the operator to use configured time period as event trigger for this PCC-Condition-Group.

Example
The following command creates a condition definition to trigger the condition based on the start and end time defined in Timedef named `timedef_night`:

```
  event-time = timedef_night
```
event-trigger

This command defines a condition based on the event triggers due to various conditions for subscriber in an IP-CAN session.

Product
IPCF

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Condition Group

Configuration

configure > context context_name > pcc-service service_name > condition group group_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pcc-condition-group)#

Syntax

[no] event-trigger operator event_trigger

---

no

Removes the specified condition definition.

---

operator

Specifies how to logically match the media type in user traffic.

operator must be one of the following:

- !=: Does not equal
- ==: Equals

---

event_trigger

Specifies the network events as condition definition for user traffic in an IP-CAN session. Following event triggers are supported with this command:

- an-gw-change
- bearer-qos-change
- bearer-setup
- bearer-termination
- default-eps-bearer-qos-change
- ip-can-change
- loss-of-bearer
- out-of-credit
- pgw-trace-control
event-trigger

*plmn-change
*qos-change
*qos-change-exceeding-authorization
*rai-change
*rat-change
*reallocation-of-credit
*recover-of-bearer
*resource-modification-request
*revalidation-timeout
*session-setup
*session-termination
*sgsn-change
*successful-resource-allocation
*tft-change
*ue-ip-address-allocate
*ue-ip-address-release
*ue-time-zone-change
*user-location-change

Usage

Use this command to define a condition based on the event triggered in network for user traffic.

Example

The following command creates a condition definition when there is a change in traffic flow template for subscriber:

```
    event-trigger = tft-change
```
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Use this command to return to the parent configuration mode.
**imsi**

This command defines a condition based on the International Mobile Station Identification number (IMSI) of a subscriber in an IP-CAN session.

**Product**
IPCF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Condition Group Configuration

```
configure > context context_name > pcc-service service_name > condition group group_name
```

Entering the above command sequence results in the following prompt:

```
[context_name] host_name(config-pcc-condition-group)#
```

**Syntax**

```
[ no ] imsi operator value imsi
[ no ] imsi operator profile-attribute spr_attr_value
[ no ] imsi operator subscription-attribute subs_prof_attr_value
```

**no**
Removes the specified condition definition.

**operator**
Specifies how to logically match the information in the analyzed field.

- `!=`: Does not equal
- `==`: Equals

**imsi**
Specifies the IMSI of subscriber to be used for condition validation in an IP-CAN session.

- `imsi` must be a string of between 8 to 15 digits which starts with 3 digit of MCC then 2 to 3 digit of MNC.
- Wildcard characters `$` and `*` are allowed. The `*` wildcard matches multiple characters and the `$` wildcard matches a single character. If you do not want the wildcard characters interpreted as a wildcard enclose them in single quotes (‘’). For example; ‘$’.

**profile-attribute**
Specifies the profile attribute value in SPR to match with IMSI in an IP-CAN session as condition.

- `spr_attr_value` must be an alphanumeric string of from 1 through 63 characters.
subscription-attribute subs_prof_attr_value

Specifies the subscriber profile attribute parameter value to match with IMSI in an IP-CAN session as condition.

subs_prof_attr_value must be an alphanumeric string of from 1 through 31 characters.

Usage

Use this command to define a condition based on the IMSI of a subscriber used in an IP-CAN session.

Example

The following command creates a condition definition to analyze the condition based on subscriber IMSI as 12334566434 in an IP-CAN session:

```
imsi = 12334566434
```
**msisdn**

This command defines a condition based on the Mobile Station International Subscriber Directory Number (MSISDN) of a subscriber in an IP-CAN session.

**Product**
- IPCF

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Condition Group Configuration

```
configure > context context_name > pcc-service service_name > condition group group_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-condition-group)#
```

**Syntax**

```
[ no ] msisdn operator value msisdn
[ no ] msisdn operator profile-attribute spr_attr_value
[ no ] msisdn operator subscription-attribute subs_prof_attr_value
```

<table>
<thead>
<tr>
<th>no</th>
<th>Removes the specified condition definition.</th>
</tr>
</thead>
<tbody>
<tr>
<td>operator</td>
<td>Specifies how to logically match the information in the analyzed field. <strong>operator</strong> must be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• !=: Does not equal</td>
</tr>
<tr>
<td></td>
<td>• ==: Equals</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>imsi</th>
<th>Specifies the MSISDN of subscriber to be used for condition validation in an IP-CAN session. <strong>msisdn</strong> must be a string of between 1 to 16 digits which contains CC + NDC/NPA + SN. Wildcard characters $ and * are allowed. The * wildcard matches multiple characters and the $ wildcard matches a single character. If you do not want the wildcard characters interpreted as a wildcard enclose them in single quotes (‘’). For example; ‘$’.</th>
</tr>
</thead>
</table>

| profile-attribute spr_attr_value | Specifies the profile attribute value in SPR to match with MSISDN in an IP-CAN session as condition. **spr_attr_value** must be an alphanumeric string of from 1 through 63 characters. |
subscription-attribute  subs_prof_attr_value

Specifies the subscriber profile attribute parameter value to match with MSISDN in an IP-CAN session as condition.

subs_prof_attr_value must be an alphanumeric string of from 1 through 31 characters.

Usage

Use this command to define a condition based on the MS ISDN of a subscriber used in an IP-CAN session.

Example

The following command creates a condition definition to analyze the condition based on subscriber MSISDN as 380561234567 in an IP-CAN session:

msisdn = 380561234567
multi-line-or

This command enables/disables the “OR” relation across all conditions exist in PCC-Condition-Group Configuration Mode.

Product
IPCF

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Condition Group Configuration

configure > context context_name > pcc-service service_name > condition group group_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pcc-condition-group)#

Syntax

[no] multi-line-or

no

Sets the PCC-Condition-Group to “AND” relation across all conditions exist in a PCC-Condition-Group Configuration Mode.

Usage
Use this command to enable the “OR” relation across all conditions exist in PCC-Condition-Group Configuration Mode.
In absence of this command the default relation of “AND” applies across all conditions exist in PCC-Condition-Group Configuration Mode.

Example

The following command enables the “OR” relation across all conditions exist in PCC-Condition-Group Configuration Mode:

multi-line-or

The following command enables the default “AND” relation across all conditions exist in PCC-Condition-Group Configuration Mode:

no multi-line-or
nai

This command defines a condition based on the Network Access Identifier (NAI) of a subscriber in an IP-CAN session between PCEF (PDSN) and IPCF over Gx interface.

Product
IPCF

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Condition Group Configuration

Syntax

[ no ] nai operator {username user_name [domain domain] | domain domain}
[ no ] nai operator profile.attribute spr_attr_value
[ no ] nai operator subscription.attribute subs_prof_attr_value

no

Removes the specified condition definition.

operator

Specifies how to logically match the information in the analyzed field.

operator must be one of the following:
- !=: Does not equal
- ==: Equals

username user_name

Specifies the subscriber user name to be used for condition validation in an IP-CAN session.

user_name must be an alpha and/or numeric string of 1 through 128 characters in length. The user name can contain all special characters.

domain domain

Specifies the domain (Realm) of subscriber to be used for condition validation in an IP-CAN session.

domain must be an alpha and/or numeric string of 1 through 128 characters in length. The domain name can contain all special characters.

profile.attribute spr_attr_value

Specifies the profile attribute value in SPR to match with NAI in an IP-CAN session as condition.

spr_attr_value must be an alphanumeric string of from 1 through 63 characters.
subscription-attribute subs_prof_attr_value

Specifies the subscriber profile attribute parameter value to match with NAI in an IP-CAN session as condition.

*subs_prof_attr_value* must be an alphanumeric string of from 1 through 31 characters.

### Usage

User this command to define a condition based on the NAI, which contains of user name and domain name, of a subscriber in an IP-CAN session between PCEF (PDSN) and IPCF over Gx interface.

This condition is defined for PCC functionality support to CDMA users over Gx interface.

### Example

The following command creates a condition definition to analyze the condition based on subscriber user name as *cdma2000_subs1* in an IP-CAN session between PDSN and IPCF having *xyz.com* as domain:

```
nai = username cdma2000_subs1 domain xyz.com
```
out-of-credit rulename

This command defines a condition based on the exhaustion of credit for subscriber Rulename at PCEF in an IP-CAN session.

Product
- IPCF

Privilege
- Security Administrator, Administrator

Mode
- Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Condition Group Configuration

configure > context context_name > pcc-service service_name > condition group group_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pcc-condition-group)#

Syntax

[no] out-of-credit rulename operator rule_name

no

Removes the specified condition definition.

operator

Specifies how to logically match the information in the analyzed field.

operator must be one of the following:

- !=: Does not equal
- ==: Equals

rule_name

Specifies the name of the Rulename for which out of credit condition is to match in an IP-CAN session.

rule_name is a pre-configured Rulename on PCEF and must be an alphanumeric string of from 1 through 63 characters.

Usage

Use this command to define a condition based on the exhaustion of credit for subscriber Rulename at PCEF in an IP-CAN session.

Example

The following command creates a condition definition to analyze the condition based on the exhaustion of credit for subscriber Rulename rule_101 at PCEF in an IP-CAN session:

    out-of-credit rulename = rule_101
**out-of-credit rulebase-name**

This command defines a condition based on the exhaustion of credit for subscriber Rulebase name at PCEF in an IP-CAN session.

**Product**

IPCF

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Condition Group Configuration

```bash
configure > context context_name > pcc-service service_name > condition group group_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-condition-group)#
```

**Syntax**

```
[no] out-of-credit rulebase-name operator rulebase_name
```

- **no**
  
  Removes the specified condition definition.

- **operator**
  
  Specifies how to logically match the information in the analyzed field. **operator** must be one of the following:
  
  - `!=`: Does not equal
  
  - `==`: Equals

- **rulebase_name**
  
  Specifies the name of the Rulebase for which out of credit condition is to match in an IP-CAN session. **rulebase_name** is a pre-configured Rulebase on PCEF and must be an alphanumeric string of from 1 through 63 characters.

**Usage**

Use this command to define a condition based on the exhaustion of credit for subscriber Rulebase name at PCEF in an IP-CAN session.

**Example**

The following command creates a condition definition to analyze the condition based on the exhaustion of credit for subscriber Rulebase name *rulebase_101* at PCEF in an IP-CAN session:

```
out-of-credit rulebase-name = rulebase_101
```
pcef-address

This command defines a condition based on the IP address of Policy and Charging Enforcement Function (PCEF) which is served by IPCF and through which subscriber is attached to an IP-CAN session.

**Product**
IPCF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Condition Group Configuration

```
configure > context context_name > pcc-service service_name > condition group group_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-condition-group)#
```

**Syntax**

```
[ no ] pcef-address {operator value pcef_ip/mask | (in-range | !in-range) value range_start_ip to range_end_ip}
```

```
[ no ] pcef-address operator profile-attribute spr_attr_value
```

```
[ no ] pcef-address operator subscription-attribute subs_prof_attr_value
```

---

**no**

Removes the specified condition definition.

---

**operator**

Specifies how to logically match the information in the analyzed field.

*operator* must be one of the following:

- `!=`: Does not equal
- `==`: Equals

---

**in-range**

Specifies the condition to accept the IP address which are in range as argument to define the PCEF address which is used by subscriber in IP-CAN session.

---

**!in-range**

Specifies the condition to accept the IP address which are NOT in range as argument to define the PCEF address which is used by subscriber in IP-CAN session.

---

**range_start_ip**

Specifies the starting IP address which is used for defining the range of PCEF IP addresses which is used by subscriber in IP-CAN session.

*range_start_ip* is an IP address and must be lesser than *end_start_ip* address.
range_end_ip

Specifies the ending IP address which is used for defining the range of PCEF IP addresses which is used by subscriber in IP-CAN session.

*range_end_ip* is an IP address and must be greater than *end_start_ip* address.

pcef_ip/mask

Specifies the IP address of the PCEF which is used by subscriber in IP-CAN session along with IP mask as well.

pcef_ip must be an IP address in IPv4 or IPv6 notation.

*mask* Specifies the IP address mask bits to determine the number of IP addresses of PCEF in condition. *mask* must be specified using the standard IPv4 dotted decimal notation.

profile-attribute spr_attr_value

Specifies the profile attribute value in SPR to match with PCEF address in an IP-CAN session as condition.

*spr_attr_value* must be an alphanumeric string of from 1 through 63 characters.

subscription-attribute subs_prof_attr_value

Specifies the subscriber profile attribute parameter value to match with PCEF address in an IP-CAN session as condition.

*subs_prof_attr_value* must be an alphanumeric string of from 1 through 31 characters.

Usage

Use this command to define a condition based on the PCEF IP address used by subscriber in an IP-CAN session.

Example

The following command creates a condition definition to analyze the condition based on PCEF P address 1.2.3.4 in an IP-CAN session:

```
pcef-address = 1.2.3.4
```
pdn-id

This command defines a condition based on the PDN or calling station id in an IP-CAN session.

**Product**
IPCF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Condition Group Configuration

```
configure > context context_name > pcc-service service_name > condition group group_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-condition-group)#
```

**Syntax**

```
[ no ] pdn-id [case-insensitive] operator value pdn_id
[ no ] pdn-id [case-insensitive] operator profile-attribute spr_attr_value
[ no ] pdn-id [case-insensitive] operator subscription-attribute subs_prof_attr_value
```

no
Removes the specified condition definition.

---

**case-insensitive**

This optional keyword sets the condition to not to consider the case of argument phrase for condition definition.

---

**operator**

Specifies how to logically match the information in the analyzed field. **operator** must be one of the following:

- `!=`: Does not equal
- `=`: Equals
- `contains`: Contains
- `!contains`: Does not contain
- `starts-with`: Starts with
- `!starts-with`: Does not start with
- `ends-with`: Ends with
- `!ends-with`: Does not end with

---

**pdn_id**

Specifies the PDN or calling station id to be used for condition validation in an IP-CAN session.
**pdn-id**

*pdn_id* must be an alphanumeric string of between 1 to 128 characters.

**profile-attribute** `spr_attr_value`

Specifies the profile attribute value in SPR to match with PDN id in an IP-CAN session as condition.

*spr_attr_value* must be an alphanumeric string of from 1 through 63 characters.

**subscription-attribute** `subs_prof_attr_value`

Specifies the subscriber profile attribute parameter value to match with PDN id in an IP-CAN session as condition.

*subs_prof_attr_value* must be an alphanumeric string of from 1 through 31 characters.

**Usage**

Use this command to define a condition based on the PDN or calling station id used in an IP-CAN session.

**Example**

The following command creates a condition definition to analyze the condition based on calling station id *ggsn_all_102* in an IP-CAN session:

```
pdn-id = ggsn_all_102
```
profile-attribute

This command defines a condition based on the matching between subscriber profile attribute value and SPR attribute value in an IP-CAN session.

Product
IPCF

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Condition Group Configuration

```
configure > context context_name > pcc-service service_name > condition group group_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-condition-group)#
```

Syntax

```
[no] profile-attribute parameter subs_prof_attr_value operator spr_attr_value
```

**no**

Removes the specified condition definition.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>parameter</td>
<td>Specifies the attribute parameter value to match with SPR attribute for condition validation in an IP-CAN session. subs_prof_attr_value must be an alphanumeric string of from 1 through 31 characters.</td>
</tr>
<tr>
<td>operator</td>
<td>Specifies how to logically match the information in the analyzed field.</td>
</tr>
<tr>
<td>operator</td>
<td>operator must be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• !=: Does not equal</td>
</tr>
<tr>
<td></td>
<td>• ==: Equals</td>
</tr>
<tr>
<td>spr_attr_value</td>
<td>Specifies the attribute value in SPR to match with Subscriber profile attribute for condition validation in an IP-CAN session. spr_attr_value must be an alphanumeric string of from 1 through 63 characters.</td>
</tr>
</tbody>
</table>

**Important:** This keyword deprecated in StarOS Release 14.0 and onward.
Usage

Use this command to define a condition based on the matching parameters between subscriber profile attribute and SPR attribute parameters used in an IP-CAN session and provides a generic way of specifying and triggering actions based on any of the subscriber profile attribute received from SPR interactions.

Example

The following command creates a condition definition to analyze the condition based on matching of subscriber profile attribute value `subs_gold_102` with SPR attribute value `spr_gold_102` in an IP-CAN session:

```plaintext
profile-attribute parameter subs_gold_102 = spr_gold_102
```
**radio-access-technology**

This command defines a condition based on the radio access technology used by subscriber in an IP-CAN session.

**Product**
IPCF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Condition Group Configuration

```
configure > context context_name > pcc-service service_name > condition group group_name
```

Entering the above command sequence results in the following prompt:
```
[context_name]host_name(config-pcc-condition-group)#
```

**Syntax**

```
[ no ] radio-access-technology operator value RAT
[ no ] radio-access-technology operator profile-attribute spr_attr_value
[ no ] radio-access-technology operator subscription-attribute subs_prof_attr_value
```

- **no**
  Removes the specified condition definition.

- **operator**
  Specifies how to logically match the media type in user traffic.
  `operator` must be one of the following:
  - `!=`: Does not equal
  - `=`: Equals

- **RAT**
  Specifies the radio access technology used by subscriber to access the network as condition definition for user traffic in an IP-CAN session.
  Following RAT are supported with this command:
  - `cdma2000-1x`: 3GPP2 CDMA 2000 - 1x RTT
  - `eutran`: Evolved Universal Terrestrial Radio Access Network (eUTRAN)
  - `gan`: Generic Access Network (GAN)
  - `geran`: GSM Edge Radio Access Network (GERAN)
  - `hrpd`: High Rate Packet Data (CDMA 2000 1xEV-DO)
  - `hspa-evolution`: Evolved High-Speed Packet Access (eHSPA/HSPA+)
  - `umb`: Ultra-Mobile Broadband
• **utran**: Universal Terrestrial Radio Access Network (UTRAN)
• **wlan**: Wireless Local Area Network (WLAN/xDSL)

### profile-attribute spr_attr_value

Specifies the profile attribute value in SPR to match with type of RAT in an IP-CAN session as condition. `spr_attr_value` must be an alphanumeric string of from 1 through 63 characters.

### subscription-attribute subs_prof_attr_value

Specifies the subscriber profile attribute parameter value to match with type of RAT in an IP-CAN session as condition. `subs_prof_attr_value` must be an alphanumeric string of from 1 through 31 characters.

### Usage

Use this command to define a condition based on the type of radio technology used for network access by subscriber in an IP-CAN session.

### Example

The following command creates a condition definition to analyze the PCC service user traffic for the radio access technology type as WLAN:

```
radio-access-technology = wlan
```
**sgsn-ip**

This command defines a condition based on the IP address of SGSN on which subscriber is attached in an IP-CAN session.

**Product**
IPCF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Condition Group Configuration

```
configure > context context_name > pcc-service service_name > condition group group_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-condition-group)#
```

**Syntax**

```
[ no ] sgsn-ip {operator value sgsn_ip/mask | {in-range | !in-range} range_start_ip to range_end_ip}

[ no ] sgsn-ip operator profile-attribute spr_attr_value

[ no ] sgsn-ip operator subscription-attribute subs_prof_attr_value
```

---

**no**

Removes the specified condition definition.

**operator**

Specifies how to logically match the information in the analyzed field.

- `!=`: Does not equal
- `==`: Equals

**in-range**

Specifies the condition to accept the IP address which are in range as argument to define the SGSN address which is used by subscriber in IP-CAN session.

**!in-range**

Specifies the condition to accept the IP address which are NOT in range as argument to define the SGSN address which is used by subscriber in IP-CAN session.

**range_start_ip**

Specifies the starting IP address which is used for defining the range of SGSN IP addresses which is used by subscriber in IP-CAN session.

`range_start_ip` is an IP address and must be lesser than `end_start_ip` address.
range_end_ip

Specifies the ending IP address which is used for defining the range of SGSN IP addresses which is used by subscriber in IP-CAN session.

*range_end_ip* is an IP address and must be greater than *end_start_ip* address.

gsn_ip/mask

Specifies the IP address of the SGSN which is used by subscriber in IP-CAN session along with IP mask as well.

*gsn_ip* must be an IP address in IPv4 or IPv6 notation.

*mask* specifies the IP address mask bits to determine the number of IP addresses of SGSN in condition. *mask* must be specified using the standard IPv4 dotted decimal notation.

profile-attribute spr_attr_value

Specifies the profile attribute value in SPR to match with SGSN IP address in an IP-CAN session as condition.

*spr_attr_value* must be an alphanumeric string of from 1 through 63 characters.

subscription-attribute subs_prof_attr_value

Specifies the subscriber profile attribute parameter value to match with SGSN IP address in an IP-CAN session as condition.

*subs_prof_attr_value* must be an alphanumeric string of from 1 through 31 characters.

Usage

Use this command to define a condition based on the SGSN IP address used by subscriber in an IP-CAN session.

Example

The following command creates a condition definition to analyze the condition based on SGSN IP address 1.2.3.4 in an IP-CAN session:

```
sgsn-ip = 1.2.3.4
```
sgsn-mcc-mnc

This command defines a condition based on the PLMN (MCC+MNC) of SGSN on which subscriber is attached in an IP-CAN session.

Product
IPCF

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Condition Group Configuration

configure > context context_name > pcc-service service_name > condition group group_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pcc-condition-group)#

Syntax

[ no ] sgsn-mcc-mnc operator {mcc mcc_value [mnc mnc_value] | [mcc mcc_value] mnc mnc_value}

[ no ] sgsn-mcc-mnc operator profile-attribute spr_attr_value

[ no ] sgsn-mcc-mnc operator subscription-attribute subs_prof_attr_value

---

no

Removes the specified condition definition.

operator

Specifies how to logically match the information in the analyzed field.
operator must be one of the following:
• !=: Does not equal
• ==: Equals

mcc mcc_value

 Specifies the Mobile Country Code in PLMN of SGSN which is used by subscriber in IP-CAN session.
mcc_value must be an integer between 101 and 998.

mnc mnc_value

Specifies the Mobile Network Code in PLMN of SGSN which is used by subscriber in IP-CAN session.
mnc_value must be an integer between 1 and 998.

profile-attribute spr_attr_value

Specifies the profile attribute value in SPR to match with PLMN of SGSN used by subscriber in an IP-CAN session as condition.
spr_attr_value must be an alphanumeric string of from 1 through 63 characters.
subscription-attribute subs_prof_att_value

Specifies the subscriber profile attribute parameter value to match with PLMN of SGSN used by subscriber in an IP-CAN session as condition.

`subs_prof_att_value` must be an alphanumeric string of from 1 through 31 characters.

### Usage

Use this command to define a condition based on the PLMN of SGSN used by subscriber in an IP-CAN session.

### Example

The following command creates a condition definition to analyze the condition based on PLMN of SGSN with MCC as 102 and MNC as 99 in an IP-CAN session:

```
sgsn-mcc-mnc = mcc 102 mnc 99
```
subscription-attribute

This command defines a condition based on the matching between subscriber subscription attribute value and SPR attribute value in an IP-CAN session.

Product
IPCF

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Condition Group Configuration

configure > context context_name > pcc-service service_name > condition group group_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pcc-condition-group)#

Syntax

[no] subscription-attribute subscription_attr_value operator spr_attr_value

- **no**
  Removes the specified condition definition.

- **subscription_attr_value**
  Specifies the subscriber subscription attribute value to match with SPR attribute for condition validation in an IP-CAN session. **subscription_attr_value** must be an alphanumeric string of from 1 through 31 characters.

- **operator**
  Specifies how to logically match the information in the analyzed field. **operator** must be one of the following:
  - !: Does not equal
  - =: Equals

- **spr_attr_value**
  Specifies the attribute value in SPR to match with subscriber subscription attribute for condition validation in an IP-CAN session. **spr_attr_value** must be an alphanumeric string of from 1 through 63 characters.

Usage

Use this command to define a condition based on the matching parameters between subscriber subscription attribute and SPR attribute value used in an IP-CAN session.

Example

...)
The following command creates a condition definition to analyze the condition based on matching of subscriber subscription attribute value `subs_gold_102` with SPR attribute value `spr_gold_101` in an IP-CAN session:

```
subscription.attribute subscribe_gold_102 = spr_gold_101
```
spr-profile-not-found

This command defines a condition based on the availability of SPR profile for a subscriber in an IP-CAN session.

Product
IPCF

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Condition Group Configuration

configure > context context_name > pcc-service service_name > condition group group_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pcc-condition-group)#

Syntax

[no] spr-profile-not-found

no

Removes the specified condition definition.

Usage
Use this command to define a condition based on the availability of SPR profile for a subscriber in an IP-CAN session.

Example
The following command creates a condition definition to analyze the condition if SPR profile is not available for a subscriber in an IP-CAN session:

spr-profile-not-found
threshold-condition usage-monitor

This command defines a condition based on the threshold conditions in usage of traffic by subscriber session in an IP-CAN session. It is used to support usage tracking and dynamic Policy control based on subscriber usage.

Product
IPCF

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Condition Group Configuration

configure > context context_name > pcc-service service_name > condition group group_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pcc-condition-group)#

Syntax

[ no ] threshold-condition usage-monitor usage_mon_name { time | vol-or-time | volume } usage operator { absolute value volume | subscription-limit | subscription-threshold subs_thres_limit }

no
Removes the specified condition definition.

usage_mon_name

Specifies a unique name for configured usage monitor condition which is used for evaluation with this condition group for user traffic in IP-CAN session.

usage_mon_name must be an alphanumeric string of 1 through 63 characters.

usage

This keyword specifies the condition as usage for threshold condition which is used for evaluation with this condition group for user traffic in IP-CAN session.

operator

Specifies how to logically match the information in the analyzed field.

operator must be one of the following:

- !=: Does not equal
- <=: Lesser than or equals
- =: Equals
- >=: Greater than or equals

{time | vol-or-time | volume }

This keywords sets the type of threshold; time or volume or both as condition definition for user traffic in IP-CAN session.
• **time**: This keyword sets the threshold condition to use time as condition definition for a user traffic in IP-CAN session.

• **vol-or-time**: This keyword sets the threshold condition to use time or volume as condition definition for a user traffic in IP-CAN session. The condition is matched if either of the two usage values fulfills the condition.

• **volume**: This keyword sets the threshold condition to use volume as condition definition for a user traffic in IP-CAN session.

---

**absolute value** `volume`

Specifies the threshold limit condition definition based on absolute usage `volume` in Kilo Bytes which is used for evaluation with this condition group for user traffic in IP-CAN session. `volume` must be an integer between 1 through 4294967295.

---

**subscription-limit**

Specifies the threshold limit condition based on Subscriber’s subscription limit which is used for evaluation with this condition group for user traffic in IP-CAN session. In this condition the system takes Subscriber’s subscription limit as defined in subscriber subscription policy for threshold limit monitoring.

---

**subscription-threshold** `subs_thres_limit`

Specifies the condition definition for threshold limit based on a configured usage monitor threshold named `subs_thres_limit` in IP-CAN session. `subs_thres_limit` is a pre-configured subscription limit in this configuration mode. This command allows the operator to use configured subscription limit as subset of a threshold condition.

---

**Usage**

Use this command to define a condition based on the duration of usage of service in seconds or volume usage in Bytes for user traffic in an IP-CAN session. This usage monitor is used to support usage tracking and dynamic Policy control based on subscriber usage.

IPCF supports the concept of Monitoring Key. PCEF, when instructed by PCRF, keeps track of usage per Monitoring Key. PCEF reports the usage when thresholds are reached or requested by PCRF. To allow operator to have dynamic Policy control, IPCF uses Usage Monitor. This Usage Monitor has attribute of volume-limit, time-limit or both. Operator can “associate” different Monitoring Keys to these usage monitors. It can be a Many-To-Many relationship between Usage-Monitor and Monitoring-Key. Operator can use Usage conditions on Usage Monitors instead of Monitoring Keys directly. IPCF tracks usage per usage-monitor. Different monitoring keys associated to a Usage-Monitor. When monitoring key is associated to a Usage-Monitor, the usage reported for that particular monitoring key is added to all the usage monitoring to which it is associated.

IPCF supports 2 types of usage monitors; it can be defined on IPCF or SSC supplied usage monitors. The name `usage_mon_name` identifies an usage-monitor, which is locally defined or received from SSC. The `absolute` value applies to both types of usage monitors. This command allows the operator to use configured threshold condition with another threshold condition as subset. A maximum of 8 thresholds can be configured per usage monitor.

---

**Example**

The following command creates a threshold condition with usage monitor name `threshold1` as usage monitor to trigger the condition based on the `subscription limit` as provide in Subscriber policy:
threshold-condition usage-monitor

threshold-condition usage-monitor threshold1 usage = subscription-limit
user-access-network

This command defines a condition based on the access location type of the subscriber in an IP-CAN session as received on Gx interface.

**Product**
IPCF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Condition Group Configuration

`configure > context context_name > pcc-service service_name > condition group group_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-condition-group)#
```

**Syntax**

```
[ no ] user-access-network operator value { home | roaming | visiting }
[ no ] user-access-network operator profile-attribute spr_attr_value
[ no ] user-access-network operator subscription-attribute subs_prof_attr_value
```

---

**no**
Removes the specified condition definition.

---

**operator**
Specifies how to logically match the information in the analyzed field.
`operator` must be one of the following:

- `!=`: Does not equal
- `==`: Equals

---

**value home**
Specifies the subscriber network access type as Home for condition validation in an IP-CAN session.
This condition contains all subscribers active in Home networks in this condition.

---

**value roaming**
Specifies the subscriber network access type as Roaming for condition validation in an IP-CAN session.
This condition contains all subscribers active in Roaming networks in this condition.

---

**value visiting**
Specifies the subscriber network access type as Visiting for condition validation in an IP-CAN session.
This condition contains all subscribers active in Visiting networks in this condition.
profile-attribute spr_attr_value

Specifies the profile attribute value in SPR to match with user access network condition validation in an IP-CAN session.

spr_attr_value must be an alphanumeric string of from 1 through 63 characters.

subscription-attribute subs_prof_attr_value

Specifies the subscriber profile attribute parameter value to match with user access network condition validation in an IP-CAN session.

subs_prof_attr_value must be an alphanumeric string of from 1 through 31 characters.

Usage

Use this command to define a condition based on the location of the user as defined in SPR attribute or subscriber profile attribute or location of user in Home, Roaming, Visiting in an IP-CAN session as received on Gx interface.

This configuration compares ULI and other location information from Gx data with the Home/roaming/visiting location as received from SSC. IPCF will also use global data as received from SSC in determining user access network through Subscriber profile attribute or SPR attribute in profile attribute.

Example

The following command creates a condition definition to analyze the condition based on location of the subscribes as roaming in an IP-CAN session:

user-access-network = value roaming
user-equipment-info esn

This command defines a condition based on the Electronic Serial Number (ESN) used for the identification of mobile device (UE) in a Non-3GPP IP-CAN session received over Gx interface between PDSN and IPCF.

**Product**
IPCF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Condition Group Configuration

```
configure > context context_name > pcc-service service_name > condition group group_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-condition-group)#
```

**Syntax**

```
[ no ] user-equipment-info esn  operator value esn
[ no ] user-equipment-info esn  operator profile-attribute spr_attr_value
[ no ] user-equipment-info esn  operator subscription-attribute subs_prof_attr_value
```

---

**no**

Removes the specified condition definition.

**operator**

Specifies how to logically match the information in the analyzed field.

*operator* must be one of the following:

- !=: Does not equal
- ==: Equals

**esn**

Specifies the Electronic Serial Number used for the identification of UE in 64 bit format as condition value for UE information received over Gx interface in a Non-3GPP IP-CAN session.

*esn* must be a 15 character long string of Hexadecimal numbers only.

**profile-attribute spr_attr_value**

Specifies the profile attribute value in SPR to match with ESN of the UE in an IP-CAN session as condition.

*spr_attr_value* must be an alphanumeric string of from 1 through 63 characters.

**subscription-attribute subs_prof_attr_value**

Specifies the subscriber profile attribute parameter value to match with ESN of the UE in an IP-CAN session as condition.

*subs_prof_attr_value* must be an alphanumeric string of from 1 through 31 characters.
Usage

Use this command to define a condition based on the ESN of the UE received over Gx interface in a Non-3GPP IP-CAN session between PDSN and IPCF.

Example

The following command creates a condition definition to analyze the condition based on the ESN of the UE as 1234567890120AF in a Non-3GPP IP-CAN session:

```
user-equipment-info esn = 1234567890120AF
```
user-equipment-info eui64

This command defines a condition based on the Extended Unique Identifier in 64 bit (EUI-64) used for the identification of mobile device (UE) in an IP-CAN session received over Gx interface.

**Syntax**

```plaintext
[ no ] user-equipment-info eui64 operator value eui64
[ no ] user-equipment-info eui64 operator profile-attribute spr_attr_value
[ no ] user-equipment-info eui64 operator subscription-attribute subs_prof_attr_value
```

- **no**
  - Removes the specified condition definition.

- **operator**
  - Specifies how to logically match the information in the analyzed field.
  - `!=`: Does not equal
  - `==`: Equals

- **eui64**
  - Specifies the Extended Unique Identifier in 64 bit format as a condition value for UE information received over Gx interface in an IP-CAN session.
  - `eui64` is a 16 character long string of Hexadecimal numbers only.

- **profile-attribute spr_attr_value**
  - Specifies the profile attribute value in SPR to match with EUI-64 value of the UE in an IP-CAN session as condition.
  - `spr_attr_value` must be an alphanumeric string of from 1 through 63 characters.

- **subscription-attribute subs_prof_attr_value**
  - Specifies the subscriber profile attribute parameter value to match with EUI-64 value of the UE in an IP-CAN session as condition.
user-equipment-info eui64

subs_prof_attr_value must be an alphanumeric string of from 1 through 31 characters.

Usage

Use this command to define a condition based on the EUI-64 value of the UE received over Gx interface in an IP-CAN session between PCEF and IPCF.

Example

The following command creates a condition definition to analyze the condition based on the EUI-64 of the UE as 0012989099832345 in an IP-CAN session:

user-equipment-info eui64 = 0012989099832345
user-equipment-info imeisv

This command defines a condition based on the International Mobile Equipment Identity Software Version (IMEI-SV) used for the identification of mobile device (UE) in an IP-CAN session received over Gx interface.

Product  
IPC

Privilege  
Security Administrator, Administrator

Mode  
Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Condition Group Configuration

configure > context context_name > pcc-service service_name > condition group group_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pcc-condition-group)#

Syntax

[ no ] user-equipment-info imeisv  operator value imei_sv
[ no ] user-equipment-info imeisv  operator profile-attribute spr_attr_value
[ no ] user-equipment-info imeisv  operator subscription-attribute subs_prof_attr_value

no

Removes the specified condition definition.

operator

Specifies how to logically match the information in the analyzed field.
operator must be one of the following:
• !=: Does not equal
• ==: Equals

imei_sv

Specifies the International Mobile Equipment Identity Software Version (IMEI-SV) as a condition value for UE information received over Gx interface in an IP-CAN session.
imei_sv is a 16 digit long string of decimal numbers only.

profile-attribute spr_attr_value

Specifies the profile attribute value in SPR to match with IMEI-SV value of the UE in an IP-CAN session as condition.
spr_attr_value must be an alphanumerical string of 63 characters.

subscription-attribute subs_prof_attr_value

Specifies the subscriber profile attribute parameter value to match with IMEI-SV value of the UE in an IP-CAN session as condition.
user-equipment-info imeisv

\[ subs_prof_attr_value \] must be an alphanumeric string of from 1 through 31 characters.

Usage

Use this command to define a condition based on the IMEI-SV value of the UE received over Gx interface in an IP-CAN session between PCEF and IPCF.

Example

The following command creates a condition definition to analyze the condition based on the IMEI-SV of the UE as 0012989099832345 in an IP-CAN session:

\[ \text{user-equipment-info eui64} = 0012989099832345 \]
user-equipment-info mac

This command defines a condition based on the Media Access Control (MAC) address used for the UE information in an IP-CAN session as received over Gx interface.

Product
IPCF

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Condition Group Configuration

configure > context context_name > pcc-service service_name > condition group group_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pcc-condition-group)#

Syntax

[ no ] user-equipment-info mac operator value mac_value
[ no ] user-equipment-info mac operator profile-attribute spr_at_value
[ no ] user-equipment-info mac operator subscription-attribute subs_prof_attr_value

---

no

Removes the specified condition definition.

operator

Specifies how to logically match the information in the analyzed field.

operator must be one of the following:

• !=: Does not equal
• ==: Equals

mac_value

Specifies the Media Access Control (MAC) address as condition value for UE information received over Gx interface in an IP-CAN session.

mac_value is a 17 character long string of Hexadecimal numbers in xx:xx:xx:xx:xx:xx format only.

profile-attribute spr_at_value

Specifies the profile attribute value in SPR to match with MAC value of the UE in an IP-CAN session as condition.

spr_at_value must be an alphanumeric string of from 1 through 63 characters.

subscription-attribute subs_prof_attr_value

Specifies the subscriber profile attribute parameter value to match with MAC value of the UE in an IP-CAN session as condition.
subs_prof_attr_value must be an alphanumeric string of from 1 through 31 characters.

Usage
Use this command to define a condition based on the MAC address value as UE information received over Gx interface in an IP-CAN session.

Example
The following command creates a condition definition to analyze the condition based on the MAC value of the UE as 00:12:98:90:99:83 in an IP-CAN session:

```
user-equipment-info mac = 00:12:98:90:99:83
```
user-equipment-info meid

This command defines a condition based on the Mobile Equipment Id (MEID) used for the identification of CDMA mobile device (UE) in a Non-3GPP IP-CAN session received over Gx interface between PDSN and IPCF.

**Product**
IPCF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Condition Group Configuration

configure > context context_name > pcc-service service_name > condition group group_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pcc-condition-group)#

**Syntax**

```
[ no ] user-equipment-info meid operator value me_id
[ no ] user-equipment-info meid operator profile-attribute spr_attr_value
[ no ] user-equipment-info meid operator subscription-attribute subs_prof_attr_value
```

<table>
<thead>
<tr>
<th>no</th>
</tr>
</thead>
<tbody>
<tr>
<td>Removes the specified condition definition.</td>
</tr>
</tbody>
</table>

**operator**

Specifies how to logically match the information in the analyzed field. 
(operator must be one of the following: 
• !=: Does not equal 
• ==: Equals

**me_id**

Specifies the Mobile Equipment identifier used for the identification of UE in 64 bit format as condition value for UE information received over Gx interface in a Non-3GPP IP-CAN session. 
me_id must be a 14 character long string of Hexadecimal numbers only.

**profile-attribute spr_attr_value**

Specifies the profile attribute value in SPR to match with Mobile Equipment id of the UE in an IP-CAN session as condition. 
spr_attr_value must be an alphanumeric string of from 1 through 63 characters.

**subscription-attribute subs_prof_attr_value**

Specifies the subscriber profile attribute parameter value to match with Mobile Equipment id of the UE in an IP-CAN session as condition.
user-equipment-info meid

subs_prof_attr_value must be an alphanumeric string of from 1 through 31 characters.

Usage
Use this command to define a condition based on the MEID of the CDMAUE received over Gx interface in a Non-3GPP IP-CAN session between PDSN and IPCF.

Example
The following command creates a condition definition to analyze the condition based on the MEID of the CDMA UE as 123456780120AF in a Non-3GPP IP-CAN session:

```plaintext
user-equipment-info meid = 123456780120AF
```
user-equipment-info modified-eui64

This command defines a condition based on the modified-Extended Unique Identifier in 64 bit (EUI-64) used for the identification of mobile device (UE) in an IP-CAN session received over Gx interface.

Product
IPCF

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Condition Group Configuration

configure > context context_name > pcc-service service_name > condition group group_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pcc-condition-group)#

Syntax

[ no ] user-equipment-info modified-eui64 operator value meui64
[ no ] user-equipment-info modified-eui64 operator profile-attribute spr_attr_value
[ no ] user-equipment-info modified-eui64 operator subscription-attribute subs_prof_attr_value

no
Removes the specified condition definition.

operator
Specifies how to logically match the information in the analyzed field.
operator must be one of the following:

• !=: Does not equal
• ==: Equals

meui64
Specifies the modified Extended Unique Identifier (EUI) in 64 bit format as condition value for UE information received over Gx interface in an IP-CAN session.
meui64 is a 16 character long string of Hexadecimal numbers only.

profile-attribute spr_attr_value
Specifies the profile attribute value in SPR to match with modified EUI-64 value of the UE in an IP-CAN session as condition.
spr_attr_value must be an alphanumeric string of from 1 through 63 characters.
subscription-attribute subs_prof_attr_value

Specifies the subscriber profile attribute parameter value to match with modified EUI-64 value of the UE in an IP-CAN session as condition.

subs_prof_attr_value must be an alphanumeric string of from 1 through 31 characters.

Usage

Use this command to define a condition based on the modified EUI-64 value of the UE received over Gx interface in an IP-CAN session between PCEF and IPCF.

Example

The following command creates a condition definition to analyze the condition based on the EUI-64 of the UE as 0012989099832345 in an IP-CAN session:

```
user-equipment-info modified-eui64 = 0012989099832345
```
user-location-info

This command defines a condition based on the UE location used in an IP-CAN session as received on \texttt{Gx} interface.

**Product**

IPCF

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Condition Group Configuration

```
configure > context context_name > pcc-service service_name > condition group group_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-condition-group)#
```

**Syntax**

```
[no] user-location-info \{cgi operator mcc mcc_value mnc mnc_value lac lac_value ci ci_value | ecgi operator mcc mcc_value mnc mnc_value ecgi ecgi_value | rai operator mcc mcc_value mnc mnc_value lac lac_value rai rai_value| sai operator mcc mcc_value mnc mnc_value lac lac_value sac sac_value| tai operator mcc mcc_value mnc mnc_value tai tai_value\}
```

- **no**
  - Removes the specified condition definition.

  ```
  no
  ```

- **cgi**
  - Specifies the Cell Global Identifier in UE location received over \texttt{Gx} interface in an IP-CAN session.

  ```
  cgi
  ```

- **ecgi**
  - Specifies the E-UTRAN Cell Global Identifier in UE location received over \texttt{Gx} interface in an IP-CAN session.

  ```
  ecgi
  ```

- **rai**
  - Specifies the Routing Area Identifier in UE location received over \texttt{Gx} interface in an IP-CAN session.

  ```
  rai
  ```

- **sai**
  - Specifies the Service Area Identifier in UE location received over \texttt{Gx} interface in an IP-CAN session.

  ```
  sai
  ```

- **tai**
  - Specifies the Tracking Area Identifier in UE location received over \texttt{Gx} interface in an IP-CAN session.

  ```
  tai
  ```

- **operator**
  - Specifies how to logically match the information in the analyzed field.

  ```
  operator
  ```

  \textit{operator} must be one of the following:
- !=: Does not equal
- ==: Equals

mcc mcc_value
Specifies the Mobile Country Code used in UE location information received over Gx interface in IP-CAN session.
mcc_value must be an integer between 101 through 998.

mnc mnc_value
Specifies the Mobile Network Code used in UE location information received over Gx interface in IP-CAN session.
mnc_value must be an integer between 1 through 998.

lac lac_value
Specifies the Location Area Code used in UE location information received over Gx interface in IP-CAN session.
lac_value must be an integer between 1 through 65535.

ci ci_value
Specifies the Cell Identifier used in UE location information received over Gx interface in IP-CAN session.
ci_value must be an integer between 1 through 65535.

ecgi ecgi_value
Specifies the E-UTRAN Cell Global Identifier used in UE location information received over Gx interface in IP-CAN session.
ecgi_value must be an integer between 1 through 1048575.

rai rai_value
Specifies the Routing Area Identifier used in UE location information received over Gx interface in IP-CAN session.
rai_value must be an integer between 1 through 65535.

sac sac_value
Specifies the Service Area Code used in UE location information received over Gx interface in IP-CAN session.
sac_value must be an integer between 1 through 65535.

tai tai_value
Specifies the Tracking Area Code used in UE location information received over Gx interface in IP-CAN session.
tai_value must be an integer between 1 through 65535.

Usage
Use this command to define a condition based on the UE location information received over Gx interface in an IP-CAN session.

Example
The following command creates a condition definition to analyze the condition based on the RAI received for UE location in an IP-CAN session:

```
user-location-info rai = mcc 102 mnc 99 lac 1003 rai 3521
```
Chapter 236
PCC-Data-Service Configuration Mode Commands

The PCC-Data-Service Configuration Mode is used to configure the data flow parameters for the media data, as well as corresponding attributes that are necessary for charging and policy enforcement decisions for the media parameters represented by its service flows in the PCC-service. A maximum of ten service data flows can be configured in a PCC-Data-Service instance.

**Important:** This configuration mode is supported from StarOS Release 12.1 onward.

Mode

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Data Service Configuration
\n**configure** > **context** **context_name** > **pcc-service** **service_name** > **data-service** **service_name**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-data-service)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
**end**

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
end

**Usage**
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Use this command to return to the parent configuration mode.
flow direction in

This command configures the flow service parameters for incoming data flow in PCC-Data-Service instance.

**Product**
IPCF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Data Service Configuration

configure > context context_name > pcc-service service_name > data-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pcc-data-service)#

**Syntax**

```
[no] flow direction in protocol {ip | tcp | udp} from {src_ip_addr[/maskbit] | any} port {src_port_num | any} to {dest_ip_addr[maskbit] | any} port {dest_port_num | any}
```

*no*

Removes the configured data service flow parameters from PCC-Data-Service instance for IPCF configuration.

**protocol {ip | tcp | udp}**

This keyword configures the data flow parameters for specific protocol. Following protocols are supported through this keyword:

- **ip**: Sets the parameters for IP traffic.
- **tcp**: Sets the parameters for TCP traffic.
- **UDP**: Sets the parameters for UDP traffic.

*from {src_ip_addr[/maskbit] | any} port {src_port_num | any} to {dest_ip_addr[maskbit] | any} port {dest_port_num | any}*

This keyword configures the data flow condition parameters for specific protocol through IP address and port as source of flow. Following parameters are defined with this keyword:

- **src_ip_addr**: specifies the specific IP address in IPv4/IPv6 notation as source of flow.
- **maskbit**: Specifies the IP address suffix in IPv4 or IPv6 notation.
- **any**: specifies that flow from any source IP address/port can be analyzed or considered.
- **port src_port_num**: specifies the specific source port parameter for flow.
  
  src_port_num is the source port number of flow and must be an integer from 1 through 65535.
flow direction in protocol tcp from any port any to any port any
flow direction out

This command configures the flow service parameters for outgoing data flow in PCC-Data-Service instance.

**Product**
IPCF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Data Service Configuration

configure > context <context_name> > pcc-service <service_name> > data-service <service_name>

Entering the above command sequence results in the following prompt:

```
[<context_name>]host_name(config-pcc-data-service)#
```

**Syntax**

```
[no] flow direction in protocol {ip | tcp | udp} from {src_ip_addr [ /maskbit] | any} port {src_port_num | any} to {dest_ip_addr [ /maskbit] | any} port {dest_port_num | any}
```

**no**
Removes the configured data service flow parameters from PCC-Data-Service instance on IPCF node.

```
protocol {ip | tcp | udp}
```

This keyword configures the data flow parameters for specific protocol.

Following protocols are supported through this keyword:

- **ip**: Sets the parameters for IP traffic.
- **tcp**: Sets the parameters for TCP traffic.
- **UDP**: Sets the parameters for UDP traffic.

```
from {src_ip_addr | any} port {src_port_num | any}
```

This keyword configures the data flow condition parameters for specific protocol through IP address and port as source of flow.

Following parameters are defined with this keyword:

- **src_ip_addr**: specifies the specific IP address in IPv4/IPv6 notation as source of flow.
- **maskbit**: Specifies the IP address suffix in IPv4 or IPv6 notation.
- **any**: specifies that flow from any source IP address/port can be analyzed or considered.
- **port src_port_num**: specifies the specific source port parameter for flow.

```
src_port_num is the source port number of flow and must be an integer from 1 through 65535.
```

```
to {dest_ip_addr | any} port {dest_port_num | any}
```

This keyword configures the data flow condition parameters for specific protocol through IP address and port as source of flow.
Following parameters are defined with this keyword:

- `dest_ip_addr`: specifies the specific IP address in IPv4/IPv6 notation as destination of flow.
- `maskbit`: Specifies the IP address suffix in IPv4 or IPv6 notation.
- `any`: specifies that flow to any destination IP address/port can be analyzed or considered.
- `port dest_port_num`: specifies the specific destination port parameter for flow.
  
  `dest_port_num` is the destination port number of flow and must be an integer from 1 through 65535.

### Usage

Use this command to configure the flow service parameters for outgoing data flow in PCC-Data-Service instance on IPCF node.

### Example

Following command sets the data service parameters for `tcp` type protocol from `any` IP/port source to `any` IP/port in outgoing direction with in a PCC-Data-Service.

```
flow direction out protocol tcp from any port any to any port any
```
metering-method

This command specifies the metering method to be used by PCEF for offline charging in a PCC-Data-Service instance on IPCF node.

Product
IPCF

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Data Service Configuration

configure > context context_name > pcc-service service_name > data-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pcc-data-service)#

Syntax

[no] metering-method {both-duration-volume | duration | volume}

- no
  Removes the configured metering method from PCC-Data-Service instance on IPCF node.
  In such scenario, the metering method pre-configured at PCEF is considered.

- both-duration-volume
  Specifies the metering method as based on volume of data usage and duration of session, both for offline charging in a PCC-Data-Service instance on IPCF node.

- duration
  Specifies the metering method as based on the duration of session usage for offline charging in a PCC-Data-Service instance on IPCF node.

- volume
  Specifies the metering method as based on the volume of data usage for offline charging in a PCC-Data-Service instance on IPCF node.

Usage

Use this command to define the metering method to be used for offline charging in a PCC-Data-Service instance on IPCF node.
If no metering method is defined, the metering method preconfigured at PCEF is considered.

Example

Following command sets the metering method as based on volume of data usage and duration of session, both for offline charging in a PCC-Data-Service instance on IPCF node.

    metering-method both-duration-volume
monitoring-key

This command defines the monitoring key under which data is monitored for the PCC-Data-Service instance.

Product
IPCF

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Data Service Configuration

configure > context context_name > pcc-service service_name > data-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pcc-data-service)#

Syntax

monitoring-key mon_key_value

[no] monitoring-key

---

no

Removes the configured monitoring-key from PCC-Data-Service instance on IPCF node.

mon_key_value

Specifies the monitoring key value under which data usage is monitored for the PCC-Data-Service instance and must be an integer from 1 through 65535.

Usage

Use this command to define the monitoring key under which data is monitored for the PCC-Data-Service instance on IPCF node.

Example

Following command sets the monitoring key 123 for data monitoring in PCC-Data-Service instance on IPCF node.

  monitoring-key 123
precedence

This command defines the precedence that is assigned to the Dynamic PCC rule created for a PCC-Data-Service instance.

Product
IPCF

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Data Service Configuration

configure > context context_name > pcc-service service_name > data-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pcc-data-service)#

Syntax

precedence preced_value

[no] precedence

no

Removes the configured precedence value from PCC-Data-Service instance on IPCF node.

preced_value

Specifies the precedence that is assigned to the dynamic PCC rule created for a PCC-Data-Service instance and must be an integer from 1 through 65535.

Usage

Use this command to define the precedence value that is assigned to the Dynamic PCC rule created for a PCC-Data-Service instance on IPCF node.

Example

Following command sets the precedence value 2 to assign to the dynamic PCC rule created for a PCC-Data-Service instance on IPCF node.

precedence 2
qos-profile

This command defines the PCC-QoS-Profile which is to use for the PCC-Data-Service instance on IPCF node.

Product
IPCF

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Data Service Configuration

configure > context context_name > pcc-service service_name > data-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pcc-data-service)#

Syntax

qos-profile qos_prof_name

[no] qos-profile

no

Removes the configured PCC-QoS-Profile from PCC-Data-Service instance on IPCF node.

qos_prof_name

Specifies the pre-configured PCC-QoS-Profile name which is to use for the PCC-Data-Service instance.

Usage

Use this command to define the PCC-QoS-Profile for a PCC-Data-Service instance on IPCF node.

Example

Following command sets the PCC-QoS-Profile ipcf_qos_prof1 for PCC-Data-Service instance on IPCF node.

qos-profile ipcf_qos_prof1
rating-group

This command defines the PCC-Rating-Group that is assigned for a PCC-Data-Service instance.

**Product**
IPCF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Data Service Configuration

configure > context context_name > pcc-service service_name > data-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pcc-data-service)#

**Syntax**

```
rating-group rating_grp_id

[no] rating-group
```

- **no**
  Removes the configured PCC-Rating-Group Id from PCC-Data-Service instance on IPCF node.

- **rating_grp_id**
  Specifies the PCC-Rating-Group Id that is assigned to the PCC-Data-Service instance and must be an integer from 1 through 99.

**Usage**

Use this command to define the PCC-Rating Id value for a PCC-Data-Service instance on IPCF node.

**Example**

Following command sets the Rating Group id 11 for a PCC-Data-Service instance on IPCF node.

```
rating-group 11
```
reporting-level

This command specifies the reporting level to be used by PCEF to report the data usage for the related PCC rule in a PCC-Data-Service instance on IPCF node.

Product
IPCF

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Data Service Configuration

configure > context context_name > pcc-service service_name > data-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pcc-data-service)#

Syntax

[no] reporting-level {service-identifier-level | rating-group-level}

no
Removes the configured usage reporting level from PCC-Data-Service instance on IPCF node. In such scenario, the reporting level configured at PCEF is considered.

service-identifier-level
Sets the data usage reporting level to be used by PCEF to report the data usage for the related PCC rule at the service identifier level in a PCC-Data-Service instance on IPCF node.

ingroup-level
Sets the data usage reporting level to be used by PCEF to report the data usage for the related PCC rule at the Rating-group level in a PCC-Data-Service instance on IPCF node.

Usage
Use this command to define the reporting level to be used by PCEF to report the data usage for the related PCC rule in a PCC-Data-Service instance on IPCF node. If no reporting level is defined, the reporting level preconfigured at PCEF is considered.

Example

Following command sets the reporting level at ‘Rating-group’ level which is to be used by PCEF to report the data usage for the related PCC rule in a PCC-Data-Service instance on IPCF node.

    reporting-level rating-group-level
service-identifier

This command defines the service identifier for a PCC-Data-Service instance.

**Product**
IPCF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Data Service Configuration

`configure > context context_name > pcc-service service_name > data-service service_name`

Entering the above command sequence results in the following prompt:

```plaintext
[context_name]host_name(config-pcc-data-service)#
```

**Syntax**

```
service-identifier svc_id

[no] service-identifier
```

### no
Removes the configured Service Identifier from PCC-Data-Service instance on IPCF node.

### svc_id
Specifies the Service Identifier that is assigned to the PCC-Data-Service instance and must be an integer from 1 through 65535.

**Usage**

Use this command to define the Service Identifier for a PCC-Data-Service instance on IPCF node.

**Example**

Following command sets the Service Identifier 1011 for a PCC-Data-Service instance on IPCF node.

```
service-identifier 1011
```
Chapter 237
PCC-Event-Notification-Interface-Endpoint Configuration Mode Commands

The PCC-Event-Notification-Interface-Endpoint configuration mode is used to enable the event notification interface mechanism for the Intelligent Policy Control Function (IPCF) and to configure the Event Notification collection server endpoint related parameters.

**Important:** This configuration mode is supported from StarOS Release 12.1 onward.

---

**Mode**

```
Exec > Global Configuration > Context Configuration > Event Notification Interface Endpoint Configuration
```

```
configure > context context_name > event-notif-endpoint endpoint_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ntfyintf-endpoint)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
address

This command binds an IP address to the local IPCF node which is to be used for event notification processing with remote event collection server endpoint during IP-CAN session in PCC-Event-Notification-Interface-Endpoint instance.

Product
IPCF

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Event Notification Interface Endpoint Configuration

configure > context context_name > event-notif-endpoint endpoint_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ntfyintf-endpoint)#

Syntax

address ip_address

ip_address

Specifies the IP address bind with local IPCF node to be used by the event collection server endpoint for event message processing during IP-CAN session in PCC-Event-Notification-Interface-Endpoint instance.

Usage
Use this command to bind an IP address to interact with the remote event notification collection server endpoint to which the event messages are sent for IP-CAN session events.

Example
Following command binds the 1.2.3.4 for event notification message with remote event notification endpoint.

address 1.2.3.4
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**
Use this command to return to the Exec mode.
**exit**

Exits the current mode and returns to the parent configuration mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

```bash
exit
```

**Usage**

Use this command to return to the parent configuration mode.
peer name

This command binds/associates a remote Event Notification collection server as peer having specified IP address and optionally port for event notification during IP-CAN session in PCC-Event-Notification-Interface-Endpoint instance.

Product
IPCF

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Event Notification Interface Endpoint Configuration

configure > context context_name > event-notif-endpoint endpoint_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ntfyintf-endpoint)#

Syntax

peer name peer_name address ip_address [port port_num]

name peer_name

Sets the in PCC-Event-Notification-Interface-Endpoint instance to use a particular peer node configured by a peer name peer_name for event notification interface.
The peer_name is name of the peer node to be sued for event collection and must be an alphanumerical string from 1 through 31 characters. peer_name allows punctuation marks.

ip-address ip_address

Sets the PCC-Event-Notification-Interface-Endpoint instance to bind the particular peer node name with IP address ip_address in IPv4 or IPv6 notation for event notification message processing.
The ip_address is an IP address in IPv4/IPv6 notation.

port port_num

This optional keyword sets a particular port number to be used with in the PCC-Event-Notification-Interface-Endpoint instance to configure a particular peer node having a pre assigned IP address ip_address in IPv4 or IPv6 notation for event notification message processing.
The port_num must be an integer between 1 and 65535.

Usage

Use this command to bind/associate a remote Event Notification collection server as peer having specified IP address and optionally port for event notification during IP-CAN session in the PCC-Event-Notification-Interface-Endpoint instance.
Multiple peers can be configured using this command and peer selection methods, primary-secondary or round-robin can be applied using peer select-algorithm command for event notification during IP-CAN session in this configuration mode.

Example
Following command configures and associates an Event Notification peer node named \textit{event_peer_1} having an IP address 1.2.3.4 with port number as 2345 in an PCC-Event-Notification-Interface-Endpoint instance.

peer name event_peer_1 ip-address 1.2.3.4 port 2345
**peer select-algorithm**

This command applies the peer selection algorithm to select the configured remote Event Notification collection server during IP-CAN session in PCC-Event-Notification-Interface-Endpoint instance.

**Product**

IPC

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > Event Notification Interface Endpoint Configuration

```bash
configure > context context_name > event-notif-endpoint endpoint_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ntfyintf-endpoint)#
```

**Syntax**

```
peer select-algorithm {primary-secondary | round-robin}
```

<table>
<thead>
<tr>
<th>primary-secondary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sets the PCC-Event-Notification-Interface-Endpoint peer selection algorithm to select the configured remote peer servers in primary and secondary method during IP-CAN session in PCC-Event-Notification-Interface-Endpoint instance. This mode is applicable only when multiple peers are configured and primary and secondary peer is defined using <code>peer select-peer</code> command in this configuration mode.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>round-robin</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sets the PCC-Event-Notification-Interface-Endpoint peer selection algorithm to select the configured remote peer servers in round-robin method mode during IP-CAN session in PCC-Event-Notification-Interface-Endpoint instance. This mode is applicable only when multiple peers are configured in this configuration mode.</td>
</tr>
</tbody>
</table>

**Usage**

Use this command apply the peer selection algorithm to select the configured remote Event Notification collection server during IP-CAN session in PCC-Event-Notification-Interface-Endpoint instance.

**Example**

Following command configures the peer selection algorithm to select the configured remote peer in `round-robin` method in PCC-Event-Notification-Interface-Endpoint instance.

```
peer select-algorithm round-robin
```

Following command configures the peer selection algorithm to select the configured primary and secondary remote peers in `primary-secondary` method in PCC-Event-Notification-Interface-Endpoint instance.

```
peer select-algorithm primary-secondary
```
peer select-peer

This command sets the configured remote Event Notification collection server as primary and secondary servers for event notification collection during IP-CAN session in PCC-Event-Notification-Interface-Endpoint instance.

**Product**
IPCF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Event Notification Interface Endpoint Configuration
configure > context context_name > event-notif-endpoint endpoint_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ntfyintf-endpoint)#
```

**Syntax**

```
peer select-peer pri_peer_name secondary sec_peer_name
```

- **pri_peer_name**
  Sets the configured remote PCC-Event-Notification-Interface-Endpoint peer as primary peer for event notification collection during IP-CAN session in PCC-Event-Notification-Interface-Endpoint instance. `pri_peer_name` must be a pre-configured peer name configured with `peer name` command in this configuration mode.

- **secondary sec_peer_name**
  Sets the configured remote PCC-Event-Notification-Interface-Endpoint peer as secondary peer for event notification collection during IP-CAN session in PCC-Event-Notification-Interface-Endpoint instance. `sec_peer_name` must be a pre-configured peer name configured with `peer name` command in this configuration mode.

**Usage**

Use this command to set the configured remote Event Notification collection server as primary and secondary node for event notification collection during IP-CAN session in PCC-Event-Notification-Interface-Endpoint instance. This configuration is used when peer selection algorithm is set to `primary-secondary` using `peer select-algorithm` command in this configuration mode.

**Example**

Following command configures the specified peer `event1` as primary and `event2` as secondary node for event notification collection during IP-CAN session in PCC-Event-Notification-Interface-Endpoint instance.

```
peer select-peer event1 secondary event2
```
Chapter 238
PCC-Policy-Service Configuration Mode Commands

The PCC-Policy-Service Configuration mode provides a mechanism for the Intelligent Policy Control Function (IPCF) to manage the external interfaces required for policy authorization purpose between IPCF and PCEF Bearer Binding and Event Reporting Function (BBERF). The PCC-Policy-Service manages Gx/Gx based on the Diameter dictionary used.

**Important:** This configuration mode is supported from StarOS Release 12.1 onward.

**Mode**

Exec > Global Configuration > Context Configuration > PCC Policy Service Configuration

```
configure > context context_name > pcc-policy-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pccpolicy-service)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
associate pcc-service

This command associates a pre-configured PCC-Service with a PCC-Policy-Service for IPCF configuration.

Product
IPCF

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PCC Policy Service Configuration
configure > context context_name > pcc-policy-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pccpolicy-service)#

Syntax
associate pcc-service pcc_service_name

[no] associate pcc-service

no

Removes/disassociate the configured PCC-Service from this PCC-Policy-Service instance configured for IPCF configuration.

pcc_service_name

Specifies the name of a pre-configured PCC-Service configured in Context Configuration mode for IPCF configuration.
The pcc_service_name is name of a predefined PCC-Service instance and must be an alphanumerical string from 1 through 63 characters.

Usage
Use this command to associate a pre-configured PCC-Service instance for IPCF configuration.

Important: For more information on PCC-Service configuration, refer PCC-Service Configuration Mode Commands.

Example
Following command binds a PCC-Service named pcc_svc1 with in a PCC-Policy-Service.

associate pcc-service pcc_svc1

Following command removes an associated PCC-Service named pcc_svc1 from a PCC-Policy-Service.

no associate pcc-service pcc_svc1
diameter dictionary

This command assigns a Diameter dictionary for Gx/Gxa messaging with a PCC-Policy-Service for IPCF configuration.

**Product**
IPCF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PCC Policy Service Configuration

`configure > context context_name > pcc-policy-service service_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pccpolicy-service)#
```

**Syntax**

```
diameter dictionary {gxa-standard | r7-standard | standard}

default diameter dictionary
```

**default diameter dictionary**

```
default
Sets the Diameter Gx dictionary to default dictionary standard (3GPP Rel. 8 standard) for a PCC-Policy-Service instance configured for IPCF configuration.
```

```
gxa-standard
Default: Disabled
Sets the Diameter Gxa dictionary to be used by a PCC-Policy-Service instance configured for IPCF configuration over Gxa interface to 3GPP Rel. 8 standard.
```

```
r7-standard
Default: Disabled
Sets the Diameter Gx dictionary to be used by a PCC-Policy-Service instance configured for IPCF configuration over Gx interface to 3GPP Rel. 7 standard.
```

```
standard
Default: Enabled
Sets the Diameter Gx dictionary to be used by a PCC-Policy-Service instance configured for IPCF configuration over Gx interface to 3GPP Rel. 8 standard.
```

**Usage**

Use this command to configure the PCC-Policy-Service to determine which of the 3GPP dictionary to be used for Gx or Gxa interface messaging for policy and/or quota management.

**Example**

Following command sets the PCC-Policy-Service to use 3GPP Rel. 8 standard dictionary for Gx interface and policy management related messaging in a PCC-Policy-Service.
default diameter dictionary
diameter origin end-point

This command binds/associates a pre-configured Diameter host/realm (PCEF/BBERF) over Gx/Gxa interface with a PCC-Policy-Service to be used for subscriber service control and policy profile management.

Product
IPCF

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PCC Policy Service Configuration

configure > context context_name > pcc-policy-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pccpolicy-service)#

Syntax

diameter origin endpoint dia_endpoint_name

no diameter origin endpoint

no

Removes the associated Diameter Origin Endpoint configuration from PCC-Policy-Service instance configured for IPCF configuration.

any

Sets the PCC-Policy-Service instance to use any available PCEF/BBERF node for policy interfaces (Gx/Gx-like) support.

dia_endpoint_name

The dia_endpoint_name is a predefined Diameter origin endpoint node and must be an alphanumerical string from 1 through 63 characters.

Usage
Use this command to bind the PCEF/BBERF node over Gx/Gx-like interface by associating a pre-configured Diameter Origin Endpoint with a PCC-Policy-Service. The Diameter origin endpoint must be a pre-configured instance in the Context Configuration Mode. For more information on Diameter origin endpoint configuration, refer Diameter Endpoint Configuration Mode Commands chapter.

Example
Following command associates a pre-configured Diameter endpoint node configuration named pcef_1 with a PCC-Policy-Service for policy profile management.

diameter origin endpoint pcef_1
Following command removes the pre-associated Diameter endpoint node configuration named `pcef_1` with a PCC-Policy-Service.

```
no diameter origin endpoint
```
**ehrpd-access-bcm**

This command configures the PCC-Policy-Service to accept the applicable Bearer-Control-Mode for eHRPD access over Gxa interface on IPCF.

**Product**
IPCF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PCC Policy Service Configuration

```
configure > context context_name > pcc-policy-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pccpolicy-service)#
```

**Syntax**

```
ehrpd-access-bcm {as-requested | ue-nw | ue-only}
```

```
default ehrpd-access-bcm
```

<table>
<thead>
<tr>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>as-requested</td>
<td>Default: Enabled. Sets the PCC-Policy-Service to accept the Bearer-Control-Mode request from Application Server (AS) for eHRPD access over Gxa interface on IPCF node.</td>
</tr>
<tr>
<td>ue-nw</td>
<td>Default: Disabled. Sets the PCC-Policy-Service to accept the Bearer-Control-Mode request from UE and/or network element for eHRPD access over Gxa interface on IPCF node.</td>
</tr>
<tr>
<td>ue-only</td>
<td>Default: Disabled. Sets the PCC-Policy-Service to accept the Bearer-Control-Mode request from UE only for eHRPD access over Gxa interface on IPCF node.</td>
</tr>
</tbody>
</table>

**Usage**

Use this command to set the PCC-Policy-Service to accept the Bearer-Control-Mode request from AS or UE or Network for eHRPD access over Gxa interface on IPCF node.

**Example**

Following command sets the PCC-Policy-Service to accept the Bearer-Control-Mode request from AS for eHRPD access over Gxa interface on IPCF node.
default ehrpd-access-bcm

Following command sets the PCC-Policy-Service to accept the Bearer-Control-Mode request only from UE for eHRPD access over Gxa interface on IPCF node.

ehrpd-access-bcm ue-only
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

exit

**Usage**

Use this command to return to the parent configuration mode.
gprs-access-bcm

This command configures the PCC-Policy-Service to accept the applicable Bearer-Control-Mode for GPRS access over Gx interface on IPCF.

Product
IPCF

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PCC Policy Service Configuration
configure > context context_name > pcc-policy-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pccpolicy-service)#

Syntax

gprs-access-bcm {as-requested | ue-nw | ue-only}

default gprs-access-bcm

default
Sets the PCC-Policy-Service to accept the Bearer-Control-Mode request from Application Server (AS) for GGSN access over Gx interface on IPCF node.

as-requested
Default: Enabled.
Sets the PCC-Policy-Service to accept the Bearer-Control-Mode request from Application Server (AS) for GGSN access over Gx interface on IPCF node.

ue-nw
Default: Disabled.
Sets the PCC-Policy-Service to accept the Bearer-Control-Mode request from UE and/or network element for GGSN access over Gx interface on IPCF node.

ue-only
Default: Disabled.
Sets the PCC-Policy-Service to accept the Bearer-Control-Mode request from UE only for GGSN access over Gx interface on IPCF node.

Usage
Use this command to set the PCC-Policy-Service to accept the Bearer-Control-Mode request from AS or UE or Network for GGSN access over Gx interface on IPCF node.

Example
Following command sets the PCC-Policy-Service to accept the Bearer-Control-Mode request from AS for GGSN access over Gx interface on IPCF node.

    default gprs-access-bcm

Following command sets the PCC-Policy-Service to accept the Bearer-Control-Mode request only from UE for GGSN access over Gx interface on IPCF node.

    gprs-access-bcm ue-only
max policy-sessions

This command configure the maximum limit of the policy sessions allowed in a PCC-Policy-Service instance on IPCF.

Product
IPCF

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PCC Policy Service Configuration
configure > context context_name > pcc-policy-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pccpolicy-service)#

Syntax

max policy-sessions max_session

default max policy-sessions

default

Sets the maximum policy sessions allowed in PCC-Policy-Service instance to default value of 10000 sessions.

max_session

Default: 10000

Specifies the maximum number of policy sessions configured in PCC-Policy-Service to allow to be connected in PCC-Quota service instance.

max_session must be an integer between 0 and 4000000.

Usage

Use this command to set the maximum number of policy sessions allowed by a PCC-Policy-Service instance on IPCF.

Example

Following command sets the maximum number of policy sessions allowed in PCC-Policy-Service instance to 10000.

default max policy-sessions
**subscriber-binding-identifier**

This command specifies the subscriber binding identifier to be used by `bindmux` for binding different subscriber session to PCC-Policy-Service on IPCF node.

**Product**

IPCF

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > PCC Policy Service Configuration

```
configure > context context_name > pcc-policy-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pccpolicy-service)#
```

**Syntax**

```
subscriber-binding-identifier {imsi | msisdn | nai | sip-uri}
```

```
default subscriber-binding-identifier
```

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Sets the subscriber binding identifier to default value; i.e. IMSI, to be used by <code>bindmux</code> for binding different subscriber session to PCC-Policy-Service on IPCF node.</td>
</tr>
<tr>
<td>imsi</td>
<td>Default: Enabled. Sets the subscriber binding identifier as IMSI to be used by <code>bindmux</code> for binding different subscriber session to PCC-Policy-Service on IPCF node.</td>
</tr>
<tr>
<td>msisdn</td>
<td>Default: Disabled. Sets the subscriber binding identifier as MSISDN to be used by <code>bindmux</code> for binding different subscriber session to PCC-Policy-Service on IPCF node.</td>
</tr>
<tr>
<td>nai</td>
<td>Default: Disabled. Sets the subscriber binding identifier as Network Access Identifier (NAI) to be used by <code>bindmux</code> for binding different subscriber session to PCC-Policy-Service on IPCF node.</td>
</tr>
<tr>
<td>sip-uri</td>
<td>Default: Disabled. Sets the subscriber binding identifier as SIP URI (Uniform Resource Identifier) to be used by <code>bindmux</code> for binding different subscriber session to PCC-Policy-Service on IPCF node.</td>
</tr>
</tbody>
</table>
Usage
Use this command to configure the bindmux in PCC-Policy-Service instance on IPCF node to use specific subscriber identifier for binding different subscriber session to IP-CAN session.

Example
The following command sets the PCC-Policy-Service to use IMSI as subscriber binding identifier for IP-CAN session on an IPCF node.

```
default subscriber-binding-identifier
```
subscription-id-absence-action

This command configures the PCC-Policy-Service instance to handle the Initial Credit Control Request (CCR-I) messages during initial authentication over Gx interface when CCR-I message received by IPCF node is without a valid Subscription-Id AVP (IMSI, NAI, E164 etc.).

Product
IPCF

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PCC Policy Service Configuration

configure > context context_name > pcc-policy-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pccpolicy-service)#

Syntax

{default} subscription-id-absence-action initial-auth {continue | reject}

---

default

Sets the PCC-Policy-Service instance to reject the CCR-I message during initial authentication over Gx interface if received without a valid Subscription-Id AVP (IMSI, NAI, E164 etc.) on IPCF node.

---

continue

Default: Disabled.
Sets the PCC-Policy-Service instance to accept the CCR-I message and continue with the session if CCR-I is received without a valid Subscription-Id AVP (IMSI, NAI, E164 etc.) on IPCF node.
In this case, IPCF will receive the CCR-I message and will do the PCC provisioning as per the operator configuration in associated PCC-Service.

---

reject

Default: Enabled.
Sets the PCC-Policy-Service instance to reject the CCR-I message and continue with the session if CCR-I is received without a valid Subscription-Id AVP (IMSI, NAI, E164 etc.) on IPCF node.
In this case, IPCF will send CCA-I message with Result-code as Permanent Error and rejects the session establishment with PCEF.

Usage
Use this command to configure the PCC-Policy-Service instance to handle the Initial Credit Control Request (CCR-I) message processing during the initial authentication over Gx interface if CCR-I message received by IPCF node has no valid Subscription-Id AVP.

Example
The following command sets the PCC-Policy-Service to reject the CCR-I request and terminations the session establishment with PCEF.
default subscription-id-absence-action initial-auth
unsolicited-provisioning

This command is used to enable/disable the support for unsolicited time-of-day-based procedures to PCC-Policy-Service on IPCF node.

**Product**
IPCF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PCC Policy Service Configuration
configure > context context_name > pcc-policy-service service_name

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-pccpolicy-service)#`

**Syntax**

```
[no | default] unsolicited-provisioning time-of-day
```

- **default**
  Sets the support for unsolicited time-of-day-based procedures to default mode; i.e. disabled, in PCC-Policy-Service instance on IPCF node.

- **no**
  Removes the configured support for unsolicited time-of-day-based procedures in PCC-Policy-Service instance on IPCF node.

**Usage**

Use this command to enable/disable the support for unsolicited time-of-day-based procedures to PCC-Policy-Service on IPCF node.
By default this command is disabled.

**Example**

The following command enables the unsolicited time-of-day-based procedures to PCC-Policy-Service on an IPCF node.

```
unsolicited-provisioning time-of-day
```
Chapter 239
PCC-QoS-Profile Configuration Mode Commands

The PCC-QoS-Profile Configuration Mode is used to define the QoS logic used by the operator for managing the QoS policy requirements and objectives for the network specific to a group of subscribers in the network. A QoS Profile represents a resource requirement identified by means of the corresponding QoS attributes like QCI, MBR, GBR, ARP etc.

**Important:** This configuration mode is supported from StarOS Release 12.1 onward.

Mode

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC QoS Profile Configuration

configure > context context_name > pcc-service service_name > qos-profile profile_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pcc-qos-profile)#

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
arp-priority

This command is used to define the Allocation and Retention Priority (ARP) values of the QoS profile in PCC-QoS-Profile which is to use in Subscriber profile in PCC-Service instance on IPCF node.

**Product**
IPCF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC QoS Profile Configuration

```
configure > context context_name > pcc-service service_name > qos-profile profile_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-qos-profile)#
```

**Syntax**

```
[no] arp-priority arp_priority pre-emption {capable | not-capable} {not-vulnerable | vulnerable}
```

- **no**
  Removes the configured ARP priority set for PCC-QoS-Profile for PCC-Service instance on IPCF node.

- **arp-priority**
  Specifies the priority value for ARP in a PCC-QoS-Profile which is to use in Subscriber profile in PCC-Service instance on IPCF node.
  *arp_priority* must be an integer from 1 through 15.

- **pre-emption {capable | not-capable}**
  Sets the Pre-emption capability related parameters with ARP priority in PCC-QoS-Profile name which is to use in Subscriber profile in PCC-Service instance on IPCF node.
  Pre-emption capability determines whether a bearer with a lower ARP priority level should be dropped to free up the required resources.
  - **capable**: This keyword indicates that the service data flow is allowed to get resources that were already assigned to another service data flow with a lower priority level.
  - **non-capable**: This keyword indicates that the service data flow is not allowed to get resources that were already assigned to another service data flow with a lower priority level.

- **{not-vulnerable | vulnerable}**
  Sets the Pre-emption vulnerability related parameters with ARP priority in PCC-QoS-Profile name which is to use in Subscriber profile in PCC-Service instance on IPCF node.
  Pre-emption vulnerability determines whether a bearer is applicable for dropping by a pre-emption capable bearer with a higher ARP priority value.
  - **not-vulnerable**: This keyword indicates that the resources assigned to the service data flow shall not be pre-empted and allocated to a service data flow with a higher priority level.
  - **vulnerable**: This keyword indicates that the resources assigned to the service data flow can be pre-empted and allocated to a service data flow with a higher priority level.
Usage
Use this command to define the ARP priority and pre-empt parameters in PCC-QoS-Profile which is to be used in Subscriber profile in PCC-Service instance on IPCF node. ARP controls how the IPCF reacts when there are insufficient resources to establish the new RAB. Typically it manages it by; 1) Deny the RAB request and 2) Preempt an existing RAB and accept the new RAB request.

Example
Following command sets the ARP Priority 2 with preemption capability and vulnerability in PCC-QoS-Profile instance on IPCF node.

```
arp-priority 2 pre-emption capable vulnerable
```
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Use this command to return to the parent configuration mode.
guaranteed-bitrate

This command defines the Guaranteed Bit Rate (GBR) value in bits per second for downlink and uplink traffic in PCC-QoS-Profile which is to use for Subscriber profile in PCC-Service instance on IPCF node.

**Product**

IPCF

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC QoS Profile Configuration

```
configure > context context_name > pcc-service service_name > qos-profile profile_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-qos-profile)#
```

**Syntax**

```
[no] guaranteed-bitrate downlink downlink_gbr uplink uplink_gbr
```

- **no**
  
  Removes the configured GBR value set for PCC-QoS-Profile for PCC-Service instance on IPCF node.

- **downlink**
  
  `downlink_gbr`
  
  Sets the Guaranteed Bit Rate allowed in downlink direction (from PCEF to UE) in bits per second for a PCC-QoS-Profile which is to use for Subscriber profile in PCC-Service instance on IPCF node. `downlink_gbr` must be an integer from 0 through 104857600. A ‘zero’ value disables the downlink in specified PCC-QoS-Profile.

- **uplink**
  
  `uplink_gbr`
  
  Sets the Guaranteed Bit Rate allowed in uplink direction (from PCEF to PDN) in bits per second for a PCC-QoS-Profile which is to use for Subscriber profile in PCC-Service instance on IPCF node. `uplink_gbr` must be an integer from 0 through 104857600. A ‘zero’ value disables the uplink in specified PCC-QoS-Profile.

**Usage**

Use this command to define the Guaranteed Bit Rate value in bits per second for downlink and uplink traffic in PCC-QoS-Profile which is to use for Subscriber profile in PCC-Service instance on IPCF node.

**Example**

Following command sets the 1024 bits per seconds as uplink GBR and 2048 bits per second as downlink GBR in PCC-QoS-Profile instance on IPCF node.

```
guaranteed-bitrate downlink 2048 uplink 1024
```
max-bitrate

This command defines the Maximum Bit Rate (MBR) value in bits per second for downlink and uplink traffic in PCC-QoS-Profile which is to use for Subscriber profile in PCC-Service instance on IPCF node.

Product
IPCF

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC QoS Profile Configuration

configure > context context_name > pcc-service service_name > qos-profile profile_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pcc-qos-profile)#

Syntax

[no] max-bitrate downlink downlink_mbr uplink uplink_mbr

[no]

Removes the configured Maximum Bit Rate value set for PCC-QoS-Profile for PCC-Service instance on IPCF node.

downlink downlink_mbr

Sets the Maximum Bit Rate allowed in downlink direction (from PCEF to UE) in bits per second for a PCC-QoS-Profile which is to use for Subscriber profile in PCC-Service instance on IPCF node.

downlink_mbr must be an integer from 0 through 104857600. A ‘zero’ value disables the downlink in specified PCC-QoS-Profile.

uplink uplink_mbr

Sets the Maximum Bit Rate allowed in uplink direction (from PCEF to PDN) in bits per second for a PCC-QoS-Profile which is to use for Subscriber profile in PCC-Service instance on IPCF node.

uplink_mbr must be an integer from 0 through 104857600. A ‘zero’ value disables the uplink in specified PCC-QoS-Profile.

Usage

Use this command to define the Maximum Bit Rate value in bits per second for downlink and uplink traffic in PCC-QoS-Profile which is to use for Subscriber profile in PCC-Service instance on IPCF node.

Example

Following command sets the 1024 bits per seconds as uplink MBR and 2048 bits per second as downlink MBR in PCC-QoS-Profile instance on IPCF node.

max-bitrate downlink 2048 uplink 1024
qci

This command sets the QoS Class Identifier (QCI) for PCC-QoS-Profile which is to use for Subscriber profile in PCC-Service instance on IPCF node.

**Product**
IPCF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC QoS Profile Configuration

```
configure > context context_name > pcc-service service_name > qos-profile profile_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-qos-profile)#
```

**Syntax**

```
[no] qci qci_id
```

- **no**
  Removes the configured QCI value set for PCC-QoS-Profile for PCC-Service instance on IPCF node.

- **qci qci_id**
  Sets the QoS Class Identifier for a PCC-QoS-Profile which is to use for Subscriber profile in PCC-Service instance on IPCF node.
  
  qci_id must be an integer from 1 through 255.

**Usage**

Use this command to set the QoS Class Identifier for PCC-QoS-Profile which is to use for Subscriber profile in PCC-Service instance on IPCF node.

**Example**

Following command sets the QCI 101 for PCC-QoS-Profile instance on IPCF node.

```
qci 101
```
Chapter 240
PCC-Service-Profile Configuration Mode Commands

The PCC-Service-Profile Configuration Mode is used to define the business logic used by the operator for managing the policy requirements and objectives for the network specific to a group of subscribers in the network. A PCC-Service-Profile manages multiple PCC-Conditions-Groups and associated PCC-Action-Sets pairs in an ordered manner. A maximum of 32 PCC-Service-Profile can be configured in a PCC-Service instance.

**Important:** This configuration mode is supported from StarOS Release 12.1 onward.

**Mode**

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Service Profile Configuration

```
configure > context context_name > pcc-service service_name > profile profile_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-profile)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
default-rulebase-name

This command is used to associate the default PCC-Rulebase with a PCC-Service-Profile which is to use in Subscriber profile in PCC-Service instance on IPCF node.

Product
IPCF

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Service Profile Configuration

configure > context context_name > pcc-service service_name > profile profile_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pcc-profile)#

Syntax

[no] default-rulebase-name rulebase_name

---

no

Removes the configured default PCC-Rulebase from PCC-Service-Profile instance on IPCF node.

---

rulebase_name

This keyword specifies the default PCC-Rulebase name to be associated with PCC-Service-Profile instance. rulebase_name is the Rulebase name configured at PCEF and must be an alphanumeric string of 1 through 63 characters.

---

Usage

Use this command to associate the default PCC-Rulebase configured on PCEF with a PCC-Service-Profile which is to use in Subscriber profile in PCC-Service instance on IPCF node.

Example

Following command associates the PCC-Rulebase named pcc_rulebase1 for PCC-Profile instance on IPCF node.

    default-rulebase-name pcc_rulebase1
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
eval-priority

This command sets the priority for evaluation of PCC-Condition-Group with corresponding PCC-Action-Set in a PCC-Service-Profile which is to use in Subscriber profile in PCC-Service instance on IPCF node.

Product  
IPCF

Privilege  
Security Administrator, Administrator

Mode  
Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Service Profile Configuration

```bash
configure > context context_name > pcc-service service_name > profile profile_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-profile)#
```

Syntax

```
[no] eval-priority last action-set actionset_name
[no] eval-priority priority_value timedef timedef_name [condition-group cond.grp_name] action-set actionset_name
[no] eval-priority priority_value condition-group cond_grp_name action-set actionset_name
```

no

Removes the configured evaluation priority for PCC-Condition-Group with corresponding PCC-Action-Set from PCC-Service-Profile instance on IPCF node.

last

Sets last evaluation priority action-set configured for the PCC-Service-Profile instance. no removes the last evaluation priority action-set.

priority_value

Specifies the priority to be set for PCC-Condition-Group with corresponding PCC-Action-Set in a PCC-Service-Profile instance. priority_value must be an integer from 1 through 1023.

timedef timedef_name

Specifies a pre-configured time definition in PCC-Timedef Configuration mode and to be set for evaluation priority in a PCC-Service-Profile instance. timedef_name is a pre-configured PCC-Timedef and must be an alphanumerical string of 1 through 63 characters.
condition-group  cond_grp_name
Specifies a pre-configured PCC-Condition-Group to be set for evaluation priority in a PCC-Service-Profile instance.
cond_grp_name is a pre-configured PCC-Condition-Group and must be an alphanumerical string of 1 through 63 characters.

Important: An special PCC-Condition-Group “none” can be used to set the default PCC-Condition-Group for any-match typically used for a default condition for a session which does not match any of the conditions specified with higher evaluation priority.

action-set  actionset_name
Specifies a pre-configured PCC-Action-Set for PCC-Condition-Group to be set for evaluation priority in a PCC-Service-Profile instance.
actionset_name is a pre-configured PCC-Action-Set and must be an alphanumerical string of 1 through 63 characters.

Usage
Use this command to set the priority for evaluation of PCC-Condition-Group with corresponding PCC-Action-Set in a PCC-Service-Profile which is to use in Subscriber profile in PCC-Service instance on IPCF node.
Additionally timedef is used to accept the Timedefs to support the time-of-day-based procedures to trigger an evaluation priority. The action is triggered only when the time of session lies in the time span defined in specific PCC-Timedef timedef_name.
Default eval-priority has the lowest priority in the PCC-Service-Profile and as default eval-priority does not have any PCC-Condition-Group associated with it, all the actions in the action-set always be applied.
A maximum of 64 PCC-Evaluation-Priorities can be configured in a PCC-Service-Profile.

Example
Following command sets the evaluation priority value as 1 for PCC-Condition-Group cond_1 along with PCC-Action-Set act_cond1 for PCC-Service-Profile instance on IPCF node:

    eval-priority 1 condition-group cond_1 action-set act_cond1

Following command sets the evaluation priority value as 2 for PCC-Condition-Group none for any-match typically used for a default condition for a session which does not match any of the conditions specified with higher evaluation priority along with PCC-Action-Set act_cond1 for PCC-Service-Profile instance on IPCF node:

    eval-priority 1 condition-group none action-set act_cond1
**exit**

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Use this command to return to the parent configuration mode.
service-tag

This command configures the PCC-Service Tags to be used for PCC-Rulename or PCC-Rule-base in a PCC-Service-Profile which is to use in Subscriber profile in PCC-Service instance on IPCF node.

**Product**
IPCF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Service Profile Configuration

```
configure > context context_name > pcc-service service_name > profile profile_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-profile)#
```

**Syntax**

```
[no] service-tag svc_tag [rule-name rule_name | rulebase-name rulebase_name]
```

---

**no**

Removes the configured PCC-Service Tags for PCC-Rulename and PCC-Rulebase from PCC-Service-Profile instance on IPCF node.

---

**svc_tag**

Specifies the name of the PCC-Service Tag to be used for PCC-Rulename and PCC-Rulebase in a PCC-Service-Profile instance.

- **svc_tag** must be an alphanumerical string of 1 through 63 characters.

---

**rule-name rule_name**

Specifies a pre-defined PCC-Rulename on PCEF to be used with PCC-Service Tag svc_tag in a PCC-Service-Profile instance.

- **rule_name** is a pre-defined PCC-Rulename on PCEF and must be an alphanumerical string of 1 through 63 characters.

---

**rulebase-name rulebase_name**

Specifies a pre-defined PCC-Rulebase name pre-defined on PCEF to be used with PCC-Service Tag svc_tag in a PCC-Service-Profile instance.

- **rulebase_name** is a pre-defined PCC-Rulebase name on PCEF and must be an alphanumerical string of 1 through 63 characters.

**Usage**

Use this command to set the PCC-Service Tag for PCC-Rulename and PCC-Rulebase which are defined on PCEF with a PCC-Service-Profile which is to use in Subscriber profile in PCC-Service instance.

**Example**
Following command sets the PCC-Service Tag named *Rule1* for PCC-Rulebase named *pcc_rulebase1* for PCC-Service-Profile instance on IPCF node:

```
service-tag Rule1 rulebase-name pcc_rulebase1
```

Following command sets the PCC-Service Tag named *Rule11* for PCC-Rulename *pcc_rule1* for PCC-Service-Profile instance on IPCF node:

```
service-tag Rule11 rule-name pcc_rule1
```
timeout long-duration

Configures the long duration timeout and inactivity duration for subscriber session before system notifies or terminates session in PCC Profile instance.

**Product**
IPCF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Service Profile Configuration

```
configure > context context_name > pcc-service service_name > profile profile_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-profile)#
```

**Syntax**

```
timeout long-duration ldt_timeout [action {detection | disconnect}]
no timeout long-duration
default timeout long-duration
```

**no**
Removes the configured long duration timeout value and action in PCC Profile instance.

**default**
Sets the the long duration timeout value to the default value of ‘0’ which disables the long duration timeout configuration in PCC Profile instance.

**long-duration ldt_timeout**
Default: 0
Designates the maximum duration of the session, in seconds, before the system automatically reports/terminates the session.
Specifies the maximum amount of time, in seconds, before the specified timeout action is activated.
`ldt_timeout` must be a value in the range from 0 through 4294967295.
The special value 0 disables the timeout specified.

**action {detection | disconnect}**
Default: Detection
Specifies the action to be taken on expiry of long duration timeout duration `ldt_timeout` set with `timeout long-duration` command.

*`detection`: sets the system to detect the sessions for which long duration timeout timer is exceeded and sends the SNMP TRAP and CORBA notification. This is the default behavior.*
**Timeout long-duration**

- **disconnect**: sets the system to send SNMP TRAP and CORBA notification and disconnect the subscriber session once the long duration timeout timer is expired.

**Usage**

Use this command to set the long duration timeout period and actions to be taken on expiry of duration of timer for subscriber session.

**Important**: Reduce the timeout duration to free session resources faster for use by new requests.

**Important**: In case of long-duration timeout configured at PCC Service Configuration mode as well as at the PCC-Profile Configuration mode level, the long-duration timeout and action set in PCC-Profile Configuration mode will prevail. This enables defining session behavior as per profile provisioning.

**Example**

Following command sets the system to detect the subscriber sessions that exceeds the long duration timer of 6000 seconds and sends SNMP TRAP and CORBA notification:

```
timeout long-duration 6000 action detection
```

Following command sets the system to detect and disconnect the subscriber sessions that exceeds the long duration timer of 6000 seconds and disconnect the session after sending SNMP TRAP and CORBA notification:

```
timeout long-duration 6000 action disconnect
```
usage-monitor

This command creates/modifies/deletes the PCC-Usage-Monitor Configuration instance to track the usage volume across the PCC-services based on the usage monitor settings in a PCC-service instance for IPCF configuration.

**Product**

IPCF

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Service Profile Configuration

```plaintext
configure > context context_name > pcc-service service_name > profile profile_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-profile)#
```

**Syntax**

```plaintext
[no] usage-monitor usage_mon_name [-noconfirm]
```

- **no**
  
  Removes the configured PCC-Usage-Monitor from PCC-Service-Profile instance for IPCF configuration.

- **usage_mon_name**
  
  Identifies the name of the PCC-Usage-Monitor instance which is to be created or modified through this command. 
  The `usage_mon_name` must be an alphanumerical string from 1 through 63 characters.

- **-noconfirm**
  
  Indicates that the command is to execute without any additional prompt and confirmation from the user.

⚠️ **Caution:** If this keyword option is used with `no usage-monitor usage_mon_name` command, the PCC-Usage-Monitor instance named `usage_mon_name` is deleted with all configured parameters without prompting any warning or confirmation.

**Usage**

Use this command to create and configure a PCC-Usage-Monitor for PCC-Service-Profile in a PCC-service instance of IPCF configuration. 
A maximum number of 8 PCC-Usage-Monitors can be configured per PCC-Service-Profile. 
Entering this command results in the following prompt:

```
[context_name]host_name(config-pcc-profile-usage-mon)#
```

The commands configured in this mode are defined in the PCC-Usage-Monitor Configuration Mode Commands chapter of Command Line Interface Reference.
Caution: This is a critical configuration. The PCC-Usage-Monitor for volume usage cannot be configured without this configuration. Any change to this configuration would lead to removing or disabling configuration parameters defined here.

Example

Following command configures the PCC-Usage-Monitor named `pcc_usage1` to track the usage of service with in a PCC-Service-Profile instance.

```
usage-monitor pcc_usage1
```
unknown-services-treatment

This command configures the PCC-Service for handling of unknown services at IPCF which is to be used in Subscriber profile in PCC-Service instance on IPCF node.

Product
IPCF

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Service Profile Configuration
configure > context context_name > pcc-service service_name > profile profile_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pcc-profile)#

Syntax

[default] unknown-services-treatment |not-allowed | qos-profile qos_prof_name precedence from start_preced to end_preced order {ascending | descending}]

default
Sets the configured PCC-Service for handling of unknown services at IPCF to default value of “Not allowed” which is to be used in Subscriber profile in PCC-Service instance on IPCF node.

not-allowed
Sets the PCC-Service-Profile instance to reject the packet filters and does not installs any dynamic rule when IPCF receives any request to authorize Packet Filters from PCEF and no matching service flow is found in data service list.

qos-profile qos_prof_name
Specifies a pre-defined PCC-QoS profile name to be used to create dynamic rule when IPCF receives any request to authorize Packet Filters from PCEF and no matching service flow is found in data service list. qos_prof_name is a pre-defined PCC-QoS Profile and must be an alphanumerical string of 1 through 63 characters.

precedence from start_preced to end_preced
Specifies the precedence parameters to install dynamic rules for selection of QoS profile when QoS profile is configured to create dynamic rule when IPCF receives any request to authorize Packet Filters from PCEF and no matching service flow is found in data service list. start_preced is an integer between 1 through 65535 and must be less than end_preced value where end_preced is an integer between 1 through 65535 and must be more than start_preced value.

order {ascending | descending}
Specifies the order of precedence for QoS profile to be used to install dynamic rule when IPCF receives any request to authorize Packet Filters from PCEF and no matching service flow is found in data service list.
• **ascending** sets the precedence setting in ascending order.
• **descending** sets the precedence setting in descending order.

---

## Usage

Use this command to set the PCC-Service Tag for PCC-Rulename and PCC-Rulebase which are defined on PCEF with a PCC-Service-Profile which is to use in Subscriber profile in PCC-Service instance. Whenever IPCF receives any request to authorize Packet Filters from PCEF, it does a lookup in data service list to find a match. If No service flow is found matching then the requested filters are treated as **unknown service request** and handled as per the mentioned configuration.

When unknown-service-treatment is set to **not-allowed**, then Packet Filters are rejected and no dynamic rule is installed. Otherwise, dynamic rule is created using the requested packet filters, data rates mentioned in the QoS profile name `qos_prof_name` and precedence value derived from the configured values.

The precedence configuration works in following manner:

- If precedence limits are configured as 1000 to 2000 with order **ascending** then precedence of subsequent dynamic rules will go from 1000 to 2000.
- If precedence limits are configured as 1000 to 2000 with order **descending** then precedence of subsequent dynamic rules will go from 2000 to 1000.

---

## Example

Following command sets the PCC-Service for handling of unknown services for PCC-Service-Profile instance on IPCF node to default action of **not allowed**:

```
default unknown-services-treatment
```
Chapter 241
PCC-Service Configuration Mode Commands

The PCC-Service Configuration Mode is used to link, consolidate and manage the policy logic for the network. It defines the authorization of resources for a subscriber’s data usage under various conditions and policies in the PCC-service.

Important: This configuration mode is supported from StarOS Release 12.1 onward

Mode

Exec > Global Configuration > Context Configuration > PCC Service Configuration

configure > context context_name > pcc-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pcc-service)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
action-set

This command is used to create a new set of action, action-set, or modify a previously configured action set and enters the PCC-Action-Set Configuration Mode. This command can also be used to delete an existing PCC-Action-Set.

Product
- IPCF

Privilege
- Security Administrator, Administrator

Mode
- Exec > Global Configuration > Context Configuration > PCC Service Configuration
  
  configure > context context_name > pcc-service service_name

  Entering the above command sequence results in the following prompt:
  
  [context_name] host_name(config-pcc-service)#

Syntax

- action-set act_set_name [-noconfirm]

  no action-set act_set_name

  no
  
  Removes the configured PCC-Action-Set from this PCC-service instance for IPCF configuration.

  act_set_name
  
  Identifies the name of the PCC-Action-Set which is to be created or modified through this command. The act_set_name must be an alphanumerical string from 1 through 63 characters.

  -noconfirm
  
  Indicates that the command is to execute without any additional prompt and confirmation from the user.

Usage

Use this command to create/remove/configure an action-set in a PCC-service instance for IPCF Configuration.

An Action-set indicates the policy and charging as well as event generation related decisions that will get activated when the corresponding Condition-Group is evaluated to TRUE within a subscriber policy/profile. A maximum of 512 PCC-Action-Sets can be configured in 1 instance of PCC-Service.

Entering this command results in the following prompt:

  [context_name] host_name(config-pcc-action-set)

Important: For more information on PCC-Action-Set configuration, refer PCC-Action-Set Configuration Mode Commands.

Example

Cisco ASR 5x00 Command Line Interface Reference

7380
Following command creates a PCC-action-set named `pcc_act1` with in a PCC-service.

```
action-set pcc_act1
```

Following command removes a pre-configured PCC-action-set named `pcc_act1` from a PCC-service.

```
no action-set pcc_act1
```
charging method

This command defines the charging method selection parameters in a PCC-service instance for IPCF.

**Product**

IPCF

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > PCC Service Configuration

`configure > context context_name > pcc-service service_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-service)#
```

**Syntax**

```
charging method {both-offline-and-online | offline | online} 
[default | no] charging method
```

<table>
<thead>
<tr>
<th>Charging Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>default</strong></td>
<td>Sets the charging method to “no” in a PCC-service instance on IPCF node.</td>
</tr>
<tr>
<td><strong>no</strong></td>
<td>Removes the configured charging method from a PCC-service instance on IPCF node.</td>
</tr>
<tr>
<td><strong>both-offline-and-online</strong></td>
<td>Default: Disabled. Defines that this PCC-service instance is configured for both, online and offline, charging method for IPCF configuration.</td>
</tr>
<tr>
<td><strong>offline</strong></td>
<td>Default: Disabled. Defines that this PCC-service instance is configured only for offline charging method for IPCF configuration.</td>
</tr>
<tr>
<td><strong>online</strong></td>
<td>Default: Disabled. Defines that this PCC-service instance is configured only for online charging method for IPCF configuration.</td>
</tr>
</tbody>
</table>

**Usage**

Use this command to define the charging method selection parameters in a PCC-service instance for IPCF. Charging method used can be online, offline or both.

**Example**

Following command defines the charging method for a PCC-service instance as both, online and offline:
default charging method
charging server

This command defines the charging server parameters in a PCC-service instance for IPCF.

**Product**
IPCF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PCC Service Configuration

```
configure > context context_name > pcc-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-service)#
```

**Syntax**

```
charging server server_name function {offline | online} {primary | secondary}
no charging server {all | function {offline | online} {primary | secondary}

no
Removes/disables the charging server parameters in a PCC-service instance for IPCF configuration.

server_name
Identifies the name of the charging server which is to be configured with these parameters in a PCC-service instance for IPCF configuration. The server_name must be an alphanumerical string from 1 through 63 characters.

offline
Sets the specific charging server to be used as offline server in a PCC-service instance for IPCF configuration.

online
Sets the specific charging server to be used as online server in a PCC-service instance for IPCF configuration.

primary
Sets the specific charging server to be used as primary charging server for offline or online charging method in a PCC-service instance for IPCF configuration.

secondary
Sets the specific charging server to be used as secondary charging server for offline or online charging method in a PCC-service instance for IPCF configuration.
**Usage**

Use this command to configure the online or offline charging servers to be used as primary or secondary in a PCC-service instance for IPCF configuration.

**Example**

Following command configures the online charging server named Gx1 as primary for online charging method for a PCC-service instance:

```
charging server Gx1 function online primary
```

Following command removes the all, online/offline/primary/secondary, type of charging servers from a PCC-service instance:

```
no charging server function all
```
**condition-group**

This command creates a new group of conditions, condition-group, or modify a previously configured condition-group and enters the PCC-Condition-Group Configuration Mode. This command can also be used to delete an existing PCC-Condition-Group.

**Product**

IPCF

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > PCC Service Configuration

`configure > context context_name > pcc-service service_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-service)#
```

**Syntax**

```condition-group cond_grp_name [-noconfirm]
```

```no condition-group cond_grp_name
```

**no**

Removes the configured PCC-condition-group from a PCC-service instance for IPCF configuration.

```cond_grp_name```

Identifies the name of the PCC-condition-group which is to be created or modified through this command. The `cond_grp_name` must be an alphanumerical string from 1 through 63 characters.

```-noconfirm```

Indicates that the command is to execute without any additional prompt and confirmation from the user.

**Usage**

Use this command to create/remove/configure a group of condition, condition-group, in a PCC-service instance for IPCF configuration.

A Condition-group is a collection of conditions that identify a network or state constraint represented as an logical expression. A condition-group may use another `condition-group` within with the nesting level limited to 3.

Within a condition-group the conditions and condition-groups can either be linked with an **AND** or an **OR** relation. A Condition is built using predefined keywords representing unique service conditions such as `user-location`, `app-service` etc.

A maximum of 1024 PCC-Condition-Groups can be configured in 1 instance of PCC-Service.

Entering this command results in the following prompt:

```
[context_name]host_name(config-pcc-condition-group)#
```
The commands configured in this mode are defined in the *PCC-Condition-Group Configuration Mode Commands* chapter of *Command Line Interface Reference*.

⚠️ **Caution:** This is a critical configuration. The PCC-Condition Group can not be configured without this configuration. Any change to this configuration would lead to removing or disabling configuration parameters defined here.

**Example**

Following command creates a PCC-condition-group named `cond_grpl` with in a PCC-service instance.

```plaintext
condition-group cond_grpl
```

Following command removes a pre-configured PCC-condition-group named `cond_grpl` from a PCC-service instance.

```plaintext
no condition-group cond_grpl
```
**data-service**

This command creates a new service for data, data-service, or modify a pre-configured data-service and enters the PCC-Data-Service Configuration Mode. This command can also be used to delete an existing PCC-Data-Service.

**Product**
IPCF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PCC Service Configuration

`configure > context context_name > pcc-service service_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-service)##
```

**Syntax**

```
data-service data_svc_name [-noconfirm]

no data-service data_svc_name
```

- **no**
  Removes the configured PCC-Data-Service from a PCC-service instance for IPCF configuration.

- **data_svc_name**
  Identifies the name of the PCC-Data-Service which is to be created or modified through this command. The `data_svc_name` must be an alphanumerical string from 1 through 63 characters.

- **-noconfirm**
  Indicates that the command is to execute without any additional prompt and confirmation from the user.

**Usage**

Use this command to create and configure a PCC-data-service in a PCC-service instance for IPCF configuration.

A PCC-Data-Service defines the flows for the media data as well as corresponding attributes that are necessary for the charging as well as policy enforcement decisions for the kind of media represented by its Service-Flows.

A maximum of 256 PCC-Data-Services can be configured in 1 instance of PCC-Service.

Entering this command results in the following prompt:

```
[context_name]host_name(config-pcc-data-service)##
```

The commands configured in this mode are defined in the *PCC-Data Service Configuration Mode Commands* chapter of *Command Line Interface Reference*. 
Caution: This is a critical configuration. The PCC-Data-service can not be configured without this configuration. Any change to this configuration would lead to removing or disabling configuration parameters defined here.

Example

Following command defines a PCC-data-service named `pcc_data_svc1` in a PCC-service instance without any confirmation prompt.

```
data-service pcc_data_svc1 -noconfirm
```

Following command removes a pre-configured PCC-data-service named `pcc_data_svc1` from a PCC-service instance without any confirmation prompt.

```
no data-service pcc_data_svc1 -noconfirm
```
emergency-apn-map-profile

This command creates an emergency APN profile with a given condition group name. The condition group will define a group of APNs which correspond to the Operator's chosen emergency-APN, and a corresponding policy profile, which defines operator's QoS configuration for the emergency APN. This command can also be used to delete an existing emergency APN profile.

Product
IPCF

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PCC Service Configuration

configure > context context_name > pcc-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pcc-service)#

Syntax

[ no ] emergency-apn-map-profile condition-group cond_grp_name profile-policy name pcc_prof_name

no
Removes/disables the set emergency APN profile from this configuration mode.

condition-group cond_grp_name
This keyword associates a pre-configured/defined PCC-Condition-Group configured in PCC-Service Configuration mode to map with specific emergency APN profile. The cond_grp_name is pre-configured PCC-Condition-Group and must be an alphanumerical string from 1 through 63 characters.

Important: For more information on PCC-Condition-Group configuration, refer condition-group command in this chapter.

profile-policy pcc_prof_name
This keyword associates a pre-configured/defined PCC-Service-Profile configured in PCC-Service Configuration mode to map with specific emergency APN profile mapping configuration. The pcc_prof_name is pre-configured PCC-Service-Profile and must be an alphanumerical string from 1 through 63 characters.

Important: For more information on PCC-Service-Profile configuration, refer profile-policy command in this chapter.
Usage

Use this command to create an emergency APN profile with a given condition group name. The condition group defines a bunch of APNs for emergency services as created by the operator. A corresponding policy profile, which defines the operator's QoS configuration for the emergency APN, is also mapped with these APNs. Emergency services, e.g., 911 in the US, are those services that can be provided via an emergency APN and may or may not require subscription. Since subscription to such services is optional, the fetching of subscriber profile information is also not mandatory.

Example

Following command sets an emergency APN profile named sos_prof1 with condition group sos_cond1 in this PCC-service instance to support emergency services for a subscriber.

```
emergency-apn-map-profile condition-group sos_cond1 profile-policy name sos_prof1
```
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
end

**Usage**
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Use this command to return to the parent configuration mode.
map-profile priority

This command defines the parameter and key priorities to match the profile condition for a subscriber in a PCC-service instance for IPCF configuration.

Product
IPCF

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PCC Service Configuration
configure > context context_name > pcc-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pcc-service)#

Syntax

[no] map-profile priority map_prio_value apn [apn_name profile-policy name pcc_prof_name]

[ no ] map-profile priority map_prio_value profile-policy name pcc_prof_name]

[ no ] map-profile priority map_prio_value subscription-attribute name subs_attrib_name [value subs_attrib_value ] profile-policy name pcc_prof_name]

no

Removes/disables the set priority value of specific profile mapping parameters.

map_prio_value

Identifies the priority value of specific profile mapping parameters.
The map_prio_value must be an integer value from 1 through 1024.

apn  apn_name

This keywords associates a pre-configured/defined APN name to map with specific profile mapping priority. The apn_name specifies the name of the APN configured for subscriber session to which a priority value is set for profile mapping and must be an alphanumerical string from 1 through 63 characters.

condition-group  cond_grp_name

This keywords associates a pre-configured/defined PCC-Condition-Group configured in PCC-Service Configuration mode to map with specific profile making priority. The cond_grp_name is pre-configured PCC-Condition-Group and must be an alphanumerical string from 1 through 63 characters.

Important: For more information on PCC-Condition-Group configuration, refer condition-group command in this chapter.
**map-profile priority**

This command identifies the keys used to match the profile for a subscriber in a PCC-service instance for IPCF configuration. The profile map is used when the subscriber session established. It is based on the priority of map and condition matches the corresponding named profile is used for the subscriber session.

**Important:** For a subscriber session, only a single profile will match.

**Example**

Following command configures the profile mapping priority to 2 for an APN named **apn_ipcf1** with PCC-Service-Profile named **pcc_prof1** with in a PCC-service instance.

```
map-profile priority 2 apn apn_ipcf1 profile-policy name pcc_prof1
```

Following command configures the profile mapping priority to 0 for all sessions with PCC-Service-Profile named **pcc_prof2** with in a PCC-service instance.

```
map-profile priority 2 profile-policy name pcc_profile2
```
monitoring-key

This command creates a monitoring key and sets the threshold to provide the facility for tracking and dynamic Policy control based on subscriber usage in a PCC-service instance for IPCF configuration.

Product
IPCF

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PCC Service Configuration

configure > context context_name > pcc-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pcc-service)#

Syntax

monitoring-key { any | mon_key_value } grant-size { time dur_value | volume volume_value [ time dur_value] }

no monitoring-key mon_key_value

default monitoring-key any

no

Resets the grant size for specified Monitoring Key mon_key_value used in this PCC service instance to default threshold of 1024 KB for grant volume and 10 second for grant time.

default

Resets the grant size for any Monitoring Key used in this PCC service instance to default threshold of 1024 KB for grant volume and 10 second for grant time.

any

Default: Enabled
This keywords sets the threshold size for ANY monitoring key to configured grant volume or grant time duration. IPCF uses the configured grant size while installing a Monitoring Key in PCEF.

mon_key_value

This keywords configures the Monitoring Key with a configurable grant volume size. IPCF installs this Monitoring Key in PCEF for usage tracking.

mon_key_value must be an integer between 1 through 65535.

grant-size { time dur_value | volume volume_value [ time dur_value] }

Default: 1024 for volume and 10 second for time
This keywords associates a configurable grant size in seconds for time or in Kilo Bytes volume for specific usage Monitor Key on IPCF to install on PCEF.
**time** `dur_value` : This keyword sets the threshold time in seconds for usage monitoring key and `dur_value` be an integer between 1 through 4294967296.

**volume** `volume_value` : This keyword sets the threshold volume in Kilo Bytes for usage Monitoring Key and `volume_value` must be an integer between 1 through 4294967296.

**Usage**

Use this command to allow operator to configure the threshold size for a monitoring key in a PCC-service instance in IPCF considering grant volume size or grant time duration. IPCF uses the configured volume size or time duration in seconds while installing a Monitoring Key in PCEF. The configured threshold values are configurable to reduce the amount of usage for any of the usage conditions. PCEF when instructed by IPCF keeps track of usage per Monitoring Key and also reports the usage when either thresholds reached or requested by IPCF.

To allow operator to have dynamic Policy control, the IPCF uses objects called as Usage Monitor. Operator can “associate” different Monitoring Keys to these usage monitors. It can be a Many-To-Many relationship between Usage-Monitor and Monitoring-Key.

Operator has option to set usage conditions on Usage Monitors instead of Monitoring Keys directly.

**Example**

Following command configures the Monitoring Key 2 for a grant volume threshold size of 2048 Kilo Bytes with in a PCC-service instance.

```
monitoring-key 2 grant-size volume 2048
```
**multiple-pcef-per-subscriber**

This command enables the IPCF to support more than one Gx-session for single subscriber session coming from multiple PCEF in a PCC-service instance.

**Product**
IPCF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PCC Service Configuration

`configure > context context_name > pcc-service service_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-service)#
```

**Syntax**

```
[no | default] multiple-pcef-per-subscriber
```

- **no**
  
  Default: Disabled
  
  Removes the multiple Gx session for a single subscriber from a PCC-service instance for IPCF configuration.

- **default**
  
  Sets the PCC-service instance to default setting to accept the multiple Gx session for a single subscriber for IPCF configuration.

**Usage**

Use this command to enable multiple Gx session and multiple PCEF support for a single subscriber in a PCC-service instance for IPCF configuration.

By default this feature is enabled.

**Example**

Following command sets the IPCF to accept multiple Gx sessions from multiple PCEFs for a single subscriber with in a PCC-service instance.

```
multiple-pcef-per-subscriber
```
profile

This command creates a new PCC-Service-Profile or modifies a previously configured policy profile and enters the PCC-Service-Profile Configuration Mode. This command can also be used to delete an existing PCC-Service-Profile.

**Product**

IPCF

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > PCC Service Configuration

configure > context context_name > pcc-service service_name

Entering the above command sequence results in the following prompt:

[context_name]hostname(config-pcc-service)#

**Syntax**

profile pcc_prof_name [-noconfirm]

no profile pcc_prof_name

**no**

Removes the configured PCC-Service-Profile from a PCC-service instance for IPCF configuration.

**pcc_prof_name**

Identifies the name of the PCC-Service-Profile which is to be created or modified through this command. The pcc_prof_name must be an alphanumerical string from 1 through 63 characters. A maximum of 32 profiles can be configured in a PCC-service instance.

**-noconfirm**

Indicates that the command is to execute without any additional prompt and confirmation from the user.

**Usage**

Use this command to create/remove/configure a PCC-Service-Profile for managing the policy requirement and objectives for network specific to a group of subscribers in the network in a PCC-service instance for IPCF configuration.  
A profile manages multiple Condition-Groups and associated Action-Sets pairs in an ordered manner. On internal or external triggers that cause the profile evaluation, the PCC-rules-engine, evaluates the conditions within the Condition-Groups in the specified priority. Corresponding actions performed for Condition-Groups that evaluates to TRUE. Once a TRUE match found the evaluation of Condition-Groups does not continue further.  
A maximum of 32 PCC-Service-Profiles can be configured in 1 instance of PCC-Service.  
Entering this command results in the following prompt:

[context_name]hostname(config-pcc-profile)#
The commands configured in this mode are defined in the *PCC-Service-Profile Configuration Mode Commands* chapter of *Command Line Interface Reference*.

⚠️ **Caution:** This is a critical configuration. The PCC-Service-Profile can not be configured without this configuration. Any change to this configuration would lead to removing or disabling configuration parameters defined here.

**Example**

Following command creates a PCC-Service-Profile named `pcc_prof1` with in a PCC-service instance.

```
profile pcc_prof1
```

Following command removes a pre-configured PCC-Service-Profile named `pcc_prof1` from a PCC-service instance.

```
no profile pcc_prof1
```
qos-profile

This command creates a new PCC-QoS-Profile for QoS parameters or modify a pre-configured PCC-QoS-Profile and enters the PCC-QoS-Profile Configuration Mode. This command can also be used to delete an existing PCC-QoS-Profile.

Product
IPCF

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PCC Service Configuration
configure > context context_name > pcc-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pcc-service)#

Syntax

qos-profile qos_prof_name [-noconfirm]

no qos-profile qos_prof_name

- no
  Removes the configured PCC-QoS-Profile from a PCC-service instance for IPCF configuration.

  qos_prof_name
  Identifies the name of the PCC-QoS-Profile which is to be created or modified through this command. The qos_prof_name must be an alphanumerical string from 1 through 63 characters.

- noconfirm
  Indicates that the command is to execute without any additional prompt and confirmation from the user.

Usage

Use this command to create and configure a PCC-QoS profile in a PCC-service instance for IPCF configuration.

A PCC-QoS-Profile represents a resource requirement identified by means of the corresponding QoS attributes such as:

- QoS class identifier
- Maximum Requested bandwidth for uplink (UL)
- Maximum Requested bandwidth downlink (DL)
- Guaranteed bandwidth for uplink (UL)
- Guaranteed bandwidth downlink (DL)
- Allocation and Retention Priority (ARP)
A maximum of 256 PCC-QoS-Profiles can be configured in 1 instance of PCC-Service. Entering this command results in the following prompt:

```
[context_name]hostname(config-pcc-qos-profile))#
```

The commands configured in this mode are defined in the PCC-QoS-Profile Configuration Mode Commands chapter of Command Line Interface Reference.

⚠️ **Caution:** This is a critical configuration. The PCC-QoS-Profiles can not be configured without this configuration. Any change to this configuration would lead to removing or disabling configuration parameters defined here.

**Example**

Following command creates a PCC-QoS-Profile named `qos_profile1` with in a PCC-service instance.

```
qos-profile qos_profile1
```

Following command removes a pre-configured PCC-QoS-Profile named `qos_profile1` from a PCC-service instance.

```
no qos-profile qos_profile1
```
spr-failure

This command defines SSC session failure handling policies in a PCC-service instance on an IPCF node.

Product
IPCF

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PCC Service Configuration
configure > context context_name > pcc-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pcc-service)#

Syntax

spr-failure after-auth {continue | terminate}
[default] spr-failure after-auth

default
Sets the configured SSC session failure handling parameters and actions to default action of continue with a PCC-service instance for IPCF configuration.

after-auth {continue | terminate}
This keyword is used to set the PCC-service to take decision on SSC communication failure after authorization of session.
Following actions are initiated on SSC session failure after authorization:

• continue: IPCF allows session to continue.
• terminate: IPCF terminates the session for subscriber.

Usage
Use this command to set the PCC-service to take decision on SSC communication failure after authorization of session.

Example
Following command sets the session failure handling policy with SSC to terminate the session on failure of communication with SSC after authorization in a PCC-service instance.

spr-failure after-auth terminate
ssc-usage-update-policy

This command provides the configuration to manage the SSC update frequency over Sp interface for usage reports received from PCEF over Gx interface in a PCC-service instance for IPCF configuration.

**Product**
IPCF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PCC Service Configuration
```
configure > context context_name > pcc-service service_name
```

Entering the above command sequence results in the following prompt:
```
[context_name]host_name(config-pcc-service)#
```

**Syntax**
```
[default] ssc-usage-update-policy [always | average-tps tps | on-terminate]
```

**default**
Sets the PCC-service to configure the SSC update frequency to **always** over Sp interface for usage reports received from PCEF over Gx interface in a PCC-service instance for IPCF configuration.

**always**
Default: Enabled
This keyword sets the PCC-service instance to generate SSC usage update every time PCC-service instance received Usage Report from PCEF over Gx interface for IPCF configuration.

**average-tps tps**
Default: Disabled
This keyword generates the SSC usage update towards the SSC over Sp interface for Usage Reports received by IPCF from PCEF over Gx interface only when average transaction-per-second exceeds the configured threshold tps. The tps specifies the average transactions-per-second on IPCF and must be an integer from 1 through 5000.

**on-terminate**
Default: Disabled
This keyword generates the SSC usage update towards the SSC over Sp interface for Usage Reports received by IPCF from PCEF over Gx interface only when IP-CAN session terminates.

**Usage**
Use this command to configure the PCC-service to manage the SSC update frequency over Sp interface for Usage Reports received from PCEF over Gx interface in a PCC-service instance for IPCF configuration.
Following command configures the SSC usage update over Sp interface every time when a usage report is received over Gx interface in a PCC-service instance.

```bash
default ssc-usage-update-policy
```
timedef

This command creates a new Time Definition (TimeDef), or modify a pre-configured Timedef and enters the PCC-TimeDef Configuration Mode. This command can also be used to delete an existing PCC-TimeDef.

Product
IPCF

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PCC Service Configuration

configure > context context_name > pcc-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pcc-service)#

Syntax

[no] timedef timedef_name [-noconfirm]

no
Removes the configured PCC-TimeDef from a PCC-service instance for IPCF configuration.

timedef_name
Identifies the name of the PCC-TimeDef which is to be created or modified through this command. The timedef_name must be an alphanumerical string from 1 through 127 characters.

-noconfirm
Indicates that the command is to execute without any additional prompt and confirmation from the user.

Usage

Use this command to create and configure a PCC-Time Definition (TimeDef) in a PCC-service instance for IPCF configuration.
The PCC-TimeDefs can be used to configured date and time for triggering the event for policy related procedures as well.
Entering this command results in the following prompt:

[context_name]host_name(config-pcc-service)#

A maximum of 512 PCC-TimeDefs can be configured in 1 instance of PCC-Service.
The commands configured in this mode are defined in the PCC-TimeDef Configuration Mode Commands chapter of Command Line Interface Reference.

⚠️ Caution: This is a critical configuration. The PCC-TimeDefs can not be configured without this configuration. Any change to this configuration would lead to removing or disabling configuration parameters defined here.
Example

Following command creates a PCC-TimeDef named `time_day1` with in a PCC-service instance.

```
timedef time_day1
```

Following command removes a pre-configured PCC-TimeDef named `time_day1` from a PCC-service instance.

```
no timedef time_day1
```
**timeout idle**

Configures the idle timeout duration for subscriber session and also sets the action to be taken by system on expiry of timeout duration.

**Product**
IPCF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PCC Service Configuration

```bash
configure > context context_name > pcc-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-service)#
```

**Syntax**

```
timeout idle idle_dur [ action reauthorize ]

[ no | default ] timeout idle
```

- **no**
  Removes the configured idle timeout value and action set in in PCC Service instance.

- **default**
  Sets the the idle timeout duration to the default value of ‘0’ which disables the idle timeout configuration in PCC Service instance.

- **idle_dur**
  Default: 0
  Designates the maximum duration of the session, in seconds, after the expiry of which the system considers the session as dormant or idle and invokes the reauthorization of session action, if configured.
  **idle_dur** must be a value in the range from 0 through 4294967295. The special value 0 disables the timeout specified.

- **action reauthorize**
  This optional keyword sets the system to trigger the reauthorization of session after expiry of the timeout duration configured through idle_dur value.

**Usage**

Use this command to set the idle time duration for subscriber session to determine the dormant session. This configuration sets the time in seconds for idle session (sessions with no activity/signaling). On expiry of this timeout duration action of reauthorization of session shall be triggered. In case of reauthorization request failure, session termination shall be triggered. Refer to the **timeout long-duration** command in this chapter for additional information.
Important: Reduce the timeout duration to free session resources faster for use by new requests.

Example

Following command sets the idle timeout duration to 450 seconds.

```
timeout idle 450
```
timeout setup

Configures the timeout duration for IPCF setup session.

Product
IPCF

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PCC Service Configuration

configure > context context_name > pcc-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pcc-service)#

Syntax

timeout setup setup_dur

[ no | default ] timeout setup

---

no

Removes the configured setup timeout value and action set in PCC Service instance.

---

default

Sets the setup timeout duration to the default value of 60. The special value of ‘0’ disables the setup timeout configuration in PCC Service instance.

---

setup_dur

Default: 60

Designates the maximum duration for the IPCF session setup, in seconds, after the expiry of which the system considers the IPCF session setup as failure and terminates the setup process.

setup_dur must be a value in the range from 0 through 120.

The special value 0 disables the setup timeout specified.

---

Usage

Use this command to set the time duration for IPCF session setup to determine the failure of IPCF setup process.

---

Example

Following command sets the IPCF session timeout duration to 30 seconds.

    timeout setup 30
timeout long-duration

Configures the long duration timeout and inactivity duration for subscriber session before system notifies or terminates session in PCC Service instance.

**Product**
- IPCF

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration > Context Configuration > PCC Service Configuration
  ```
  configure > context context_name > pcc-service service_name
  ```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-service)#
```

**Syntax**

```
timeout long-duration ldt_timeout [ action {detection | disconnect } ]

[ no | default] timeout long-duration
```

- no
  - Removes the configured long duration timeout value and action in PCC Service instance.

- default
  - Sets the the long duration timeout value to the default value of ‘0’ which disables the long duration timeout configuration in PCC Service instance.

- long-duration ldt_timeout
  - Default: 0
  - Designates the maximum duration of the session, in seconds, before the system automatically reports/terminates the session.
  - Specifies the maximum amount of time, in seconds, before the specified timeout action is activated.
  - ldt_timeout must be a value in the range from 0 through 4294967295.
  - The special value 0 disables the timeout specified.

- action {detection | disconnect}
  - Default: Detection
  - Specifies the action to be taken on expiry of long duration timeout duration ldt_timeout set with timeout long-duration command.
    - **detection**: sets the system to detect the sessions for which long duration timeout timer is exceeded and sends the SNMP TRAP and CORBA notification. This is the default behavior.
    - **disconnect**: sets the system to send SNMP TRAP and CORBA notification and disconnect the subscriber session once the long duration timeout timer is expired.
timeout long-duration

Usage
Use this command to set the long duration timeout period and actions to be taken on expiry of duration of timer for subscriber session.

Important: Reduce the timeout duration to free session resources faster for use by new requests.

Important: In case of long-duration timeout configured at PCC Service Configuration mode as well as at the PCC-Profile Configuration mode level, the long-duration timeout and action set in PCC-Profile Configuration mode will prevail. This enables defining session behavior as per profile provisioning.

Example
Following command sets the system to detect the subscriber sessions that exceeds the long duration timer of 6000 seconds and sends SNMP TRAP and CORBA notification:

    timeout long-duration 6000 action detection

Following command sets the system to detect and disconnect the subscriber sessions that exceeds the long duration timer of 6000 seconds and disconnect the session after sending SNMP TRAP and CORBA notification:

    timeout long-duration 6000 action disconnect
Chapter 242
PCC-Sp-Endpoint Configuration Mode Commands

The PCC-Sp-Endpoint Configuration mode provides a mechanism for Intelligent Policy Control Function (IPCF) to support the Sp interface endpoint. It represents a client end for SSC interactions. The PCC-Sp-Endpoint configuration mode facilitates the configuration of Sp interface, and manages the connection and operational parameters related to its peer.

Important: This configuration mode is supported from StarOS Release 12.1 onward.

Mode

Exec > Global Configuration > Context Configuration > PCC Sp Endpoint Configuration

configure > context context_name > pcc-sp-endpoint endpoint_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-spendpoint)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
access-type

This command is used to define the type of access protocol to be used with a PCC-Sp-Endpoint instance for IPCF configuration.

Product
IPCF

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PCC Sp Endpoint Configuration

configure > context context_name > pcc-sp-endpoint endpoint_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-spendpoint)#

Syntax

access-type {diameter | ldap}

default access-type

default

Sets access type protocol to be used by endpoints to default protocol of Diameter protocol in a PCC-Sp-Endpoint instance for IPCF configuration.

diameter

Default: Enabled
Sets access type protocol to be used by endpoints to Diameter protocol in a PCC-Sp-Endpoint instance for IPCF configuration.

ldap

Default: Disabled
Sets access type protocol to be used by endpoints to Lightweight Directory Access Protocol (LDAP) in a PCC-Sp-Endpoint instance for IPCF configuration.

Usage

Use this command to define the type of access protocol to be used with a PCC-Sp-Endpoint instance for IPCF configuration.

Example

Following command sets the access type of protocol to Diameter for a PCC-Sp-Endpoint instance.

default access-type
**diameter dictionary**

This command is used to assign a Diameter dictionary for interaction with SSC and messaging over Sp interface in a PCC-Sp-Endpoint instance of IPCF configuration.

**Product**

IPCF

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > PCC Sp Endpoint Configuration

```bash
configure > context context_name > pcc-sp-endpoint endpoint_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config- spendpoint)#
```

**Syntax**

```
diameter dictionary { sh-custon-starent | sh-custom2 | sh-standard }
```

**default diameter dictionary**

```
default
  Sets the Diameter Sh dictionary to default dictionary sh-custon-starent (3GPP Rel. 8 Sh standard) for Sh interaction and messaging over Sp interface in a PCC-Sp-Endpoint instance of IPCF configuration.
```

```
sh-custom-starent
  Default: Enabled
  Sets the Diameter Sh dictionary to default dictionary sh-custon-starent for Sh interaction and messaging over Sp interface in a PCC-Sp-Endpoint instance of IPCF configuration.
```

```
sh-custom2
  Default: Disabled
  Sets the Diameter Sh dictionary to sh-custom2 with Cisco ULI AVP support for Sh interaction and messaging over Sp interface in a PCC-Sp-Endpoint instance of IPCF configuration.
```

```
sh-standard
  Default: Disabled
  Sets the Diameter Sh dictionary to default dictionary sh-standard (3GPP Rel. 8 standard) for Sh interaction and messaging over Sp interface in a PCC-Sp-Endpoint instance of IPCF configuration.
```

**Usage**

Use this command to assign a Diameter dictionary for Sh interaction and messaging over Sp interface in a PCC-Sp-Endpoint instance of IPCF configuration.

**Example**

Following command sets the Diameter dictionary for Sh interaction and messaging over Sp interface in a PCC-Sp-Endpoint instance of IPCF configuration to 3GPP Rel. 8 standard.
diameter dictionary sh-standard
diameter origin end-point

This command is used to bind/associate a pre-configured Diameter host/realm (SSC) over Sp interface for SPR interactions with a PCC-Sp-Endpoint instance to be used for subscriber profile and policy management.

**Product**
IPCF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PCC Sp Endpoint Configuration

```
configure > context context_name > pcc-sp-endpoint endpoint_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sp-endpoint)#
```

**Syntax**

```
diameter origin endpoint ssc_node_name
```

```
no diameter origin endpoint
```

- **no**
  Removes the associated Diameter Origin Endpoint configuration from PCC-Sp-Endpoint instance configured for IPCF configuration.

- **ssc_node_name**
  The `ssc_node_name` is a predefined Diameter origin endpoint node (SSC) and must be an alphanumerical string from 1 through 63 characters.

**Usage**

Use this command to bind the SSC node over Sp interface by associating a pre-configured Diameter Origin Endpoint configuration with a PCC-Sp-Endpoint instance. The Diameter origin endpoint must be a pre-configured instance in the Context Configuration Mode. For more information on Diameter origin endpoint configuration, refer Diameter Endpoint Configuration Mode Commands chapter.

**Example**

Following command associates a pre-configured Diameter endpoint node configuration named `ssc_1` with a PCC-Sp-Endpoint instance for subscriber policy profile management.

```
diameter origin endpoint ssc_1
```

Following command removes the pre-associated Diameter endpoint node configuration named `ssc_1` from a PCC-Sp-Endpoint instance.

```
no diameter origin endpoint
```
diameter peer-select

This command nominates primary and secondary Diameter peers amongst the peers configured under Diameter Endpoint Configuration instance which is associated with a PCC Sp-Endpoint configuration.

Product
IPCF

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PCC Sp Endpoint Configuration

configure > context context_name > pcc-sp-endpoint endpoint_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-spendpoint)#

Syntax

diameter peer-select peer pri_peer_name [row-precedence row_prec_name selection-condition imsi {mcc mcc-string [mnc mnc-string] [msin msin-string] | mnc mnc-string [msin msin-string] | msin msin-string}] [realm realm_name] [secondary-peer sec_peer_name [realm sec_realm_name]]

no diameter peer-select

no diameter peer-select row-precedence

---

no

To remove all the configuration parameters.
To remove a particular selection-condition, a row-precedence value is specified.

peer pri_peer_name

Sets a configured Diameter peer, which is configured in Diameter Endpoint configuration associated with PCC-Sp-Endpoint instance configuration, as primary in Diameter peer selection process for IPCF configuration.

The pri_peer_name is a pre-configured Diameter peer in Diameter Endpoint configuration which is associated with a PCC-Sp-Endpoint configuration and must be an alphanumerical string from 1 through 63 characters. pri_peer_name allows punctuation marks.

row-precedence row_prec_name

The row-precedence decides order of evaluation of the selection conditions.
The row_prec_name is an integer between 1 and 63. Lower the value, higher is the priority of evaluation.

selection-condition

The selection-condition parameter is used to define Diameter SPR peer selection condition.
**imsi**

It indicates that the selection condition is based on subscriber IMSI.

---

**mcc mcc-string**

It indicates that the selection condition is based on MCC component of subscriber IMSI. The `mcc-string` can have one of the following formats: `mccval1` or `mccval1-mccval2`. The first format compares single MCC value and second one incorporates the range with `mccval1 <= mccval2`. The values for both `mccval1` and `mccval2` must be between 100 to 999.

---

**mnc mnc-string**

It indicates that the selection condition is based on MNC component of subscriber IMSI. The `mnc-string` can have one of the following formats: `mncval1` or `mncval1-mncval2`. The first format compares single MNC value and second one incorporates the range with `mncval1 <= mncval2`. The values for both `mncval1` and `mncval2` must be between 1 to 999.

---

**msin msin-string**

It indicates that the condition is based on MSIN component of subscriber IMSI. The `msin-string` can have following format: `msinval1-msinval2`. The format incorporates the range with `mccval1 <= mccval2`. The values for both `mccval1` and `mccval2` must be of maximum of 10 digits.

---

**realm realm-name**

This keyword optionally defines the realm (domain) of a configured **primary** Diameter peer, which is configured in Diameter Endpoint configuration associated with PCC-Sp-Endpoint instance configuration, in Diameter peer selection process for IPCF configuration. The `realm_name` is the realm (domain) of the associated primary Diameter peer in Diameter Endpoint configuration which associated with a PCC-Sp-Endpoint configuration. The `realm_name` must be an alpha and/or numeric string of 1 to 127 characters. The realm may typically be a company or service name and it allows punctuation marks.

---

**secondary-peer sec_peer_name**

Sets a configured Diameter peer, which is configured in Diameter Endpoint configuration associated with PCC-Sp-Endpoint instance configuration, as **secondary** in Diameter peer selection process for IPCF configuration. The `sec_peer_name` is a pre-configured Diameter peer in Diameter Endpoint configuration which is associated with a PCC-Sp-Endpoint configuration and must be an alphanumerical string from 1 through 63 characters. `sec_peer_name` allows punctuation marks.

---

**realm sec_realm-name**

This keyword optionally defines the realm (domain) of a configured **secondary** Diameter peer, which is configured in Diameter Endpoint configuration associated with PCC-Sp-Endpoint instance configuration, in Diameter peer selection process for IPCF configuration. The `sec_realm_name` is the realm (domain) of the associated primary Diameter peer in Diameter Endpoint configuration which associated with a PCC-Sp-Endpoint configuration. The `sec_realm_name` must be an alpha and/or numeric string of from 1 to 127 characters. The realm may typically be a company or service name and it allows punctuation marks.
Usage
Use this command to nominate primary and secondary Diameter peers amongst the peers configured under Diameter Endpoint Configuration instance which is associated with a PCC-Sp-Endpoint configuration. When both primary and secondary are down, the remaining Diameter peers are chosen based on their configured weight in round robin manner.
When row-precedence and selection-conditions are not defined for peer selection configuration, the row precedence value is assumed to be 64 (which is the lowest). This is a default peer selection when all the other configured selection conditions fail.
Multiple Diameter peers can be configured in a PCC-Sp-Endpoint instance by entering this command multiple times.

Example
Assume the operator has two MCC-MNC combinations: 123-456 and 123-457 respectively for subscriber IMSI values. If operator wishes to divert subscribers with these two different combinations to different SSC peers (say ssc123456 and ssc123457) then the operator needs to use following commands under PCC-Sp-Endpoint:

diameter peer-select row-precedence 4 selection-condition imsi mcc 123 mnc 456 peer ssc123456

diameter peer-select row-precedence 6 selection-condition imsi mnc 123 mnc 456 peer ssc223457

Following command nominates a pre-configured Diameter peer dia1 as primary and dia2 as secondary for Diameter peer selection process in a PCC-Sp-Endpoint configuration instance.

diameter peer-select peer dia1 secondary peer dia2
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Use this command to return to the parent configuration mode.
profile-data

This command allows the operator to specify data-reference and service indication AVP values used in UDR/SNR message for profile data sent over Sp endpoint when access type is set to Diameter.

Product
IPCF

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PCC Sp Endpoint Configuration
configure > context context_name > pcc-sp-endpoint endpoint_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-spendpoint)#

Syntax

profile-data key data-reference data_ref_value [service-indication svc_ind_value]
default profile-data key

default

Specifies the data-reference value used in UDR/SNR message for profile data sent over Sp endpoint to default value of ‘0’ (zero) and service indication AVP value to profile data when access type is set to Diameter in PCC-Sp-Endpoint instance.

data-reference data_ref_value

Default: 0
Specifies the data-reference values used in UDR/SNR message for profile data sent over Sp endpoint when access type is set to Diameter in PCC-Sp-Endpoint instance.
The data reference value data_ref_value must be an integer from 1 through 65535.

service-indication svc_ind_value

Specifies the service indication AVP value used in UDR/SNR message for profile data sent over Sp endpoint when access type is set to Diameter in PCC-Sp-Endpoint instance.

Important: The Service-Indication values are set as per application logic and are supposed to be used only with SSC.

The service indication value svc_ind_value must be a string of alpha and/or numeric characters from 1 to 32 characters.
Usage

Use this command to allow the operator to specify data-reference and service indication AVP values used in UDR/SNR message for profile data sent over Sp endpoint when access type is set to Diameter in PCC-Sp-Endpoint configuration instance. Default service-indication value varies as per other interface configuration default profile-data key is used to set the service indication value.

Example

Following command set the data-reference value used in UDR/SNR message for profile data sent over Sp endpoint to default value of '0' (zero) and service-indication value as per application logic when access type is set to Diameter in PCC-Sp-Endpoint instance.

```text
default profile-data key
```
**profile-update-notification**

This command sets the system to indicate whether SSC and IPCF are capable of supporting profile update notifications in a PCC-Sp-Endpoint instance.

**Product**
IPCF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PCC Sp Endpoint Configuration

```plaintext
configure > context context_name > pcc-sp-endpoint endpoint_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-spendpoint)#
```

**Syntax**

```
profile-update-notification {allow | disallow}
```

**default profile-update-notification**

- **default**
  
  Set the PCC-Sp-Endpoint instance default mode for supporting profile update notifications in a PCC-Sp-Endpoint instance and also to use the same in a PCC-Sp-Endpoint configuration instance.

- **allow**
  
  Default: Enabled
  
  Set the PCC-Sp-Endpoint instance to support the profile update notifications and also allow to use the same in Sp interaction.

- **disallow**
  
  Default: Disabled
  
  Set the PCC-Sp-Endpoint instance to not to support the profile update notifications and also does not allow to use the same in Sp interaction.

**Usage**

Use command to set to indicate whether SSC and IPCF are capable of supporting profile update notifications in a PCC-Sp-Endpoint instance. It also sets that whether profile update notification should be used or not for a PCC-Sp-Endpoint configuration instance.

**Example**

Following command indicates that SSC and IPCF are capable of supporting profile update notifications in a PCC-Sp-Endpoint instance and also allow to use it for a PCC-Sp-Endpoint configuration instance.

```
default profile-update-notification
```
spr subscriber identifier

This command sets the PCC-Sp-Endpoint instance to indicate how a subscriber is uniquely identified in SPR database while requesting subscriber data from SSC.

**Product**
IPCF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PCC Sp Endpoint Configuration
`configure > context context_name > pcc-sp-endpoint endpoint_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-spendpoint)#
```

**Syntax**

```
spr subscriber identifier {imsi | msisdn | nai}
```

**default spr subscriber identifier**

```
default
```
Sets the PCC-Sp-Endpoint instance to use subscriber IMSI to identify subscriber uniquely in SPR database while requesting subscriber data from SSC.

```
imsi
```
Default: Enabled
Sets the PCC-Sp-Endpoint instance to use subscriber IMSI to identify subscriber uniquely in SPR database while requesting subscriber data from SSC.

```
msisdn
```
Default: Disabled
Sets the PCC-Sp-Endpoint instance to use subscriber MSISDN to identify subscriber uniquely in SPR database while requesting subscriber data from SSC.

```
nai
```
Default: Disabled
Sets the PCC-Sp-Endpoint instance to use Network Address Identifier as token to identify subscriber uniquely in SPR database while requesting subscriber data from SSC.
This token facilitates CDMA users for Policy Control and Charging functions.

**Usage**

Use command to set the PCC-Sp-Endpoint instance to indicate how a subscriber is uniquely identified in SPR database on SSC while requesting subscriber data. By default it uses Subscriber IMSI for identification in SPR database.
For IP-CAN session between PDSN and IPCF the subscriber token NAI facilitates the Policy Control and Charging functions to subscribers.

Example

Following command sets the PCC-Sp-Endpoint instance to use a subscriber IMSI to uniquely identified in SPR database at SSC.

```
default spr subscriber identifier
```
Chapter 243

PCC-TimeDef Configuration Mode Commands

The PCC-TimeDef Configuration Mode is used to configure various time definitions (TimeDefs) in the PCC-service instance. A PCC-TimeDef specifies the start and end time for triggering policy-related procedures or conditions.

**Important:** This configuration mode is supported from StarOS Release 12.1 onward.

**Mode**

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC TimeDef Configuration

`configure > context context_name > pcc-service service_name > timedef timedef_name`

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-pcc-timedef)#`

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Use this command to return to the parent configuration mode.
start date

This command defines PCC-TimeDefs with a start and end dates with time for an event to trigger a procedure or condition in an IP-CAN session.

Product
IPCF

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC TimeDef Configuration

configure > context context_name > pcc-service service_name > timedef timedef_name

Entering the above command sequence results in the following prompt:

[context_name] host_name(config-pcc-timedef)#

Syntax

(no) start date start_date time start_time end date end_date time end_time

no

Removes the specified time definition.

date start_date

Specifies the start date start_date in MM/DD/YY format.
Following format is used for MM/DD/YY in start_date:

- MM specifies the month of the start date from January through December and must be an integer between 1 through 12.
- DD specifies the date of month of the start date 1 through 31 and must be an integer between 1 through 31.
- YY specifies the year of the start date from 2010 through 2037 and must be an integer between 10 through 37.

time start_time

Specifies the start time start_time in HH MIN SS format.
Following format is used for HH MIN SS in start_time:

- HH specifies the hour of the start date in 24 hour format and must be an integer between 00 through 23.
- MIN specifies the minutes of the hour of the start date must be an integer between 00 through 59.
- SS specifies the seconds of the minute of the start date must be an integer between 00 through 59.

date end_date

Specifies the end date end_date in MM/DD/YY format.
Following format is used for MM/DD/YY in end_date:
- **MM** specifies the month of the end date from January through December and must be an integer between 1 through 12.
- **DD** specifies the date of month of the end date 1 through 31 and must be an integer between 1 through 31.
- **YY** specifies the year of the end date from 2010 through 2037 and must be an integer between 10 through 37.

```
time end_time
```

Specifies the end time `end_time` in **HH MIN SS** format.
Following format is used for `HH MIN SS` in `end_time`:
- **HH** specifies the hour of the end date in 24 hour format and must be an integer between 00 through 23.
- **MIN** specifies the minutes of the hour of the end date must be an integer between 00 through 59.
- **SS** specifies the seconds of the minute of the end date must be an integer between 00 through 59.

**Usage**

Use this command to define a PCC-TimeDef with a start and end dates with time for an event to trigger a procedure or condition in an IP-CAN session.

**Example**

The following command defines a PCC-TimeDef with start date as December 31st 2010 at 00 Hrs. 30 mins. and 00 seconds and end date as January 31st 2011 at 23 Hrs. 59 mins. and 59 seconds:

```
start date 12/31/10 time 00 30 00 end date 01/31/11 time 23 59 59
```
start day

This command defines PCC-TimeDefs with a start and end week days with time for an event to trigger a procedure or condition in an IP-CAN session.

Product
IPCF
Privilege
Security Administrator, Administrator
Mode
Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC TimeDef Configuration

```
configure > context context_name > pcc-service service_name > timedef timedef_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-timedef)#
```

Syntax

```
[start day start_weekdays time start_time end day end_weekdays time end_time]
```

**no**

Removes the specified time definition.

**day start_weekdays**

Specifies the start day as week days.
Following days are used as `start_weekdays`:

- **friday** specifies Friday of the week as start day.
- **monday** specifies Monday of the week as start day.
- **saturday** specifies Saturday of the week as start day.
- **sunday** specifies Sunday of the week as start day.
- **thursday** specifies Thursday of the week as start day.
- **tuesday** specifies Tuesday of the week as start day.
- **wednesday** specifies Wednesday of the week as start day.

**time start_time**

Specifies the start time `start_time` in **HH MIN SS** format.
Following format is used for **HH MIN SS** in `start_time`:

- **HH** specifies the hour of the start day in 24 hour format and must be an integer between 00 through 23.
- **MIN** specifies the minutes of the hour of the start day must be an integer between 00 through 59.
- **SS** specifies the seconds of the minute of the start day must be an integer between 00 through 59.
### PCC-TimeDef Configuration Mode Commands

**end day end_weekdays**

Specifies the end day as week days. Following days are used as `end_weekdays`:

- `friday` specifies Friday of the week as end day.
- `monday` specifies Monday of the week as end day.
- `saturday` specifies Saturday of the week as end day.
- `sunday` specifies Sunday of the week as end day.
- `thrusday` specifies Thursday of the week as end day.
- `tuesday` specifies Tuesday of the week as end day.
- `wednesday` specifies Wednesday of the week as end day.

**time end_time**

Specifies the end time `end_time` in `HH MIN SS` format. Following format is used for `HH MIN SS` in `end_time`:

- `HH` specifies the hour of the end day in 24 hour format and must be an integer between 00 through 23.
- `MIN` specifies the minutes of the hour of the end day must be an integer between 00 through 59.
- `SS` specifies the seconds of the minute of the end day must be an integer between 00 through 59.

### Usage

Use this command to define a PCC-TimeDef with a start and end weekdays with time for an event to trigger a procedure or condition in an IP-CAN session.

### Example

The following command defines a PCC-TimeDef with start day as Friday at 00 Hrs. 30 mins. and 00 seconds and end day as Sunday at 23 Hrs. 59 mins. and 59 seconds:

```
start day friday time 00 30 00 end day sunday time 23 59 59
```
start time

This command defines PCC-TimeDefs with a start and end time of a day for an event to trigger a procedure or condition in an IP-CAN session.

Product
IPCF

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC TimeDef Configuration

configure > context context_name > pcc-service service_name > timedef timedef_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pcc-timedef)#

Syntax

[no] start time start_time end time end_time

no
Removes the specified time definition.

time start_time
Specifies the start time start_time in HH MIN SS format.
Following format is used for HH MIN SS in start_time:

• HH specifies the hour of the day in 24 hour format and must be an integer between 00 through 23.
• MIN specifies the minutes of the hour of the day must be an integer between 00 through 59.
• SS specifies the seconds of the minute of the day must be an integer between 00 through 59.

d time end_time
Specifies the end time end_time in HH MIN SS format.
Following format is used for HH MIN SS in end_time:

• HH specifies the end hour of the day in 24 hour format and must be an integer between 00 through 23.
• MIN specifies the minutes of the end hour of the day must be an integer between 00 through 59.
• SS specifies the seconds of the minute of the end hour must be an integer between 00 through 59.

Usage
Use this command to define a PCC-TimeDef with a start and end time for an event to trigger a procedure or condition in an IP-CAN session.

Example

The following command defines a PCC-TimeDef with start at 00 Hrs. 30 mins. and 00 seconds and end at 23 Hrs. 59 mins. and 59 seconds:
start time 00 30 00 end time 23 59 59
**time-slot**

This command defines PCC-TimeDefs with a start and end week days with time for an event to trigger a procedure or condition in an IP-CAN session.

**Product**
IPCF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC TimeDef Configuration
configure > context context_name > pcc-service service_name > timedef timedef_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-timedef)#
```

**Syntax**

```
[ no ] time-slot slot_num{ [ no ] time-slot slot_num

[ no ] time-slot slot_num

no

Removes the specified time slot definition.

slot_num

Specifies the time slot number to be configured with this command and it must be an integer between 1 through 64.

date start_date

Specifies the start date start_date in MM/DD/YY format. Following format is used for MM/DD/YY in start_date:

- **MM** specifies the month of the start date from January through December and must be an integer between 1 through 12.
- **DD** specifies the date of month of the start date 1 through 31 and must be an integer between 1 through 31.
- **YY** specifies the year of the start date from 2010 through 2037 and must be an integer between 10 through 37.

time start_time

Specifies the start time start_time in HH:MIN:SS format. Following format is used for HH:MIN:SS in start_time:

- **HH** specifies the hour of the start date in 24 hour format and must be an integer between 00 through 23.
**MIN** specifies the minutes of the hour of the start date must be an integer between 00 through 59.

**SS** specifies the seconds of the minute of the start date must be an integer between 00 through 59.

**end date  end_date**

Specifies the end date **end_date** in **MM/DD/YY** format.
Following format is used for **MM/DD/YY** in **end_date**:

- **MM** specifies the month of the end date from January through December and must be an integer between 1 through 12.
- **DD** specifies the date of month of the end date 1 through 31 and must be an integer between 1 through 31.
- **YY** specifies the year of the end date from 2010 through 2037 and must be an integer between 10 through 37.

**time  end_time**

Specifies the end time **end_time** in **HH MIN SS** format.
Following format is used for **HH MIN SS** in **end_time**:

- **HH** specifies the hour of the end date in 24 hour format and must be an integer between 00 through 23.
- **MIN** specifies the minutes of the hour of the end date must be an integer between 00 through 59.
- **SS** specifies the seconds of the minute of the end date must be an integer between 00 through 59.

**day  start_weekdays**

Specifies the start day as week days.
Following days are used as **start_weekdays**:

- **friday** specifies Friday of the week as start day.
- **monday** specifies Monday of the week as start day.
- **saturday** specifies Saturday of the week as start day.
- **sunday** specifies Sunday of the week as start day.
- **thursday** specifies Thursday of the week as start day.
- **tuesday** specifies Tuesday of the week as start day.
- **wednesday** specifies Wednesday of the week as start day.

**time  start_time**

Specifies the start time **start_time** in **HH MIN SS** format.
Following format is used for **HH MIN SS** in **start_time**:

- **HH** specifies the hour of the start day in 24 hour format and must be an integer between 00 through 23.
- **MIN** specifies the minutes of the hour of the start day must be an integer between 00 through 59.
- **SS** specifies the seconds of the minute of the start day must be an integer between 00 through 59.

**end day  end_weekdays**

Specifies the end day as week days.
Following days are used as $end\_weekdays$:

- **friday** specifies Friday of the week as end day.
- **monday** specifies Monday of the week as end day.
- **saturday** specifies Saturday of the week as end day.
- **sunday** specifies Sunday of the week as end day.
- **thrusday** specifies Thursday of the week as end day.
- **tuesday** specifies Tuesday of the week as end day.
- **wednesday** specifies Wednesday of the week as end day.

\[time\] $end\_time$

Specifies the end time $end\_time$ in $HH\ MIN\ SS$ format.

Following format is used for $HH\ MIN\ SS$ in $end\_time$:

- $HH$ specifies the hour of the end day in 24 hour format and must be an integer between 00 through 23.
- $MIN$ specifies the minutes of the hour of the end day must be an integer between 00 through 59.
- $SS$ specifies the seconds of the minute of the end day must be an integer between 00 through 59.

\[time\] $start\_time$

Specifies the start time $start\_time$ in $HH\ MIN\ SS$ format.

Following format is used for $HH\ MIN\ SS$ in $start\_time$:

- $HH$ specifies the hour of the day in 24 hour format and must be an integer between 00 through 23.
- $MIN$ specifies the minutes of the hour of the day must be an integer between 00 through 59.
- $SS$ specifies the seconds of the minute of the day must be an integer between 00 through 59.

\[time\] $end\_time$

Specifies the end time $end\_time$ in $HH\ MIN\ SS$ format.

Following format is used for $HH\ MIN\ SS$ in $end\_time$:

- $HH$ specifies the end hour of the day in 24 hour format and must be an integer between 00 through 23.
- $MIN$ specifies the minutes of the end hour of the day must be an integer between 00 through 59.
- $SS$ specifies the seconds of the minute of the end hour must be an integer between 00 through 59.

**Usage**

Use this command to define a time slot with a start day, start time, and start date option for an event to trigger a procedure or condition in an IP-CAN session. A maximum of 12 time-slots can be configured through this command.

**Example**

The following command defines a time slot 2 which will start on Friday at 00:30:00 and ends on Saturday at 23:00:00:

```
start day friday start time 00 30 00 end day saturday time 23 00 00
```
Chapter 244
PCC-Usage-Monitor Configuration Mode Commands

The PCC-Usage-Monitor Configuration mode provides a mechanism to set the usage threshold limit in a PCC-Service-Profile to trigger a required condition and action set in PCC-Service instance.

**Important:** This configuration mode is supported from StarOS Release 12.1 onward.

Mode

Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Service Profile Configuration > PCC Usage-Monitor Configuration

```
configure > context context_name > pcc-service service_name > profile profile_name > usage-monitor usage_monitor_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-profile-usage-mon)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Use this command to return to the parent configuration mode.
usage-limit time

Sets the usage limit by time for a subscriber profile for a PCC-Service-Profile on an IPCF node.

**Product**
IPCF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Service Profile Configuration > PCC Usage-Monitor Configuration

```
configure > context context_name > pcc-service service_name > profile profile_name >
usage-monitor usage_monitor_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-profile-usage-mon)#
```

**Syntax**

```
[ default ] usage-limit time time_dur
```

- **default**
  
  Sets the usage limit time to 10 seconds for IP-CAN traffic in a PCC-Service-Profile.

- **time** time_dur
  
  Default: 10 secs.
  
  Specifies the usage duration (in seconds) for a PCC-service profile instance.
  
  `time_dur` must be an integer from 1 through 4294967296.

**Usage**

Use this command to set the usage limit in duration for subscriber profile for a PCC-Service-Profile on IPCF node.

**Example**

The following command sets the usage duration limit to 20000 seconds within a PCC-Service-Profile.

```
usage-limit time 20000
```
usage-limit volume

Sets the usage limit by volume for a subscriber profile for a PCC-Service-Profile on an IPCF node.

Product
IPCF

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PCC Service Configuration > PCC Service Profile Configuration > PCC Usage-Monitor Configuration

```
configure > context context_name > pcc-service service_name > profile profile_name > usage-monitor usage_monitor_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pcc-profile-usage-mon)#
```

Syntax

```
[default usage-limit volume [downlink dlink_volume | total total_volume | uplink uplink_volume]
```

---

default

Sets the usage limit volume to “0” for downlink, uplink and total bucket in a PCC-Service-Profile.

---

downlink dlink_volume

Specifies the usage volume (in kilobytes) in the downlink direction (from PCEF to UE) as an integer from 1 through 4294967296. A “0” (zero) value disables the downlink volume usage. Default: 0

---

total total_volume

Specifies the usage volume (in kilobytes) in the downlink and uplink directions (from PCEF to UE and PCEF to PDN) as an integer from 1 through 4294967296. A “0” (zero) value disables the downlink volume usage. Default: 0

---

uplink uplink_volume

Specifies the usage volume (in kilobytes) in the uplink direction (from PCEF to PDN) as an integer from 1 through 4294967296. A “0” (zero) value disables the downlink volume usage. Default: 0

---

Usage

Use this command to set the usage limit in volume for subscriber profile for a PCC-Service-Profile on IPCF node.

Example

The following command sets the usage limit volume to 20000 kilobytes in the upload direction within a PCC-Service-Profile.

```
usage-limit volume uplink 20000
```
The following command sets the usage limit volume to 400000 kilobytes in the download direction within a PCC-Service-Profile.

```
usage-limit volume downlink 400000
```
Chapter 245
PCP Configuration Mode Commands

The Port Control Protocol Service Configuration Mode is used to manage Port Control Protocol (PCP) service related configurations.

Important: This configuration mode is customer specific. For more information, contact your Cisco account representative.

Exec > ACS Configuration > Port Control Protocol Service Configuration

```
active-charging service service_name > pcp-service service_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-pcp-service)#
```

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed (s).
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Use this command to return to the parent configuration mode.
policy-control

This command enters the PCP Policy Control Configuration mode to configure policy control parameters for PCP service.

**Important:** This command is customer specific. For more information, contact your Cisco account representative.

**Product**
ACS
NAT
PSF

**Privilege**
Security Administrator, Administrator
Exec > ACS Configuration > Port Control Protocol Service Configuration

```
active-charging service service_name > pcp-service service_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-pcp-service)#
```

**Syntax**

```
[ default ] policy-control
```

- **default**
  Configures this command with the default setting.
  Default: Enabled

**Usage**

Use this command to enter the PCP Policy Control Configuration Mode to configure the policy control parameters for the PCP service.

On entering this command, the CLI prompt changes to:

```
[context_name]hostname(config-pcp-policy-control)#
```

Also see the **PCP Policy Control Configuration Mode Commands** chapter.
server

Configures the IP address of the PCP server to receive PCP packets.

**Important:** This command is customer specific. For more information, contact your Cisco account representative.

**Product**
- ACS
- NAT
- PSF

**Privilege**
- Security Administrator, Administrator
- Exec > ACS Configuration > Port Control Protocol Service Configuration

```bash
active-charging service service_name > pcp-service service_name
```

Entering the above command sequence results in the following prompt:
```
[local]host_name(config-pcp-service)#
```

**Syntax**

```bash
server ipv4-address ipv4_address [port port_number]

no server ipv4-address
```

- **server ipv4_address**
  - Specifies the IPv4 address of the server to receive PCP packets.
  - `ipv4_address` must be specified using the IPv4 dotted-decimal notation.

- **port port_number**
  - Specifies the UDP port number where PCP Request messages are received by the PCP service.
  - `port_number` must be an integer from 1 through 65535.
  - Default: 5351

**Usage**

Use this command to configure the IPv4 address on which the PCP service will receive PCP packets and the port on which PCP Request messages will be received from the PCP service.

**Example**

The following command configures the IPv4 address 1.2.3.4 with port number 5351 for the PCP service:

```bash
server ipv4-address 1.2.3.4 port 5351
```
Chapter 246
PCP Policy Control Configuration Mode Commands

The PCP Policy Control Configuration Mode is used to manage PCP policy control related configurations.

Important: This configuration mode is customer specific. For more information, contact your Cisco account representative.

Exec > ACS Configuration > PCP Configuration > Port Control Protocol Service Policy Control Configuration

active-charging service service_name > pcp-service service_name > policy-control

Entering the above command sequence results in the following prompt:

[local]host_name(config-pcp-policy-control)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed(s).
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
**exit**

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```Syntax
exit
```

**Usage**

Use this command to return to the parent configuration mode.
request-opcode

This command allows you to configure various PCP Request Opcode options.

Important: This command is customer specific. For more information, contact your Cisco account representative.

Product

ACS
NAT
PSF

Privilege

Security Administrator, Administrator
Exec > ACS Configuration > PCP Configuration > Port Control Protocol Service Policy Control Configuration

active-charging service service_name > pcp-service service_name > policy-control

Entering the above command sequence results in the following prompt:

[local]host_name(config-pcp-policy-control)#

Syntax

[ no ] request-opcode [ announce | map [ filter | prefer-failure ] | peer ] +

default request-opcode [ announce | map | peer ] +

no

Deletes the specific PCP opcode settings.

announce

Configures PCP ANNOUNCE opcode to process Announce Request messages.

map [ filter | prefer-failure ]

Configure PCP MAP opcode to process MAP Request messages.

•filter: MAP opcode received with this option contains remote IP/port. Processing will be the same as MAP without option but NAT binding will be 5-tuple if remote port is non-zero or 4-tuple if remote port is zero.

•prefer-failure: MAP opcode received with this option contains mapping IP/port which will be non-zero. Processing will be the same as MAP without option but if NAT binding allocation fails with the suggested mapping IP/port, then error will be returned.

peer

Configures PCP PEER opcode to process Peer Request messages.
Usage

Use this command to configure various PCP Request Opcode options.
**response-opcode**

This command allows you to configure various PCP Response Opcode options.

**Product**

ACS  
NAT  
PSF

**Privilege**

Security Administrator, Administrator

```
Exec > ACS Configuration > PCP Configuration > Port Control Protocol Service Policy Control Configuration
```

```
active-charging service service_name > pcp-service service_name > policy-control
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-pcp-policy-control)#
```

**Syntax**

```
response-opcode { map | peer } [ error { long life-time long_life_time | short life-time short_life_time } ] | success life-time succ_life_time ] +
{ default | no } response-opcode { map | peer } +
```

- **default**
  
  Configures this command with its default setting.

- **map**
  
  Configures the lifetime for which Map mappings are available.

- **peer**
  
  Configures the lifetime for which Peer mappings are available.

- **error**
  
  Configures the lifetime for long and short error cases, in seconds.  
  `long_life_time` and `short_life_time` must be an integer from 30 through 7200.

- **success**
  
  Configures the lifetime for successful long and short cases, in seconds. 
  `succ_life_time` must be an integer from 30 through 7200.

- **peer**
  
  Configures this command with its default setting.
Usage

Use this command to configure the PCP Response Opcode options.

Example

The following command configures the MAP opcode with lifetime for long and short error cases set to 600 and 30 respectively:

```
response-opcode map error long life-time 600 short life-time 30
```
Chapter 247
PDG Service Configuration Mode Commands

The PDG Service Configuration Mode is used to specify the properties required for the UEs in the WLAN (Wireless Local Access Network) to interface with the Packet Data Gateway/Tunnel Termination Gateway (PDG/TTG).

Mode

Exec > Global Configuration > Context Configuration > PDG Service Configuration

configure > context context_name > pdg-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pdg-service)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
aaa attribute

Sets the attributes that the system uses in AAA messages.

Product
PDG/TTG

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PDG Service Configuration
configure > context context_name > pdg-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pdg-service)#

Syntax

aaa attribute { 3gpp-negotiated-qos-profile string }

no aaa attribute

---

3gpp-negotiated-qos-profile string

Specifies the 3GPP negotiated QoS profile to use in AAA messages during IMS emergency call handling as an alphanumeric string of 1 through 31 characters.

no aaa attribute

Removes a previously configured AAA attribute.

---

Usage

Specifies the 3GPP negotiated QoS profile to use in AAA messages during IMS emergency call handling.

Example

The following command specifies the 3GPP negotiated QoS profile to use during IMS emergency call handling:

aaa attribute 3gpp-negotiated-qos-profile 100
### associate sgtp-service

Identifies the SGTP service to be associated with the PDG service to enable TTG functionality on the PDG/TTG. TTG functionality supports GTP-C (GTP control plane) messaging and GTP-U (GTP user data plane) messaging between the TTG and the GGSN over the Gn’ interface.

Important: This command can be used before the associated service instance is created and configured but care should be used to match the service names.

<table>
<thead>
<tr>
<th>Product</th>
<th>PDG/TTG</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privilege</td>
<td>Security Administrator, Administrator</td>
</tr>
<tr>
<td>Mode</td>
<td>Exec &gt; Global Configuration &gt; Context Configuration &gt; PDG Service Configuration</td>
</tr>
</tbody>
</table>

**Syntax**

```
[ no ] associate sgtp-service sgtp_service_name [ context sgtp_context_name ]
```

**no**

Removes the service association definition from the configuration.

**sgtp-service sgtp_service_name**

Specifies which SGTP service configuration, by naming the SGTP service instance, to associate with this PDG service.

*sgtp_service_name* is an alphanumeric string of 1 through 63 characters with no spaces.

**context sgtp_context_name**

Defines the context in which the SGTP service was created. If no context is specified, the current context is used.

*sgtp_context_name* is an alphanumeric string of 1 through 63 characters with no spaces.

**Usage**

Use this command to associate the SGTP service to be associated with the PDG service to enable TTG functionality on the PDG/TTG.

**Example**

The following command associates SGTP service *sgtp_service_1* with this PDG service:

```
associate sgtp-service sgtp_service_1 context sgtp_context_1
```
certificate-selection

Configures the PDG/TTG to select the trusted certificate (and the private key for calculating the AUTH payload) to be included in the first IKE_AUTH message from the PDG/TTG based on the APN (Access Point Name). The selected certificate is associated with the APN included in the IDr payload of the first IKE_AUTH message from the UE.

Product
PDG/TTG

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PDG Service Configuration

configure > context context_name > pdg-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pdg-service)#

Syntax

[ no ] certificate-selection apn-based

default certificate-selection

certificate-selection apn-based

Selects a trusted certificate for the first IKE-AUTH message based on the APN.

no certificate-selection

Disables APN-based certificate selection and resumes sending a certificate bound to a crypto template.

default certificate-selection

Sets the default certificate selection method to a certificate bound to a crypto template.

Usage

Configures the PDG/TTG to select the trusted certificate to be included in the first IKE_AUTH message based on the APN.

Example

Use the following example to enable APN-based certificate selection:

certificate-selection apn-based
bind

Binds the PDG service IP address to a crypto template and specifies the maximum number of sessions the PDG service supports.

**Product**
PDG/TTG

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PDG Service Configuration

`configure > context context_name > pdg-service service_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pdg-service)#
```

**Syntax**

```
[ no ] bind address ipv4_address { crypto-template string } mode { ttg | pdg } [ max-sessions number ]
```

---

**no**

Removes a previously configured binding.

```
bind address ipv4_address
```

Specifies the IPv4 address of the PDG service with which the UE attempts to establish an IKEv2/IPSec tunnel. This address must be a valid IP address within the context. This is a mandatory parameter.

```
crypto-template string
```

Specifies the name of the crypto template to be bound to the PDG service. This is the name of the IPSec policy to be used as a template for PDG/TTG subscriber session IPSec policies. The crypto template includes most of the IPSec and IKEv2 parameters for keepalive, lifetime, NAT-T, and cryptographic and authentication algorithms. There must be one crypto template per PDG service. This is a mandatory parameter.

*string* is an alphanumeric string of 0 through 127 characters.

```
mode { ttg | pdg }
```

Default: There is no default value.

Specifies whether the PDG service provides TTG or PDG functionality, as follows:

- In TTG mode, PDN connectivity is provided through the GGSN. PDG functionality is provided by the combined TTG and GGSN.
- In PDG mode, PDN connectivity and PDG functionality are provided directly through the PDG service.

This is a mandatory parameter.

---

**Important:** PDG mode is not supported in this software release.
Dependencies:
When you configure the PDG service to be in TTG mode, you must also configure the SGTP service using the `associate sgtp-service` command, as the TTG needs to connect with the GGSN to complete the PDG functionality.

The following behaviors occur when the PDG service operates in TTG mode:

- If the SGTP service associated with PDG service is not configured, the PDG service is not started.
- If the SGTP service associated with PDG service is not started, the PDG service is not started.
- If the SGTP service associated with PDG service is stopped, the PDG service is stopped.
- If the SGTP service associated with PDG service is re-started, the PDG service is re-started.
- If the SGTP service is not yet configured, whenever the SGTP service is started, the PDG service is started.

Note that starting or stopping the PDG service has no impact on the SGTP service.

```
max-sessions number
```

Specifies the maximum number of sessions to be supported by the PDG service as an integer from 0 through 1000000. Default: 1000000.

If the `max-sessions` value is changed on an existing system, the new value takes effect immediately if it is higher than the current value. If the new value is lower than the current value, existing sessions remain established, but no new sessions are permitted until usage falls below the newly-configured value.

Usage
Use this command in PDG Service Configuration Mode to bind the IP address used as the connection point for establishing IKEv2/IPSec sessions to a crypto template. You can also use it to define the maximum number of sessions the PDG service supports.

Example
The following command binds a PDG service with an IP address of 10.2.3.4 to the crypto template `crypto_template_1`, sets the mode to TTG, and sets the maximum number of sessions to 500000:

```
bind address 10.2.3.4 crypto-template crypto_template_1 mode ttg max-sessions 500000
```
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
end
```

**Usage**

Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**
Use this command to return to the parent configuration mode.
ip gnp-qos-dscp

Configures the quality of service (QoS) differentiated service code point (DSCP) used when sending data packets over the Gn’ interface in the uplink direction.

**Product**
PDG/TTG

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PDG Service Configuration

    configure > context context_name > pdg-service service_name

Entering the above command sequence results in the following prompt:

    [context_name]host_name(config-pdg-service)#

**Syntax**

```
[ no ] ip gnp-qos-dscp {   background dscp | conversational dscp | interactive dscp | streaming dscp | interactive [ traffic-handling-priority traffic_priority ] { allocation-retention-priority allocation_retention_priority } } +
default ip gnp-qos-dscp
```

no

Disables the overriding of the ToS (Type of Service) field and enables the pass-through option.

**background dscp**

Specifies the DSCP marking to be used for packets of sessions subscribed to the 3GPP background class, in which the data transfer is not time-critical (for example, in e-mail exchanges). This traffic class is the lowest QoS.

*dscp:* Sets the DSCP for the specified traffic class. See the dscp section below.

**conversational dscp**

Specifies the DSCP marking to be used for packets of sessions subscribed to the 3GPP conversational class, in which there is a constant flow of traffic in both the uplink and downlink direction. This traffic class is the highest QoS.

*dscp:* Sets the DSCP for the specified traffic pattern. See the dscp section below.

**interactive [ traffic-handling-priority traffic_priority ]**

Specifies the DSCP marking to be used for packets of sessions subscribed to three possible traffic priorities in the 3GPP interactive class, in which there is an intermittent flow of packets in the uplink and downlink direction. This traffic class has a higher QoS than the background class, but not as high as the streaming class. *traffic_priority* is the 3GPP traffic handling priority and can be the integers 1, 2 or 3.
**allocation-retention-priority** `allocation_retention_priority`

Specifies the DSCP for the interactive class if the allocation priority is present in the QoS profile.  
`allocation-retention-priority` can be the integers 1, 2, or 3.  
DSCP uses the values in the following table based on the traffic handling priority and allocation/retention priority if the allocation priority is present in the QoS profile.

<table>
<thead>
<tr>
<th>Allocation Priority</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic Handling Priority</td>
<td>ef</td>
<td>ef</td>
<td>ef</td>
</tr>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>af21</td>
<td>af21</td>
<td>af21</td>
</tr>
<tr>
<td>3</td>
<td>af21</td>
<td>af21</td>
<td>af21</td>
</tr>
</tbody>
</table>

**Important**: If you only configure DCSP marking for interactive traffic classes without specifying ARP, it may not properly take effect. The CLI allows this scenario for backward compatibility however, it is recommended that you configure all three values.

**streaming** `dscp`

Specifies the DSCP marking to be used for packets of sessions subscribed to the 3GPP streaming class, in which there is a constant flow of data in either in the uplink or downlink direction. This traffic class has a higher QoS than the interactive class, but not as high as the conversational class.

dscp: Set the DSCP for the specified traffic pattern. See the dscp section below.

**dscp**

Default:

- **background**: be
- **interactive**
- **Traffic Priority 1**: ef
- **Traffic Priority 1**: af21
- **Traffic Priority 1**: af21
- **streaming**: af11
- **conversational**: ef

Specifies the DSCP for the specified traffic pattern. `dscp` can be configured to any one of the following:

- af11: Assured Forwarding 11 per-hop-behavior (PHB)
- af12: Assured Forwarding 12 PHB
- af13: Assured Forwarding 13 PHB
- af33: Assured Forwarding 33 PHB
- af41: Assured Forwarding 41 PHB
- af42: Assured Forwarding 42 PHB
Related Keywords

- af21: Assured Forwarding 21 PHB
- af22: Assured Forwarding 22 PHB
- af23: Assured Forwarding 23 PHB
- af31: Assured Forwarding 31 PHB
- af32: Assured Forwarding 32 PHB
- af41: Assured Forwarding 41 PHB
- af42: Assured Forwarding 42 PHB
- af43: Assured Forwarding 43 PHB
- be: Best effort forwarding PHB
- ef: Expedited forwarding PHB

More than one of the above keywords can be entered within a single command.

Usage

DSCP levels can be assigned to specific traffic patterns in order to ensure that data packets are delivered according to the precedence with which they’re tagged. The diffserv markings are applied to the IP header of every subscriber data packet transmitted over the Gn’ interface(s).

The four traffic patterns have the following order of precedence: background (lowest), interactive, streaming, and conversational (highest). Data packets falling under the category of each of the traffic patterns are tagged with a DSCP that further indicate their precedence as shown in the following tables:

<table>
<thead>
<tr>
<th>Drop Precedence</th>
<th>Class</th>
<th>Class</th>
<th>Class</th>
<th>Class</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>af11</td>
<td>af21</td>
<td>af31</td>
<td>af41</td>
</tr>
<tr>
<td>Medium</td>
<td>af12</td>
<td>af22</td>
<td>af32</td>
<td>af41</td>
</tr>
<tr>
<td>High</td>
<td>af13</td>
<td>af23</td>
<td>af33</td>
<td>af43</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Precedence (low to high)</th>
<th>DSCP</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Best Effort (be)</td>
</tr>
<tr>
<td>2</td>
<td>Class 1</td>
</tr>
<tr>
<td>3</td>
<td>Class 2</td>
</tr>
<tr>
<td>4</td>
<td>Class 3</td>
</tr>
<tr>
<td>5</td>
<td>Class 4</td>
</tr>
<tr>
<td>6</td>
<td>Express Forwarding (ef)</td>
</tr>
</tbody>
</table>

The DSCP level can be configured for multiple traffic patterns within a single instance of this command.

Example

The following command configures the DSCP level for the streaming traffic pattern to be ef:

```
ip gnp-qos-dscp streaming ef
```
The following command configures the DSCP levels for the conversational, streaming, interactive and background traffic patterns to be ef, af22, and af41, respectively:

```
ip gnp-qos-dscp conversational ef streaming ef interactive af22 background af41
```
**ip qos-dscp**

Configures the quality of service (QoS) differentiated service code point (DSCP) used when sending data packets over the Wu interface in the downlink direction.

**Product**
PDG/TTG

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PDG Service Configuration

```
configure > context context_name > pdg-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pdg-service)#
```

**Syntax**

```
ip qos-dscp { qci { 1 { dscp-pt } | 2 { dscp-pt } | 3 { dscp-pt } | 4 { dscp-pt } | 5 { allocation-retention-priority 1..3 | dscp-pt } | 6 { allocation-retention-priority 1..3 | dscp-pt } | 7 { allocation-retention-priority 1..3 | dscp-pt } | 8 { allocation-retention-priority 1..3 | dscp-pt } | 9 { dscp-pt } + } allocation-retention-priority
```

```
no ip qos-dscp { qci { 1 | 2 | 3 | 4 | 5 { allocation-retention-priority 1..3 | dscp-pt } | 6 { allocation-retention-priority 1..3 | dscp-pt } | 7 { allocation-retention-priority 1..3 | dscp-pt } | 8 { allocation-retention-priority 1..3 | dscp-pt } | 9 { allocation-retention-priority 1..3 | dscp-pt } | 9 {+ allocation-retention-priority }
```

**allocation-retention-priority**

Specifies the DSCP for interactive class if the allocation priority is present in the QOS profile.

** allocation-retention-priority ** can be the integers 1, 2, or 3.

DSCP values use the following matrix to map based on traffic handling priority and Alloc/Retention priority if the allocation priority is present in the QOS profile.

The following table shows the DSCP value matrix for **allocation-retention-priority**.

**Table 37. Default DSCP Value Matrix**

<table>
<thead>
<tr>
<th>Traffic Handling Priority</th>
<th>Allocation Priority 1</th>
<th>Allocation Priority 2</th>
<th>Allocation Priority 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ef</td>
<td>ef</td>
<td>ef</td>
</tr>
<tr>
<td>2</td>
<td>af21</td>
<td>af21</td>
<td>af21</td>
</tr>
<tr>
<td>3</td>
<td>af21</td>
<td>af21</td>
<td>af21</td>
</tr>
</tbody>
</table>
**qci**

Configures the QCI attribute of QoS. Here the qci_val is the QCI for which the negotiate limit is being set, it ranges from 1 to 9.

**dscp**

Default QCI:
- 1: ef
- 2: ef
- 3: af11
- 4: af11
- 5: ef
- 6: ef
- 7: af21
- 8: af21
- 9: be

Specifies the DSCP for the specified traffic pattern. dscp can be configured to any one of the following:

<table>
<thead>
<tr>
<th>af11: Assured Forwarding 11 per-hop-behavior (PHB)</th>
<th>af32: Assured Forwarding 32 PHB</th>
</tr>
</thead>
<tbody>
<tr>
<td>af12: Assured Forwarding 12 PHB</td>
<td>af33: Assured Forwarding 33 PHB</td>
</tr>
<tr>
<td>af13: Assured Forwarding 13 PHB</td>
<td>af41: Assured Forwarding 41 PHB</td>
</tr>
<tr>
<td>af21: Assured Forwarding 21 PHB</td>
<td>af42: Assured Forwarding 42 PHB</td>
</tr>
<tr>
<td>af22: Assured Forwarding 22 PHB</td>
<td>af43: Assured Forwarding 43 PHB</td>
</tr>
<tr>
<td>af23: Assured Forwarding 23 PHB</td>
<td>be: Best effort forwarding PHB</td>
</tr>
<tr>
<td>af31: Assured Forwarding 31 PHB</td>
<td>ef: Expedited forwarding PHB</td>
</tr>
</tbody>
</table>

More than one of the above keywords can be entered within a single command.

**Usage**

You can assign DSCP to specific traffic patterns to ensure that data packets are delivered according to the precedence with which they are tagged. The diffserv markings are applied to the outer IP header of every GTP data packet. The diffserv marking of the inner IP header is not modified.

The traffic patterns are defined by QCI (1 to 9). Data packets falling under the category of each of the traffic patterns are tagged with a DSCP that further indicate their precedence as shown in the following tables:
Table 38. Class structure for assured forwarding (af) levels

<table>
<thead>
<tr>
<th>Drop Precedence</th>
<th>Class</th>
<th>Class 2</th>
<th>Class 3</th>
<th>Class 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>af11</td>
<td>af21</td>
<td>af31</td>
<td>af41</td>
</tr>
<tr>
<td>Medium</td>
<td>af12</td>
<td>af22</td>
<td>af32</td>
<td>af41</td>
</tr>
<tr>
<td>High</td>
<td>af13</td>
<td>af23</td>
<td>af33</td>
<td>af43</td>
</tr>
</tbody>
</table>

Table 39. DSCP Precedence

<table>
<thead>
<tr>
<th>Precedence (low to high)</th>
<th>DSCP</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Best Effort (be)</td>
</tr>
<tr>
<td>1</td>
<td>Class 1</td>
</tr>
<tr>
<td>2</td>
<td>Class 2</td>
</tr>
<tr>
<td>3</td>
<td>Class 3</td>
</tr>
<tr>
<td>4</td>
<td>Class 4</td>
</tr>
<tr>
<td>5</td>
<td>Express Forwarding (ef)</td>
</tr>
</tbody>
</table>

The DSCP level can be configured for multiple traffic patterns within a single instance of this command. The no ip qos command can be issued to remove a QOS setting and return it to it’s default setting.

Example

The following command configures the DSCP level for QCI to be Expedited Forwarding, `ef`:

```
   ip qos-dscp qci 1 ef
```
ip source-violation

Sets the parameters for IP source validation. Source validation is useful if packet spoofing is suspected, or for verifying packet routing and labeling within the network.

Product
PDG/TTG

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PDG Service Configuration
configure > context context_name > pdg-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pdg-service)#

Syntax

ip source-violation { clear-on-valid-packet | drop-limit num period secs }
default ip source-violation { drop-limit num period secs }
no ip source-violation clear-on-valid-packet

clear-on-valid-packet
Configures the service to reset the drop-limit counters upon receipt of a properly addressed packet. Default: disabled

drop-limit num
Sets the maximum number of allowed IP source violations within the detection period before dropping a call. If num is not specified, the value is set to the default value. num is an integer from 1 to 1000000. Default: 10

period secs
Sets the detection period (in seconds) for IP source violations as an integer from 1 through 1000000. If secs is not specified, the value is set to the default value. Default: 120

default ip source-violation { drop-limit num period secs }
Sets or restores the IP source violation detection defaults, as follows:

• drop-limit: Sets or restores the maximum number of IP source violations within the detection period before dropping the call to the default value of 10.

• period: Sets or restores the detection period for IP source violations to the default value of 120 seconds.

no ip source-violation clear-on-valid-packet
The drop-limit counters are not reset upon receipt of a properly addressed packet.
**Usage**

Source validation is useful if packet spoofing is suspected or for verifying packet routing and labeling within the network.

Source validation requires the source address of received packets to match the IP address assigned to the subscriber (either statically or dynamically) during the session.

This function operates in the following manner: When a subscriber packet is received with a source IP address violation, the system increments the IP source violation drop-limit counter and starts the timer for the IP source violation period. Every subsequent packet received with a bad source address during the IP source violation period causes the drop-limit counter to increment. For example, if the drop-limit is set to 10, after 10 source violations, the call is dropped. The detection period timer continues to count throughout this process.

**Example**

The following command sets the drop limit to 15 and leaves the other values at their default values:

```
  ip source-violation drop-limit 15
```
max-tunnels-per-ue

Specifies the maximum number of IKEv2/IPSec tunnels allowed per UE by the PDG/TTG. This maximum number is specified per PDG service.

Product
PDG/TTG

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PDG Service Configuration

configure > context context_name > pdg-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pdg-service)#

Syntax

max-tunnels-per-ue integer

default max-tunnels-per-ue

integer

Specifies the maximum number of IKEv2/IPSec tunnels allowed per UE as an integer from 1 to 11. Default: 11

default max-tunnels-per-ue

Sets the maximum number of IKEv2/IPSec tunnels allowed per UE to its default value, which is 11.

Usage

Use this command to set the maximum number of IKEv2/IPSec tunnels allowed per UE.

Example

Use the following command to set the maximum number of IKEv2/IPSec tunnels allowed per UE to 2:

max-tunnels-per-ue 2
**plmn id**

Configures location specific mobile network identifiers used to help translate local emergency and service-related numbers. Default is disabled.

**Product**
PDG/TTG

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PDG Service Configuration

```
configure > context context_name > pdg-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pdg-service)#
```

**Syntax**

```
plmn id mcc mcc_number mnc mnc_number
no plmn id mcc mcc_number mnc mnc_number
```

- **mcc mcc_number**
  Specifies the mobile country code (MCC) portion of the PLMN identifier as an integer from 200 through 999.

- **mnc mnc_number**
  Specifies the mobile network code (MNC) portion of the PLMN identifier as a 2- or 2-digit integer from 00 through 999.

- **no plmn id mcc mcc_number mnc mnc_number**
  Removes a previously configured PLMN identifier for the PDG service.

**Usage**
The PLMN ID is included in the RAI (Routing Area Identity) field of the PDP Create Request messages sent to the GGSN. Multiple PDG services can be configured with the same PLMN identifier. Up to five PLMN IDs can be configured for each PDG service.

**Example**
The following command configures the PLMN identifier with an MCC of 462 and MNC of 2:

```
plmn id mcc 462 mnc 02
```
setup-timeout

Specifies the maximum time allowed to set up a session.

Product
PDG/TTG

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PDG Service Configuration
configure > context context_name > pdg-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pdg-service)#

Syntax

```plaintext
setup-timeout integer

default setup-timeout
```

setup-timeout integer

Sets the session setup timeout value (in seconds) as an integer from 2 through 300. Default: 60

default setup-timeout

Sets or restores the default session setup timer value to 60 seconds.

Usage
The PDG/TTG clears both the user session and tunnels if a call does not initiate successfully before the session setup timer expires.

Example
The following command sets the session setup timeout value to the default value of 60 seconds:

```plaintext
default setup-timeout
```
Chapter 248
PDIF Service Configuration Mode Commands

The PDIF Service Configuration Mode is used to configure the properties required for a mobile station to interface with a Packet Data Interworking Function (PDIF).

**Mode**

Exec > Global Configuration > Context Configuration > PDIF Service Configuration

```
configure > context context_name > pdif-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pdif-service)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
aaa attribute

Sets the system attributes for AAA messages.

**Product**
PDIF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PDIF Service Configuration

```bash
configure > context context_name > pdif-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pdif-service)#
```

**Syntax**

```bash
aaa attribute { 3gpp2-bsid string | 3gpp2-service-option integer | calling-station-id integer | 3gpp2-serving-pcf ip-address }
```

```bash
no aaa attribute
```

```bash
default aaa attribute 3gpp2-service-option integer
```

- **no**

  Removes a previously configured AAA attribute.

- **default**

  Returns the specified aaa attribute to the original default system settings.

- **3gpp2-bsid string**

  Specifies the base-station ID and consists of the SID + NID + CELLID. `string` must contain 12 hexadecimal upper-case ASCII characters.

- **3gpp2-service-option integer**

  Specifies the radius attribute value when sending authentication and accounting messages as an integer from 0 through 32767. Default: 4095

- **calling-station-id integer**

  Specifies the calling station phone number as a sequence of 1 through 15 digits.

- **3gpp2-serving-pcf ip-address**

  Use this command to generate attribute values without creating a new ASR 5000ASR 5500 image.
Usage
If the RADIUS protocol is being used, accounting messages can be sent over a AAA interface to the RADIUS server.
3gpp2-serving-pcf attribute value (if configured) is sent in both RADIUS authentication and accounting messages. If the attribute value is not configured (or explicitly “not configured” using the no keyword), RADIUS attributes are still included with just type and length. This is because inclusion/exclusion of RADIUS attributes are still controlled through the dictionary, not via the CLI.

Example
The following command identifies the base station ID:

```
    aaa attribute 3gpp2-bsid 0ab2389acb3
```
aaa authentication

Sets the aaa authentication for first and second phase authentication when multiple authentication is configured on the system.

Product
PDIF

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PDIF Service Configuration

configure > context context_name > pdif-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pdif-service)#

Syntax

aaa authentication { { first-phase | second-phase } | { context-name name aaa-group name } }

no aaa authentication { first-phase | second-phase }

no aaa authentication { first-phase | second-phase }

Removes any existing authentication configuration.

first-phase context-name name aaa-group name

Specifies the context name and the aaa group name configured in the context for the first authentication phase.

Important: First phase authentication is mandatory when multiple authentication is configured on the system.

• context-name name: Specifies the context where the aaa server group is defined as an alphanumeric string of 1 through 79 characters.

• aaa-group name: Specifies the name of the aaa-group to be used for authentication as an alphanumeric string of 1 through 79 characters.

second-phase context-name name aaa-group name

Specifies the context name and the aaa group name configured in the context for the second authentication phase.

• context-name name: Specifies the context where aaa server group is defined as an alphanumeric string of 1 through 79 characters.

• aaa-group name: Specifies the name of the aaa-group to be used for authentication as an alphanumeric string of 1 through 63 characters.
Usage

Two phase-authentication happens in IKEv2 setup for setting up the IPSec session. The first authentication uses Diameter AAA EAP method and second authentication uses RADIUS AAA authentication. The same AAA context may be used for both authentications. PDIF service allows you to specify only a single AAA group, which could normally be used for the first authentication method.

A given AAA group only supports either Diameter or RADIUS authentication. If the NAI in the first authentication is different from NAI in the second authentication each NAI can point to a different domain profile in the PDIF. Each domain profile may be configured with each AAA group, one for Diameter and the other for RADIUS.

Example

Use the following to configure first-phase authentication for an aaa group named `aaa-10` in the PDIF context:

```
first-phase context-name pdif aaa-group aaa-10
```
bind

Binds the service IP address to a crypto template and configures the number of sessions the PDIF can support.

**Product**
PDIF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PDIF Service Configuration

```
configure > context context_name > pdif-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pdif-service)#
```

**Syntax**

```
bind address address { crypto-template string } [ max-sessions number ]
no bind
```

- **no**
  Removes a previously configured binding.

- **address**
  Specifies the IP address of the service.

- **crypto-template string**
  Specifies the name of the crypto template to be bound to the service as an alphanumeric string of 0 through 127 characters.

- **max-sessions number**
  Specifies the maximum number of sessions to be supported by the service as an integer from 0 to 3000000.
  Default: 3000000
  If the max-sessions value is changed on an existing system, the new value takes effect immediately if it is higher than the current value. If the new value is lower than the current value, existing sessions remain established, but no new sessions are permitted until usage falls below the newly-configured value.

**Usage**

Binds the IP address used as the connection point for establishing the IKEv2 sessions to the crypto template. It can also define the number of sessions the PDIF can support.

**Example**

The following command binds a service with the IP address 13.1.1.1 to the crypto template T1 and sets the maximum number of sessions to 200000:

```
bind address 13.1.1.1 crypto-template T1 max-sessions 200000
```
default

Sets or restores the default condition for the selected parameter.

**Product**

PDIF

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > PDIF Service Configuration

```bash
configure > context context_name > pdif-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pdif-service)#
```

**Syntax**

```bash
default { { aaa attribute 3gpp2-service-option } | duplicate-session-detection | hss { failure-handling mac-address-validation-failure | mac-address-validation | update-profile } | ip source-violation { drop-limit | period } | setup-timeout | subscriber name | username mac-address-stripping } }
```

---

**aaa attribute 3gpp2-service-option**

Configures the default value 4095.

---

**duplicate-session-detection**

Configures the default to be NAI-based.

---

**hss { failure-handling mac-address-validation-failure | mac-address-validation | update-profile }**

Configures the HSS server defaults:
- **failure-handling mac-address-validation-failure**: By default, the MAC address is validated by IMS-Sh interface.
  - **mac-address-validation**: By default, validating the MAC address is disabled.
  - **update-profile**: By default, updating the PDIF profile is disabled.

---

**ip source-violation { drop-limit | period }**

Configures IP source-violation detection defaults.
- **drop-limit**: Default number of IP source violations permitted in detection period before the call is dropped is 10.
- **period**: Default detection period is 120 seconds.

---

**setup-timeout**

Default call setup time limit is 60 seconds.
**subscriber name**

Configures the default subscriber name. *name* is a string of 1-127 characters.

**username mac-address-stripping**

Default is to disable stripping the MAC address from the username.

**Usage**

Configures the default settings for a given parameter.

**Example**

Use the following example to configure the default call setup time limit:

```
default setup-timeout
```
duplicate-session-detection

Configures the PDIF to detect duplicate call sessions using old IMSI or NAI addresses and clear old call information.

**Product**
PDIF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PDIF Service Configuration
configure > context context_name > pdif-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pdif-service)#

**Syntax**

```
[ no | default ] duplicate-session-detection { imsi-based | nai-based }
```

- **no**
  Stops duplicate session detection.

- **default**
  Configures the default setting, which is NAI-based detection.

- **imsi-based**
  Configures the PDIF to detect duplicate call sessions based on the IMSI address.

- **nai-based**
  Configures the PDIF to detect duplicate call sessions based on the NAI address. This is the default setting.

**Usage**

If an MS leaves the Wi-Fi coverage area and subsequently comes back online, it may initiate a new session setup procedure. After both the device authentication with HSS and the subscriber authentication with AAA server are completed, PDIF runs the internal mechanism to see whether there was any other session bound with the same IMSI. If an old session is detected, PDIF starts clearing this old session by sending a proxy-MIP Deregistration request to the HA. PDIF resumes new session setup by sending a proxy-MIP registration request. When the old session is aborted, PDIF sends Diameter STR messages and RADIUS Acct STOP messages to corresponding AAA servers.

PDIF allows duplicate session detection based on either the NAI or IMSI addresses. When detecting based on NAI, it is the first-phase (device authentication) NAI that is used.

**Example**

The following command configures duplicate session detection to use IMSI addressing:

```
duplicate-session-detection imsi
```
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
end

**Usage**
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

exit

Usage
Use this command to return to the parent configuration mode.
**hss**

Configures the Home Subscriber Server (HSS) parameters.

**Product**
PDIF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PDIF Service Configuration

```
configure > context context_name > pdif-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pdif-service)#
```

**Syntax**

```
hss { failure-handling { { mac-address-validation-failure | update-profile } action { continue | terminate } } | update-profile | mac-address-validation } 

[ no | default ] hss { failure-handling | update-profile | mac-address-validation }
```

- **no**
  Removes a previously configured HSS profile.

- **default**
  Resets the defaults for this command.

- **failure-handling mac-address-validation-failure**
  Configures how the HSS is to handle errors.
  If HSS returns a list of MAC addresses and if PDIF fails to match the subscriber MAC address against the list, the session is always terminated.

  - **action { continue | terminate }**
    Configures the action to be performed depending on the failure type.
    - **continue**: Ignores a mac-address-validation-failure and continue the session.
    - **terminate**: Terminates the session on a mac-address-validation-failure.

- **mac-address-validation**
  If mac-address-validation is enabled, the PDIF queries the HSS for a list of MAC addresses associated with the Mobile Directory Number (MDN). Default: Disabled

- **update-profile**
  Update the HSS with the subscriber profile. Default: Disabled
Usage

An HSS provides MAC address validation and store part of the subscriber profile. This command enables or disables validation and profile updates, and configures how the system responds to failures: terminate or continue a session.

An ims-sh-service and Diameter interface need to be configured to communicate with the HSS.

Example

The following example enables mac-address validation:

```
hss mac-address-validation
```
ims-sh-service

Associates the IMS-Sh-service parameters.

Product
PDIF

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PDIF Service Configuration

configure > context context_name > pdif-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pdif-service)#

Syntax

ims-sh-service name name

no ims-sh-service name name

no

Removes a previously configured IMS-Sh-service.

name

Names the IMS-Sh-service in the pdif-service context.

Usage

This command is used to name the IMS-Sh-service.

Example

The following command names the IMS-Sh-service ims1:

ims-sh-service name ims1
**ip source-violation**

Sets the parameters for IP source validation. Source validation is useful if packet spoofing is suspected or for verifying packet routing and labeling within the network.

Source validation requires that the source address of the received packets matches the IP address assigned to the subscriber (either statically or dynamically) during the session.

**Product**
PDIF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PDIF Service Configuration

```bash
configure > context context_name > pdif-service service_name
```

Entering the above command sequence results in the following prompt:

```
context_name host_name(config-pdif-service)#
```

**Syntax**

```bash
ip source-violation { clear-on-valid-packet | drop-limit num | period secs }

no ip source-violation clear-on-valid-packet
```

**clear-on-valid-packet**

Configures the service to reset the reneg-limit and drop-limit counters after receipt of a properly addressed packet. Default: disabled

**drop-limit**

```bash
num
```

Sets the number of allowed source violations within a detection period before forcing a call disconnect. If `num` is not specified, the value is set to the default.

`num` is an integer from 1 to 1000000. Default: 10

**period**

```bash
secs
```

Sets the length of time (in seconds) for a source violation detection period to last. If `secs` is not specified, the value is set to the default.

`secs` is an integer from 1 to 1000000. Default: 120

**Usage**

This function is intended to allow the operator to configure a network to prevent problems such as when a user gets handed back and forth between two PDIFs a number of times during a handoff scenario.

This function operates in the following manner:

When a subscriber packet is received with a source address violation, the system increments the IP source-violation drop-limit counter and starts the timer for the IP-source violation period. Every subsequent packet received with a bad source address during the IP-source violation period causes the drop-limit counter to increment.
For example, if the drop-limit is set to 10, after 10 source violations, the call is dropped. The period timer continues to count throughout this process.

Example

The following command sets the drop limit to 15 and leaves the other values at their defaults:

```
ip source-violation drop-limit 15
```
**mobile-ip**

Sets the MIP FA context for the specific PDIF service.

**Product**

PDIF

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > PDIF Service Configuration

```plaintext
configure > context context_name > pdif-service service_name
```

Entering the above command sequence results in the following prompt:

```plaintext
[context_name]host_name(config-pdif-service)#
```

**Syntax**

```plaintext
mobile-ip foreign-agent context string [ fa-service string ]

no mobile-ip
```

- **no**
  
  Removes previously configured parameters.

- **foreign-agent context string**
  
  Specifies the context name in which the FA is configured as an alphanumeric string of 1 through 79 characters.

- **fa-service string**
  
  Specifies the name of the FA service in the FA context as an alphanumeric string of 1 through 79 characters.

**Usage**

Shows in which context the FA is located and names the FA service.

**Example**

This command configures MIP for the FA context named *fal*:

```plaintext
mobile-ip foreign-agent context fal
```
setup-timeout

Configures the maximum time allowed to set up a session.

**Product**

PDIF

**Privilege**

Security-Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > PDIF Service Configuration

```
configure > context context_name > pdif-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pdif-service)#
```

**Syntax**

```
setup-timeout integer

default setup-timeout
```

```
setup-timeout integer

Specifies the session setup timer (in seconds) as an integer from 2 through 300. Default: 60
```

```
default setup-timeout

Defaults the session setup timer to 60 seconds.
```

**Usage**

PDIF clears both user session and tunnels if a call does not initiate successfully before the timer expires.

**Example**

The following command sets the setup-timeout to the default 30 seconds:

```
default setup-timeout
```
username

Configures mac-address-stripping on a username coming in from a mobile station session.

**Product**
PDIF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PDIF Service Configuration

```config
configure > context context_name > pdif-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pdif-service)#
```

**Syntax**

```
username mac-address-stripping

[ default | no ] username mac-address-stripping
```

- **username mac-address-stripping**
  
  Configures mac-address stripping from the Network Access Identifier (NAI).

- **default**
  
  Configures the default parameter which is **disabled**.

- **no**
  
  Returns the configuration to the default condition.

**Usage**

When enabled, PDIF strips the MAC address from a mobile username NAI before sending to the RADIUS AAA server.

**Example**

The following example disables mac-address-stripping.

```
no username mac-address-stripping
```
Chapter 249
PDSN Service Configuration Mode Commands

The PDSN Service Configuration Mode is used to create and manage PDSN service instances for the current context.

Mode

Exec > Global Configuration > Context Configuration > PDSN Service Configuration
configure > context context_name > pdsn-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pdsn-service)#

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
a11-signalling-packets
Applies DSCP marking for IP header carrying outgoing A11-signalling packets.

Product
PDSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PDSN Service Configuration
configure > context context_name > pdsn-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pdsn-service)#

Syntax
a11-signalling-packets ip-header-dscp hexa_number

[ no | default ] a11-signalling-packets ip-header-dscp

<table>
<thead>
<tr>
<th>no</th>
</tr>
</thead>
</table>
| Disables the a11-signalling-packets ip-header-dscp option configuration.

<table>
<thead>
<tr>
<th>default</th>
</tr>
</thead>
</table>
| Sets / Restores default value assigned for specified parameter a11-signalling-packets ip-header-dscp.

hexa_number

a Hexa decimal number between 0x0 and 0x3F.

Usage
Use this command to configured value of DSCP to be set for all outgoing A11 signaling msg. By default the CLI is disabled and DSCP is marked as 0 in ip-header.

Example
The following command configures value of DSCP to be set for all outgoing to A11 signaling message 0x3F:

a11-signalling-packets ip-header-dscp 0x3F
aaa 3gpp2-service-option

Specifies the value for the 3gpp2-service option.

Product
PDSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PDSN Service Configuration
configure > context context_name > psdn-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-psdn-service)#

Syntax

aaa 3gpp2-service-option number
no aaa 3gpp2-service-option
default aaa 3gpp2-service-option

---

no
Disables the aaa 3gpp2-service option configuration.

---

default
Sets / Restores default value assigned for specified parameter aaa 3gpp2-service-option.

---

number
Service option number is integer and should be between 0 to 32767.

---

Usage

Allows the configuration of a default service option value to be sent in accounting when service option values are not received from PCF. The PDSN will default the service option value to the configured value if the value is not specified by the PCF.

Example

The following command sets the service option to be 40:

    aaa 3gpp2-service-option 40
aaa nas-ip-address

Product
PDSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PDSN Service Configuration
configure > context context_name > pdsn-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-psdn-service)#

Syntax

aaa nas-ip-address IPv4 address

no aaa nas-ip-address

default aaa 3nas-ip-address

no
Disables the aaa nas-ip-address option configuration.

default
Sets / Restores default value assigned for specified parameter aaa nas-ip-address by default this is disabled.

ipv4 address
Specifies the IPv4 addresses to be used.

Usage
Allows the configuration.

Example
The following command configures 1.2.3.4:

aaa as-ip-address 1.2.3.4
access-flow traffic-validation

If access-flow traffic-validation is enabled for the service and the subscriber then the flows are checked against the filter rules. If the packets does not match the filter rules, and N violations occur in K seconds, the rp connection is downgraded to best-effort flow, if it is not already a best-effort flow.

Product
PDSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PDSN Service Configuration
configure > context context_name > pdn-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pdsn-service)#

Syntax

access-flow traffic-validation [ threshold { interval seconds | violations limit } ]

no access-flow traffic-validation

default access-flow traffic-validation [ threshold { interval | violations } ]

---

no

Disable traffic validation for the service.

---

default

Traffic validation configuration for the service is set to the default value.

---

threshold { [ violations limit ] [ interval seconds ] }

violations limit: Sets the parameters that determine traffic access violations. This is determined by setting the maximum number of violations within a set time period. must be an integer from 1 through 100000.

interval seconds Sets the time interval, in seconds. must be an integer from 1 through 100000.

---

Usage

Use this command to enable traffic validation for the current PDSN service.

Example

The following command enables traffic validation for the current PDSN service and sets the limit allowed to 100 violations within 5 seconds:

access-flow traffic-validation threshold violations 100 interval 5
access-network

Configures access network parameters.

Product
PDSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PDSN Service Configuration

configure > context context_name > pdsn-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pdsn-service)#

Syntax

access-network { accounting identifier identifier_name | realm realm_name }
no access-network { accounting identifier | realm } }

no
Disables the access-network.

accounting identifier
Configures accounting for the access-network. This value must be a string from 1 to 128 characters in length.

realm realm_name
Configures the realm for the access-network. realm_name must be a string from 1 to 128 characters in length.

Usage
Use this command to configure access-network parameters for accounting and realms.

Example
The following command creates an access-network realm named realm2.

access-network realm realm2
airlink bad-sequence-number

Configures PDSN behavior for airlink related parameters.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PDSN Service Configuration

```
configure > context context_name > psdn-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-psdn-service) #
```

```
airlink bad-sequence-number { accept | deny [use-deny-code { poorly-formed-request | unsupported-vendor-id}]

[ no | default ] airlinkbad-sequence-number
```

**no**
Disables the deny of bad-sequence number and accept it.

---

**default**

It is the default behavior.

---

**accept**

Accepts the A11 RRQ messages that have an Airlink Sequence number less than or equal to a previously received sequence number.

It is the default behavior.

---

**deny**

Rejects the A11 RRQ messages that have an Airlink Sequence number less than or equal to a previously received sequence number.

It uses `poorly-formed-request` option by default to deny a request.

---

**use-deny-code { poorly-formed-request | unsupported-vendor-id }**

These are optional keywords that used with `deny` sub-command to deny the A11 RRQ messages that have either an unsupported vendor Id or A11 Requests with bad/poor formation.

**unsupported-vendor-id** denies request on the basis of vendor Id.

**poorly-formed-request** will deny the A11 request on the basis of request formation or structure. It is the default deny code for `deny` sub-command.

---

**Usage**

This command is used to configure the airlink parameters for A11 RRQs.

When configured it denies the A11 RRQ messages that have an Airlink Sequence number less than or equal to a previously received sequence number.
Example

The following command would configure the system to deny all A11 RRQ messages having unsupported vendor Id or bad structure of message, including those having arilink sequence number less than or equal to a previously received sequence number:

```
airlinkbad-sequence-number deny
```
allow alt-ppp

Allows proprietary modified versions of PPP type sessions to connect this PDSN service.

Product
PDSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PDSN Service Configuration

configure > context context_name > pdsn-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pdsn-service)#

Syntax

allowalt-ppp

no allow alt-ppp

default allow alt-ppp

Disables the allowed alternate PPP feature.

Sets the specified parameter to default.

Usage

This command is used to deviate from standard PPP protocol and use a proprietary modified version of PPP with a pre-defined non-negotiable PPP parameters.

It is a vendor-specific licensed feature command.

Example

allow alt-ppp
always-on-indication

Enables/disables the inclusion of 3GPP2 Always On Indicators in messages to the PCF.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PDSN Service Configuration
configure > context context_name > pdsn-service service_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pdsn-service)#
```

**Syntax**

```
always-on-indication

no always-on-indication
```

**Usage**

This command is available when the 3GPP2 Always-On RP Extensions feature-use license is installed. When enabled, this command causes the PDSN service to include the Always On Indicators in the Normal Vendor Specific Extension (NVSE) part of an A11 Session Update message to the PCF. The indicator will only be sent for those subscriber sessions in which Always On functionality is enabled as determined after a successful authentication: the 3GPP2-Always-On attribute is set to a value of 1 (Active) for subscribers configured on a AAA server, or the always-on parameter is set for locally configured subscribers. This functionality is enabled by default.

**Example**

use the following command to Enables the inclusion of 3GPP2 Always On Indicators in messages to the PCF.

```
always-on-indication
```
associate

Associates a PDSN-service with a Quality of Service (QoS) policy.

Product
PDSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PDSN Service Configuration

configure > context context_name > pdsn-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pdsn-service)#

Syntax

associate qci-qos-mapping string

no associate qci-qos-mapping

no
Disables the configuration to associate PDSN-service with qos policy.

qci-qos-mapping string

qci-qos-mapping configures QCI to QoS mapping for this PDSN service.

string a string of size 1 to 63.

Usage

The following is used for configuration to associate PDSN-service with qos policy.

Example

associate qci-qos-mapping sample
**authentication**

Configures authentication parameters for specific PDSN service.

**Product**

PDSN

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

```plaintext
configure > context context_name > pdsn-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pdsn-service)#
```

**Syntax**

```plaintext
authentication { [ allow-noauth ] [ chap chap_priority ] [ mschap mschap_priority ] [ pap pap_priority ] } | [ msid-auth ]
```

**default authentication**

**allow-noauth**

*Default: Disabled*

This option configures the system to provide subscribers with network access even though they have not been authenticated. This command issued by itself would cause the system to not attempt to authenticate subscribers.

When the allow-noauth option is used in conjunction with commands specifying other authentication protocols and priorities to use, then if attempts to use those protocols fail, the system will treat the allow-noauth option as the lowest priority.

If no authentication is allowed, then NAI construct will be implemented in order to provide accounting records for the subscriber.

**chap chap_priority**

*Default: 1*

This option configures the system to attempt to use the Challenge Handshake Authentication Protocol (CHAP) to authenticate the subscriber.

A `chap_priority` must be specified in conjunction with this option. Priorities specify which authentication protocol should be attempted first, second, third and so on.

`chap_priority` must be an integer from 1 through 1000. The lower the integer, the higher the preference.

CHAP is enabled by default as the highest preference.

**mschap mschap_priority**

*Default: Disabled*
This option configures the system to attempt to use the Microsoft Challenge Handshake Authentication Protocol (MSCHAP) to authenticate the subscriber.
A `mschap_priority` must be specified in conjunction with this option. Priorities specify which authentication protocol should be attempted first, second, third and so on.
`mschap_priority` must be an integer from 1 through 1000. The lower the integer, the higher the preference.

```
mschap_priority
```

**Default:** 1

This option configures the system to attempt to use the Password Authentication Protocol (PAP) to authenticate the subscriber.
A `pap_priority` must be specified in conjunction with this option. Priorities specify which authentication protocol should be attempted first, second, third and so on.
`pap_priority` must be an integer from 1 through 1000. The lower the integer, the higher the preference. PAP is enabled by default as the second highest preference.

```
pap  pap_priority
```

**Default:** 2

This option configures the system to attempt to authenticate the subscriber based on their Mobile Station Identity (MSID).

```
msid-auth
```

**Default:** Disabled

Use to specify how the PDSN service should handle authentication and what protocols to use. The flexibility is given to configure this option to accommodate the fact that not every mobile will implement the same authentication protocols.
The chassis is shipped from the factory with the authentication options set as follows:
- allow-noauth disabled
- chap enabled with a priority of 1
- mschap disabled
- msid-auth disabled
- pap enabled with a priority of 2

**Important:** At least one of the keywords must be used to complete the command.

**Example**

The following command would configure the system to allow no authentication for subscribers and would perform accounting using the default NAI-construct of `username@domain`:

```
authentication allow-noauth
```

The following command would configure the system to attempt subscriber authentication first using CHAP, then MSCHAP, and finally PAP. If the allow-noauth command was also issued, if all attempts to authenticate the subscriber using these protocols fail, then the subscriber would be allowed access:

```
authentication chap 1 mschap 2 pap 3
```
**bcmcs**

Sets the BCMCS (Broadcast Multicast Service) group username and password for RADIUS access.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PDSN Service Configuration

```
configure > context context_name > pdsn-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pdsn-service)#
```

**Syntax**

```
bcmcs { customptt | encrypted grppasswd group_passwd | flow-id value [flow-id-type { flow-id | program-id }] | grppasswd group_password | grpusrname group_name | ptt { destination-context dest_name | disconnect-dscp-label dscp_label | mtu transmission_unit | rohc-profile-name rohc_profile_name } }

default bcmcs [ custom ptt | ptt { disconnect-dscp-label | mtu | rohc-profile-name } ]

no bcmcs { custom ptt | flow-id value [flow-id-type { flow-id | program-id }] | grppasswd | grpusrname | ptt { destination-context | disconnect-dscp-label | mtu | rohc-profile-name } }
```

---

**custom**

Customise the BCMCS configuration.

---

**flow-id value**

Set the BCMCS flow-id. This value must be a hex string between 0x1000 and 0xFFFFFFFF. Making this entry opens a new mode: bcmcs-flow-id.

**rohc-profile name**

Configure ROHC parameters name, name should be string of size 1 to 63.

---

**grpusrname group_name**

Sets the BCMCS group name for RADIUS access requests. This value must be a string from 1 to 127 characters in length.

---

**encrypted grppasswd group_passwd**

Set the BCMCS group password for RADIUS access requests. This value must be a string from 1 to 63 characters in length.

Password can be encrypted or clear.
ptt {destination-context dest_name | disconnect-dscp-label dscp_label | mtu transmission_unit | rohc-profile-name rohc_profile_name }

destination-context: Specify the intended destination context name. This value must be string of 1 to 79 characters in length.
disconnect-dscp-label: Configures the DSCP label to be present in the In Call Signalling packet based on which In Call Signalling and Media Flows will be disconnected. This value must be a Hexadecimal number between 0x0 and 0xFF.
mtu transmission_unit: Configures maximum transmission unit. This value must be ranging from 100 to 2000. Default is 1500.
rohc_profile_name rohc_profile_name: Profile name of the ROHC compressor and decompressor. This value should be a string of 1 to 63.

Usage
Use this command to set the BCMCS group username and password for RADIUS access requests.

Example

```bash
bcmcsgrpusername group_name bcmcsgrppasswd group_password
```
bind

Binds the PDSN service to a logical IP interface serving as the R-P interface. Specifies the maximum number of subscribers that can access this service over the interface.

**Product**

PDSN

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

configure > context context_name > pdsn-service service_name

Entering the above command sequence results in the following prompt:

[context_name] host_name(config-pdsn-service)#

**Syntax**

bind address [ max-subscribers count ]

no bind address

no

Removes a previously configured binding.

address

Specifies the IP address (address) of the interface configured as the R-P interface. address is specified in dotted decimal notation.

max-subscribers count

**Default:** 500000

Specifies the maximum number of subscribers that can access this service on this interface.

count can be configured to any integer value between 0 and 2500000.

**Important:** The maximum number of subscribers supported is dependent on the license key and the number of active PACs/PSCs installed in the system. A fully loaded system with 13 active PACs/PSCs can support 2500000 total subscribers. Refer to the license key command for additional information.

**Usage**

Associate or tie the PDSN service to a specific logical IP address. The logical IP address or interface takes on the characteristics of an R-P interface. Only one interface can be bound to a service. The interface should be configured prior to issuing this command.

This command also sets a limit as to the number of simultaneous subscribers sessions that can be facilitated by the service/interface at any given time.

When configuring the max-subscribers option, be sure to consider the following:

- The total number of interfaces that you will configure for use as R-P interfaces
• The maximum number of subscriber sessions that all of the interfaces may handle during peak busy hours
• The average bandwidth for each of the sessions
• The type of physical port (10/100Base-Tx or 1000Base-T) to which these interfaces will be bound

Taking these factors into account and distributing your subscriber session across all available interfaces will allow you to configure your interfaces to optimally handle sessions without degraded performance.

Example

The following command would bind the logical IP interface with the address of 192.168.3.1 to the PDSN service and specifies that a maximum of 600 simultaneous subscriber sessions can be facilitated by the interface/service at any given time.

bind address 192.168.3.1 max-subscribers 600

The following command disables a binding that was previously configured:

nobind address
data-available-indicator

Enables sending Data Available Indicator extension in R-P Registration Reply.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PDSN Service Configuration

```
configure > context context_name > psdn-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-psdn-service)#
```

**Syntax**

```
[ no | default ] data-available-indicator
```

- **no**
  - Default: Disabled
  - Disable the sending of the Data Available Indicator extension in R-P Registration Reply.

- **default**
  - Sets / Restores default value assigned for specified parameter for `data-available-indicator`.

**Usage**

Use this command to enable or disable the sending of the Data Available Indicator extension in R-P Registration Reply.

**Example**

Use the following command to enable sending the Data Available Indicator extension in R-P Registration Reply:

```
data-available-indicator
```

Use the following command to disable sending the Data Available Indicator extension in R-P Registration Reply:

```
no data-available-indicator
```
data-over-signaling

Enables the data-over-signaling marking feature for A10 packets.

Product
PDSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PDSN Service Configuration
configure > context context_name > pdsn-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pdsn-service)#

Syntax

[ no | default ] data-over signaling

default
Sets / Restores default value assigned for specified parameter for data-over signaling

no
Default: Enabled
Disable the data-over signaling feature for A10 packets.

Usage

Use this command to enable or disable the data-over signaling feature for A10 packets.

Important: This is a customer-specific command.

Example

no data-over-signaling
default subscriber

Specifies the name of a subscriber profile configured within the same context as the PDSN service from which to base the handling of all other subscriber sessions handled by the PDSN service.

Product
PDSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PDSN Service Configuration

`configure > context context_name > pdsn-service service_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pdsn-service)#
```

Syntax

```
defaultsubscriber profile_name

no default subscriber
```

no

Enables/Disables the option `default subscriber profile_name`

profile_name

Specifies the name of the configured subscriber profile. `profile_name` can be between 1 and 127 alpha and/or number characters and is case sensitive.

Usage

Each subscriber profile specifies “rules” such as permissions, PPP settings, and timeout values. By default, the PDSN service will use the information configured for the subscriber named default within the same context. This command allows for multiple PDSN services within the same context to apply different “rules” to sessions they process. Each set of rules can be configured under a different subscriber name which is pointed to by this command.

Use the `no default subscriber profile_name` command to delete the configured default subscriber.

Example

To configure the PDSN service to apply the rules configured for a subscriber named `user1` to every other subscriber session it processes, enter the following command:

```
default subscriber user1```
direct-lte-indicator

Enables sending Direct LTE Indicator VSA in Access Request.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PDSN Service Configuration

configure > context context_name > pdsn-service service_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pdsn-service)#
```

**Syntax**

```
[ no | default ] direct-lte-indicator
```

- **default**
  
  Sets / Restores default value assigned for specified parameter for *data-over signaling*

- **no**
  
  Default: Enabled
  
  Disables sending Direct LTE Indicator VSA in Access Request.

**Usage**

Use this command to enable or disable sending Direct LTE Indicator VSA in Access Request.

**Important:** This is a customer-specific command.

**Example**

```
nodirect-lte-indicator
```
dormant-transition

Configures the PDSN behavior to terminate A10 session, when the PDSN receives the A11-RRQ (Type 4) before the session for the original MN is established completely.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PDSN Service Configuration

`configure > context context_name > pdsn-service service_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pdsn-service)#
```

**Syntax**

```
[ no | default ] dormant-transition initial-session-setup
```

- **no**
  Terminates the A10 session, when PDSN receives the A11-RRQ (Type 4) before the original session established completely.

- **default**
  Keeps the A10 session live in case of A11-RRQ (Type 4) is received before the original session is established completely.

**Usage**

When the status of A10 session goes to dormant before the session for the original MN is established completely, the different MN may possibly send the A11-RRQ (Type 4) to the PDSN and PPP renegotiation may start.

This command is used to terminate the A10 session when the PDSN receives the A11-RRQ (Type 4) before the session for original MN is established completely.

**Example**

Following command is used to release the A10 session in case of receiving A11-RRQ (Type 4) before the original session is established completely:

```
no dormant-transition initial-session-setup
```
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**
Use this command to return to the Exec mode.
enhanced-pcf-redirection

Enables or disables PDSN support for enhanced PCF redirection.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PDSN Service Configuration

```
configure > context context_name > pdsn-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pdsn-service)#
```

**Syntax**

```
[no] enhanced-pcf-redirection
```

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Disables PDSN support for enhanced PCF redirection.</td>
</tr>
<tr>
<td>enhanced-pcf-redirection</td>
<td>Enables PDSN support for enhanced PCF redirection.</td>
</tr>
</tbody>
</table>

**Usage**

Use this command to enable or disable PDSN support for enhanced PCF redirection. By default, this feature is disabled.

**Important:** This is a customer-specific command.

**Example**

The following command will disable PDSN support for enhanced PCF redirection.

```
no enhanced-pcf-redirection
```
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Use this command to return to the parent configuration mode.
**fragment**

Enables or disables PPP payload fragmentation.

**Product**

PDSN

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

`configure > context context_name > pdsn-service service_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pdsn-service)#
```

**Syntax**

```
[ no | default ] fragment ppp-data
```

- **no**
  
  Disables the fragmentation of ppp data.

- **default**
  
  Default enables ppp data fragmentation.

**Usage**

This command is to indicate to the RP module to NOT fragment PPP payloads being sent to the PCF, if the total packet size (PPP+GRE+IP) exceeds 1500 bytes. Disabling fragmentation may cause the `sessmgr` to perform outer IP fragmentation of the outgoing packet, if the resulting packet exceeds the MED MTU.

**Example**

The following command enables PPP payload fragmentation.

```
fragment ppp-data
```
**gre**

Configures Generic Routing Encapsulation (GRE) parameters for the A10 protocol within the PDSN service.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PDSN Service Configuration

```bash
configure > context context_name > pdsn-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pdsn-service)#
```

**Syntax**

```bash
gre { checksum | checksum-verify | ip-header-dscp value { all-control-packets | setup-packets-only } | protocol-type {any | byte-stream | ppp } | reorder-timeout value | segmentation | sequence-mode { none | reorder } | sequence-numbers | threegppp2-ext-header qos-marking }

no gre { checksum | checksum-verify | ip-header-dscp | segmentation | sequence-numbers | threegppp2-ext-headers qos-marking }

default gre { checksum | checksum-verify | ip-header-dscp | segmentation | sequence-numbers | threegppp2-ext-headers qos-marking }

no gre { checksum | checksum-verify | ip-header-dscp | segmentation | sequence-numbers | threegppp2-ext-headers qos-marking }

default gre { checksum | checksum-verify | ip-header-dscp | segmentation | sequence-numbers | threegppp2-ext-headers qos-marking }
```

---

**no**

Disables the specified functionality.

---

**default**

Restores the specified parameter to its default setting.

---

**checksum**

Default: disabled

Enables the introduction of the checksum field in outgoing GRE packets.

---

**checksum-verify**

Default: disabled

Enables verification of the GRE checksum (if present) in incoming GRE packets.

---

**ip-header-dscp value { all-control-packets | setup-packets-only }**

Default: Disabled

Used to configure the QoS Differentiated Services Code Point (DSCP) marking for GRE packets.
value: Represents the DSCP setting. It represents the first six most-significant bits of the ToS field. It can be configured to any hex value from 0x0 through 0x3F.

all-control-packets: Dictates that the DSCP marking is to be provided in all GRE control packets.

setup-packets-only: Dictates that the DSCP marking is to be provided only in GRE setup packets.

\[ \text{protocol-type} \{ \text{any} | \text{byte-stream} | \text{ppp} \} \]

Specifies the protocol used for GRE encapsulation that is acceptable to:
any: Specifies that the PDSN service will accept GRE packets encapsulated using any protocol.
byte-stream: Specifies that the PDSN service will accept GRE packets only encapsulated using byte stream. Using byte stream encapsulation, PPP packets are framed at different intervals and sent.
ppp: Specifies that the PDSN service will accept GRE packets only encapsulated using the Point-to-Point Protocol (PPP). Using PPP encapsulation, PPP packets are framed at regular intervals and sent.

reorder-timeout

Default: 100

Configures max number of milliseconds to wait before processing reordered out-of-sequence GRE packets. milliseconds must be an integer from 0 through 5000.

segmentation

Default: disabled

Enables GRE Segmentation for the PDSN service.

sequence-mode \{ none | reorder \}

Default: none

Configures handling of incoming out-of-sequence GRE packets.
none: Specifies that sequence numbers in packets are ignored and all arriving packets are processed in the order they arrive.
reorder: Specifies that out of sequence packets are stored in a sequencing queue until one of the conditions is met:
- The reorder timeout occurs: All queued packets are sent for processing and the accepted sequence number is updated to the highest number in the queue.
- The queue is full (five packets): All packets in the queue are sent for processing, the reorder timer is stopped and the accepted sequence number is updated to the highest number in the queue.
- An arriving packet has a sequence number such that the difference between this and the packet at the head of the queue is greater than five. All the packets in the queue are sent for processing, the reorder timer is stopped and the accepted sequence number is updated to the highest number that arrived.
- A packet arrives that fills a gap in the sequenced numbers stored in the queue and creates a subset of packets whose sequence numbers are continuous with the current accepted sequence number. This subset of packets in the queue is sent for processing. The reorder timer continues to run and the accepted sequence number is updated to the highest number in the subset delivered.

sequence-numbers

Enables insertion of GRE sequence numbers in data that is about to be transmitted over the A10 interface. Data coming into the system containing sequence numbers but that is out of sequence is not re-sequenced.
threegpp2-ext-headers qos-marking

When threegpp2-ext-headers qos-marking is enabled and the PCF negotiates capability in the A11 RRQ, the PDSN will include the qos optional data attribute in the GRE 3gpp2 extension header.

The no keyword, enables qos-marking in the gre header based on the tos value in the header.

Usage

The gre protocol-type command can be used to prevent the PDSN service from servicing PCFs that use a specific form of encapsulation.

Use the no gre sequence-numbers command to disable the inclusion of GRE sequence numbers in the A10 data path.

The chassis is shipped from the factory with the authentication options set as follows:

- protocol-type any
- sequence-numbers enabled

Example

Use this command to configure the PDSN service to exclude byte stream encapsulated GRE traffic:

    gre protocol-type ppp
**inter-pdsn-handoff mobility-event-indicator**

Configures the PDSN to support the Mobility Event Identifier (MEI) during inter-PDSN handoffs. The presence of the Mobility Event Indicator (MEI) and Access Network Identifier (ANID) elements in a A11 handoff request represents an Inter-PDSN handoff.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PDSN Service Configuration

`configure > context context_name > pdsn-service service_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pdsn-service)#!
```

**Syntax**

```
inter-pdsn-handoff mobility-event-indicator

no inter-pdsn-handoff mobility-event-indicator

default inter-pdsn-handoff mobility-event-indicator
```

---

**no**

Disables support for the MEI during inter-PDSN handoffs.

---

**default**

Sets / Restores default value assigned for `inter-pdsn-handoff mobility-event-indicator`. By default it is disabled.

---

**Usage**

Use this command to configure support for the MEI during inter-PDSN handoffs.

**Example**

Use the following command to enable support for the MEI during inter-PDSN handoffs

```
inter-pdsn-handoff mobility-event-indicator
```
inter-pdsn-handover

Configures Inter-PDSN handoff related parameters.

Product
PDSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PDSN Service Configuration

configure > context context_name > pdsn-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pdsn-service)#

Syntax

inter-pdsn-handover use-canid-panid

no inter-pdsn-handover use-canid-panid

default inter-pdsn-handover use-canid-panid

Usage
Disables support for the MEI during inter-PDSN handoffs parameters.

default
Sets / Restores default value assigned for inter-pdsn-handoff mobility-event-indicator. By default it is disabled.

Example
Use this command to configure Inter-PDSN handoff related parameters.

Use the following command to configure Inter-PDSN handoff related parameters.

    inter-pdsn-handover use-canid-panid
ip header-compression rohc

Enters PDSN Service ROHC Configuration Mode and allows you to configure ROHC parameters that the PDSN conveys to the PCF in the initial A11 RRP message before PPP authentication.

By default, ROHC is disabled for a PDSN service.

Product
PDSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PDSN Service Configuration
configure > context context_name > pdsn-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pdsn-service)#

Syntax

ipheader-compression rohc
default ipheader-compression rohc
no ipheader-compression rohc

Usage
Use this command to enter the PDSN Service ROHC Configuration Mode or disable ROHC for the current PDSN service.

Example
The following command disables ROHC for the current PDSN service and sets all of the values for commands in PDSN Service ROHC Configuration Mode back to their default settings:

no ip header-compression rohc
**ip local-port**

Configures the local User Datagram Protocol (UDP) port for the R-P interfaces’ IP socket.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PDSN Service Configuration
configure > context context_name > pdsn-service service_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pdsn-service)#
```

**Syntax**

```
ip local-port number
```

```
default ip local-port
```

```
  number
  Default: 699
  Specifies the UDP port number.
  number can be any integer value between 1 and 65535.
```

```
default
  Designates UDP port, default value as 699.
```

**Usage**

Specify the UDP port that should be used for communications between the Packet Control Function (PCF) and the PDSN.

**Important:** The UDP port setting on the PCF must match the local-port setting for the PDSN service on the system in order for the two devices to communicate.

**Example**

Use the following command to specify a UDP port of 3950 for the PDSN service to use to communicate with the PCF on the R-P interface:

```
iplocal-port 3950
```
**ip source-violation**

Sets the parameters for IP source validation. Source validation is useful if packet spoofing is suspected or for verifying packet routing and labeling within the network.

Source validation requires the source address of received packets to match the IP address assigned to the subscriber (either statically or dynamically) during the session.

**Product**

PDSN
PDIF

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

configure > context context_name > pdsn-service service_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pdsn-service)#
```

**Syntax**

```
ip source-violation { clear-on-valid-packet | drop-limit num | period secs | reneg-limit num }

no ip source-violation clear-on-valid-packet

defaultip source-violation { drop-limit | period | reneg-limit }
```

**Syntax Description**

- **no**
  
  Enables/Disables `ip source-violation clear-on-valid-packet`.

- **default**
  
  Configure default settings related to `ip source-violation`.

- **clear-on-valid-packet**
  
  Default: disabled
  
  Configures the service to reset the reneg-limit and drop-limit counters after receipt of a properly addressed packet.

- **drop-limit num**
  
  Default: 10
  
  Sets the number of allowed source violations within a detection period before forcing a call disconnect. If `num` is not specified, the value is set to the default. `num` can be any integer value from 1 to 1000000.

- **period secs**
  
  Default: 120
The length of time, in seconds, for a source violation detection period to last. drop-limit and reneg-limit counters are decremented each time this value is reached.

The counters are decremented in this manner: reneg-limit counter is reduced by one (1) each time the period value is reached until the counter is zero (0); drop-limit counter is halved each time the period value is reached until the counter is zero (0). If \( secs \) is not specified, the value is set to the default. 

\( secs \) can be any integer value from \( 1 \) to \( 1000000 \).

**reneg-limit num**

Default: \( 5 \)

Sets the number of allowed source violations within a detection period before forcing a PPP renegotiation. If \( num \) is not specified, the value is set to the default.

\( num \) can be any integer value from \( 1 \) to \( 1000000 \).

**Usage**

This function is intended to allow the operator to configure a network to prevent problems such as when a user gets handed back and forth between two PDISFs/PDSNs a number of times during a handoff scenario.

This function operates in the following manner:

When a subscriber packet is received with a source address violation, the system increments both the IP source-violation reneg-limit and drop-limit counters and starts the timer for the IP source-violation period.

Every subsequent packet received with a bad source address during the IP source-violation period causes the reneg-limit and drop-limit counters to increment.

For example, if reneg-limit is set to 5, then the system allows 5 packets with a bad source address (source violations), but on the 5th packet, it renegotiates PPP.

If the drop-limit is set to 10, the above process of receiving 5 source violations and renegotiating PPP occurs only once. After the second 5 source violations, the call is dropped. The period timer continues to count throughout this process.

If the configured source-violation period is exceeded at any time before the call is dropped, the reneg-limit counter is checked. If the reneg-limit counter equals zero, the drop-limit counter is decremented by half.

**Example**

The following command sets the drop limit to 15 and leaves the other values at their defaults:

```
ip source-violation drop-limit 15
```
### lifetime

Specifies the time that an A10 connection can exist before its registration is considered expired.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PDSN Service Configuration

```
configure > context context_name > pdsn-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pdsn-service)#
```

#### Syntax

```
lifetime time

no lifetime

default lifetime
```

- **no lifetime**
  Specifies that an A10 connection can exist for an infinite amount of time.

- **default lifetime**
  Sets / Restores default value assigned for `lifetime` as 1800.

- **time**
  Default: 1800
  Specifies the time that an A10 connection can exist before its registration is considered expired.
  `time` is measured in seconds and can be configured to any integer value between 1 and 65534.

#### Usage

Set a limit to the amount of time that a subscriber session can remain up whether or not the session is active or dormant. If the lifetime timer expires before the subscriber terminates the session, their connection will be terminated automatically.

Use the `no lifetime` command to delete a previously configured lifetime setting. If after deleting the lifetime setting you desire to return the lifetime parameter to its default setting, use the `default lifetime` command.

#### Example

The following command specifies a time of 3600 seconds (1 hour) for subscriber sessions on this PDSN service:

```
lifetime 3600
```
max-retransmissions

Configures the maximum number of times the PDSN service will attempt to communicate with a PCF before it marks it as unreachable.

Product
PDSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PDSN Service Configuration

configure > context context_name > pdsn-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pdsn-service)#

Syntax

max-retransmissions count

default max-retransmissions

default

Sets / Restores default value assigned for max-retransmissions as 5.

count

Specifies the maximum number of times the PDSN service will attempt to communicate with a PCF before it marks it as unreachable.

count can be configured to any integer value between 1 and 1,000,000.

Usage

If the value configured for the max-retransmissions is reached the call will be dropped.

The chassis is shipped from the factory with the Internet maximum number of retransmissions set to 5.

Example

The following command configures the maximum number of retransmissions for the PDSN service to 3:

max-retransmissions 3
mobile-ip foreign-agent context

For Mobile IP support, specifies the context in which the FA service(s) are configured.

**Product**

PDSN

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

`configure > context context_name > pdsn-service service_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pdsn-service)#
```

**Syntax**

```
mobile-ip foreign-agent context context_name [ fa-service name ]
```

```
no mobile-ip foreign-agent context
```

<table>
<thead>
<tr>
<th>no</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enables/Disables mobile-ip foreign-agent context</td>
</tr>
</tbody>
</table>

```
context_name
```

Specifies the name of the previously configured context that facilitates the FA service(s). context_name must be between 1 and 79 alpha or numeric characters and is case sensitive.

```
[ fa-service name ]
```

This optional keyword allows you to link the PDSN service to a particular FA service in the specified context. name is the name of the FA service to link to. name is a string of size 1 to 63

**Usage**

FA services on the system can be configured either in the same or different contexts from those facilitating PDSN services. When they are configured in separate contexts, this command configured with a PDSN service instructs the PDSN service to route traffic to the context facilitating the FA service.

Use the `no mobile-ip foreign-agent context` to delete a previously configured destination context.

**Example**

The following command instructs the PDSN service to use the context named FA-destination for FA functionality:

```
mobile-ip foreign-agent context fa-destination
```
mobile-ipv6

Configures Mobile IPv6 parameters within specific PDSN service.

Product
PDSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PDSN Service Configuration
configure > context context_name > psdn-service service_name

Entering the above command sequence results in the following prompt:
[context_name]host_name(config-psdn-service)#

Syntax

mobile-ipv6 mobile-access-gateway context context_name [ mag-service name ]

mobile-access-gateway

Configures Mobile Access Gateway (MAG) parameters within specific PDSN service.

class context context_name

Designates name of the context in which the MAG service is configured. Must be followed by context name of MAG service.
context_name is a string of size 1 to 79.

mag-service name

Designates name of the MAG service in that context. Must be followed by MAG service name.
name is a string of size 1 to 63.

Usage
This command is used to configure Mobile IPv6 parameters and Mobile Access Gateway (MAG) parameters within specific PDSN service.

Example
The following command configures Mobile IPv6 parameters and Mobile Access Gateway (MAG) parameters within specific PDSN service.

mobile-ipv6 mobile-access-gateway context psdn1 mag-service serv1
**msid length**

Configures checking the length of the A11 MSID in A11 Session Specific Extn and airlink records.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PDSN Service Configuration

```
configure > context context_name > pdsn-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pdsn-service)#
```

**Syntax**

```
msid length { [ min min_length ] | max max_length }
```

**default msid length**

```
default
```

Specifies the default length of MSID (10 to 15) as per standard. By default `msid` is disabled.

```
min min_length
```

Specifies the minimum length for MSID.

`min_length` is any Integer value between 10 to 15, but should be less than `max_length` specified with `max`. Default is 10.

```
max max_length
```

Specifies the maximum length for MSID.

`max_length` is any Integer value between 10 to 15, but should be more than `min_length` specified with `min`. Default is 15.

**Usage**

MSID length can be configured either in the standard length or different customized length form. This command is used to specify the allowed length of MSID.

**Example**

The following command specifies an MSID length between 12 and 15:

```
msid length min 12 max 15
```
nai-construction

Specifies a domain alias that will be used to represent the context which the PDSN service should use for AAA functionality.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PDSN Service Configuration

```
configure > context context_name > pdsn-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pdsn-service)#
```

**Syntax**

```
nai-construction domain alias

no nai-construction domain
```

```
domain alias
```

`alias` represents the “domain” name that you would like to associate with the context in which AAA functionality is configured. `alias` can be between 1 and 79 alpha and/or numeric characters and is case-sensitive.

**Usage**

Enabling NAI will be constructed for the subscriber in the event that their mobile station (MS) does not negotiate CHAP, PAP, or MSCHAP. If this option is selected, no further attempts will be made to authenticate the user. Instead, the constructed NAI will be used for accounting purposes.

The context specified by this command would be used to provide the communication with the RADIUS accounting server.

Use the `no nai-construction domain` command to deleted a configured alias.

**Important:** This command should only be used if the PDSN service is configured to allow no authentication using the authentication allow-noauth command.

Additionally, the `aaa constructed-nai` command in the Context Configuration mode can be used to configure a password for constructed NAIs.

**Example**

The following command configured a domain alias of `aaa_context` for the PDSN service to use when an NAI is constructed for a subscriber session:

```
nai-construction domain aaa_context
```
new-call conflict

Enable or disable to send A11-RUPD to current PCF, when system receives the A11-RRQ(Type1) from new PCF during the session exists.

Product
PDSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PDSN Service Configuration

    configure > context context_name > pdsn-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pdsn-service)#

Syntax

[ no | default ] new-call conflict terminate-session-old-pcf

no
Disable to send A11-RUPD to current PCF, when system receives the A11-RRQ(Type1) from new PCF during the session exists.

default
Enable to send A11-RUPD to current PCF, when system receives the A11-RRQ(Type1) from new PCF during the session exists.

Usage
This configuration supports to enable or disable to send A11-RUPD to current PCF, when the system receives the A11-RRQ(Type1) from new PCF during the session exists.

If the configuration is **no new-call conflict terminate-session-old-pcf** system will not send registration update to old PCF on receiving a new call (A11-RRQ(Type1)) request for an existing active/dormant session. The default behavior is to send registration updates.

Example
The following command configured a system to send a registration update on receiving an A11-RRQ (Type 1) request for an existing active/dormant session:

    new-call conflict terminate-session-old-pcf
**pcf-monitor**

Enables the monitoring of all the PCFs that have sessions associated with it. The PDSN stops monitoring a PCF if it is determined to be down. Once a PCF is determined to be down, the PDSN tears down all sessions that correspond to the PCF and generates AAA Accounting Stop messages. All the PCFs that are connected to the PDSN service are monitored.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PDSN Service Configuration

configure > context context_name > pdsn-service service_name

Entering the above command sequence results in the following prompt:

```plaintext
[context_name]host_name(config-pdsn-service)#
```

**Syntax**

```plaintext
cpf-monitor [ interval seconds | max-inactivity-time seconds | num-retry num | timeout seconds ]

[ no | default ] pcf-monitor
```

---

**pcf-monitor**

Entering the command with no keywords enables the PCF monitoring function with all parameters set to the defaults.

---

**no**

Disables the pcf monitoring function.

---

**default**

Sets / Restores default value assigned for pcf-monitor.

---

**interval seconds**

Default: 60 seconds
Sets the amount of time to wait between ping request messages.
seconds must be an integer in the range from 1 through 3600.

---

**max-inactivity-time seconds**

Default: 120 seconds
The maximum amount of time (seconds) with no A10 traffic from a PCF before the ICMP-ping mechanism is triggered.
seconds must be an integer from 1 through 3600.
num-retry num

Default: 5
Sets the number of times that the PDSN retries to ping the PCF. When num-retry for a given PCF has been exhausted with no response, sessions that correspond to the non-responsive PCF are terminated and Accounting Stop records for each terminated session are generated. num must be an integer in the range from 0 through 100.

timeout seconds

Default: 3 seconds
The amount of time to wait for a response before retrying. seconds must be in the range from 1 through 10.

Usage
Use this command to enable the PDSN service to monitor the PCFs that have sessions associated with the PDSN service.

Example
The following command enables PCF monitoring with parameters set to the defaults:

    pcf-monitor

The following command enables PCF monitoring and sets the timeout to 10 seconds:

    pcf-monitor timeout 10

The following command disables pcf-monitoring:

    no pcf-monitor
pcf-session-id-change restart-ppp

Manages current session and PPP renegotiation on GRE-key change without any change in PCF/PANID/CANID. This command disables or enables the PPP renegotiation restart on receiving an RP registration request from the current PCF with GRE key (PCF session Id) change. With this command the PDSN aborts and restarts the call causing PPP renegotiation.

This is enabled by default.

**Product**

PDSN

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > PDSN Service Configuration

`configure > context context_name > pdsn-service service_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pdsn-service)#
```

**Syntax**

```
[ no | default ] pcf-session-id-change restart-ppp
```

<table>
<thead>
<tr>
<th>no</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disables the pcf-session-id-change restart-ppp function. With this option PDSN does not restart the PPP renegotiation on GRE key change from current PCF in an RP registration request, unless it indicates change in PCF/PANID/CANID.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set the pcf-session-id-change function to the default state on enabled.</td>
</tr>
</tbody>
</table>

**Usage**

GRE key (PCF session ID) is sued to identify the data packet for a session and is negotiated through the A11 signaling messages between PCF and PDSN. By default PDSN aborts and restart the PPP renegotiation on receipt of any RP registration request with change in GRE key or PCF session Id. With use of no pcf-session-id-change restart-ppp command PDSN is configured to disable the restart of call or PPP renegotiation on receipt of any RP registration request with changed GRE key, unless it has any PCF/ANID/CANID change. PDSN silently switches the GRE key for the session, retaining the existing PPP session.

**Example**

The following command disables the PPP renegotiation restart action on receipt of any RP RRQ with changed GRE key from same PCF/PANID/CANID.

```
no pcf-session-id-change restart-ppp
```
pdsn type0-tft attempt-inner-match

Configures a type0 traffic flow template (tft) to a type1 traffic flow template.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PDSN Service Configuration

```
configure > context context_name > pdsn-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pdsn-service)#
```

**Syntax**

```
[ no | default ] pdsn type0-tft attempt-inner-match
```

- **no**
  
  Disables *pdsn type0-tft attempt-inner-match*.

- **default**
  
  Sets / Restores default value assigned for *pdsn type0-tft attempt-inner-match*.

**Usage**

This CLI is used make PDSN match inner IP packets for an AIMS call. When enabled, the PDSN tries to match a type-0 tft to match both outer and inner packet, so that MN can use a Type-0 filter for HoA traffic which are tunneled.

This is disabled by default.

**Example**

The following command enables type0 tft:

```
pdsn type0-tft attempt-inner-match
```
peer-pcf

Configures settings for any PCF that has a connection with this PDSN.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PDSN Service Configuration

```
configure > context context_name > pdsn-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pdsn-service)#
```

**Syntax**

```
peer-pcf { ip_address | ip_address/mask } bcmcs-framing { hdlc-like | segment-based }
```

- `ip_address` must be specified using the standard IPv4 dotted decimal notation or colon notation for IPv6.
- `ip_address/mask` must be specified using the standard IPv4 dotted decimal notation or colon notation for IPv6, followed by the mask.

```
bcmcs-framing { hdlc-like | segment-based }
```

Specifies the type of bcmcs_framing to use for this PCF connection.

- `hdlc-like`: applies HDLC-like framing for all BCMCS flows
- `segment-based`: applies segment-based framing for all BCMCS flows

**Usage**
Use this command to configure the settings for any PCF that is connected to this PDSN. You can also specify bcmcs framing settings to use for the connection.

**Example**

The following command configures the peer-pcf for an IP address of 131.2.3.4:

```
peer-pcf 131.2.3.4
```
pma-capability-indicator

Enables sending PMIP Capability Indicator VSA in Access Request.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PDSN Service Configuration

```bash
configure > context context_name > pdsn-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pdsn-service)#
```

**Syntax**

```
pma-capability-indicator  [ 3gpp2 ]
[ no  |  default  ] pma-capability-indicator
```

---

3gpp2

Use 3GPP2 defined VSA. Default is to use Custom1 VSA.

---

no

Enables/Disables sending PMIP Capability Indicator VSA in Access Request.

---

default

Sets / Restores default value assigned for PMIP Capability Indicator.

---

**Usage**

Use this command to enable sending PMIP Capability Indicator VSA in Access Request.

**Example**

The following command enables sending PMIP Capability Indicator using 3GPP2 defined VSA in Access Request.

```
pma-capability-indicator 3gpp2
```
policy

Configures PDSN service policies.

Product
PDSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PDSN Service Configuration

configure > context context_name > pdsn-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pdsn-service)#

Syntax

policy msid-match msid_with_wildcards redirect address [ weight weight_num ] [ address2 [ weight weight_num ]... address16 [ weight weight_num ] ] [ weight weight_num ]

no policy msid-match msid_with_wildcards

policy overload { redirect address [ weight weight_num ] [ address2 [ weight weight_num ] ... address16 [ weight weight_num ] ] | reject [ use-reject-code { admin-prohibited | insufficient-resources } ] }

no policy overload [ redirect address [ address2 ... address16 ] ]

default policy overload

no policy pcf-zone-matchzone_number

[ default | no ] policy rrq mei-from-current-pcf suppress-ppp-restart

policy service-option enforce

[ default | no ] policy service-option

policy unknown-cvse enforce

[ default | no ] policy unknown-cvse

---

no

Enables/Disables the PDSN service policies.

---

default

Sets / Restores default value assigned for specified PDSN service policies.
policy msid-match msid_with_wildcards redirect address [ weight weight_num ] [ address2 [ weight weight_num ] ... address16 [ weight weight_num ] ] [ weight weight_num ]

Specifies how a PDSN service should handle an incoming call that matches a list of wildcard MSIDs.

- **msid_with_wildcards**: An MSID in which up to 16 digits have been replaced with the wildcard ‘$’. This defines the list of possible matches for incoming calls.
- **redirect**: This option enables a redirect policy for overloading conditions. When a redirect policy is invoked, the PDSN service rejects new sessions with an A11 Registration Reply Code of 88H (unknown PDSN address) and provides the IP address of an alternate PDSN. This command can be issued multiple times.
- **address**: The IP address of an alternate PDSN expressed in IP v4 dotted decimal notation. Up to 16 IP addresses can be specified either in one command or by issuing the redirect command multiple times. If you try to add more than 16 IP addresses to the redirect policy the CLI issues an error message. If you specify an IP address and weight that already exists in the redirect policy the new values override the existing values.
- **weight weight_num**: When multiple addresses are specified, they are selected in a weighted round-robin scheme. Entries with higher weights are more likely to be chosen. If a weight is not specified the entry is automatically assigned a weight of 1. weight_num must be an integer from 1 through 10.

policy overload { redirect address [ weight weight_num ] [ address2 [ weight weight_num ] ... address16 [ weight weight_num ] ] | reject [ use-reject-code { admin-prohibited | insufficient-resources } ] } }

Specifies how a PDSN service should handle an overload condition.

- **redirect**: This option enables a redirect policy for overloading conditions. When a redirect policy is invoked, the PDSN service rejects new sessions with an A11 Registration Reply Code of 88H (unknown PDSN address) and provides the IP address of an alternate PDSN. This command can be issued multiple times.
- **address**: The IP address of an alternate PDSN expressed in IP v4 dotted decimal notation. Up to 16 IP addresses can be specified either in one command or by issuing the redirect command multiple times. If you try to add more than 16 IP addresses to the redirect policy the CLI issues an error message. If you specify an IP address and weight that already exists in the redirect policy the new values override the existing values.
- **weight weight_num**: When multiple addresses are specified, they are selected in a weighted round-robin scheme. Entries with higher weights are more likely to be chosen. If a weight is not specified the entry is automatically assigned a weight of 1. weight_num must be an integer from 1 through 10.
- **reject**: This option will cause any overload traffic to be rejected. The PDSN will send an A11 Registration Reply Code of 82H (insufficient resources).
- **use-reject-code admin-prohibited**: When this keyword is specified and traffic is rejected, the error code admin prohibited is returned instead of the error code insufficient resources. This is the default behavior.
- **use-reject-code insufficient-resources**: When this keyword is specified and traffic is rejected, the error code insufficient resources is returned instead of the error code admin prohibited.

policy pcf-zone-match zone_number redirect address [ weight weight_num ] [ address2 [ weight weight_num ] ... address16 [ weight weight_num ] ] [ [ redirect address [ weight weight_num ] [ address2 [ weight weight_num ] ... address16 [ weight weight_num ] ] ]

Specifies how a PDSN service should handle an incoming call that matches a predefined zone number.

- **zone_number**: An integer between 1 and 32 that defines the zone incoming calls must match for redirection.
- **redirect**: This option enables a redirect policy for overloading conditions. When a redirect policy is invoked, the PDSN service rejects new sessions with an A11 Registration Reply Code of 88H (unknown PDSN address) and provides the IP address of an alternate PDSN. This command can be issued multiple times.
address: The IP address of an alternate PDSN expressed in IP v4 dotted decimal notation. Up to 16 IP addresses can be specified either in one command or by issuing the redirect command multiple times. If you try to add more than 16 IP addresses to the redirect policy the CLI issues an error message. If you specify an IP address and weight that already exists in the redirect policy the new values override the existing values.

weight weight_num: When multiple addresses are specified, they are selected in a weighted round-robin scheme. Entries with higher weights are more likely to be chosen. If a weight is not specified the entry is automatically assigned a weight of 1. weight_num must be an integer from 1 through 10.

policy rrq mei-from-current-pcf suppress-ppp-restart
rrq configures policy for PPP restart after getting mei in rrq.
mei-from-current-pcf mei is received in rrq from current pcf.
suppress-ppp-restart suppresses ppp restart when mei is received in rrq from current pcf

policy service-option enforce
service-option configures R-P service-option to use for specific PDSN service. Must be followed by valid service-option number, ranging from 0 to 1000.
enforce designates enforcement of R-P service-option number.

policy unknown-cvse enforce
unknown-cvse configures PDSN service unknown cvse policy.
enforce enforces unknown cvse policy where unknown CVSEs in RRQs will cause Deny

Usage
Policies can be implemented to dictate PDSN service behavior for various conditions such as overloading. The system invokes the overload policy if the number of calls currently being processed exceeds the licensed limit for the maximum number of sessions supported by the system. The system automatically invokes the overload policy when an on-line software upgrade is started.
Use the no policy { overload | service-option } command to delete a previously configured policy. If after deleting the policy setting you desire to return the policy parameter to its default setting, use the default policy command.
The chassis is shipped from the factory with the policy options set as follows:
• overload disabled
• sequence-numbers enforced enabled

Caution: Incorrect configuration of the policy msid-match and policy pcf-zone-match keywords could result in sessions failing to be established. For example, if PDSN1 is configured to redirect sessions to PDSN2 while PDSN2 is configured to redirect sessions to PDSN1, a loop is created in which all sessions would fail to be connected. In addition, sessions will not be established if the PDSN to which the sessions are being redirected is unavailable.

Example
The following command configures the PDSN service to redirect traffic to two different destinations with weights of 1 and 10 respectively:

policy overload redirect 192.168.1.100 weight 1 192.168.1.200 weight 10
ppp

Sets PPP tunneling parameters for subscribers in the current PDSN service.

Product
PDSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PDSN Service Configuration

configure > context context_name > pdsn-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-psdn-service)#

Syntax

ppp [ tunnel-context context_name | tunnel-type { l2tp | none } ]

[ no | default ] ppp tunnel-type

no
Enables/Disables the PPP tunneling parameters for subscribers in the current PDSN service.

default
Sets / Restores default value assigned for PPP tunneling parameters for subscribers in the current PDSN service.

tunnel-context context_name
The name of the context that has a LAC service configured to handle all tunnels from this PDSN service.

tunnel-type { l2tp | none }
12tp: Force all subscriber sessions in this PDSN service to use L2TP tunneling.
none: Do not force L2TP tunneling. This is the default.

Important: If the context specified by the ppp tunnel-context context_name command does not have a LAC service configured and tunnel-type is set to l2tp or the call is rejected.

Important: If the PPP tunnel context has not been set or has been cleared with the no ppp tunnel-context command and tunnel-type is set to l2tp, the context where the current PDSN service resides is used. If that context does not have a LAC service configured the call is rejected.

Usage
Use this command to enable or disable forced L2TP tunneling for all subscribers using this PDSN service. Also use this command to define which context defines the L2TP tunneling parameters.
Example

To set the tunnel context to the context named `context1` and enable forced L2TP tunneling, use the following commands;

```plaintext
ppp tunnel-context context1
ppp tunnel-type l2tp
```

To enable forced L2TP tunneling with IPSEC security, use the following commands;

```plaintext
ppp tunnel-type l2tp-secure
```

To disable forced tunneling, use the following command;

```plaintext
ppp tunnel-type none
```

To clear the setting for the tunnel context, use the following command;

```plaintext
no ppp tunnel-context
```
qos-profile-id-mapping

Creates the customized QoS profile identifier to QoS mapping for IMS authorization support.

**Product**
PDSN

**HA**

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PDSN Service Configuration

```
configure > context context_name > pdsn-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pdsn-service) #
```

**Syntax**

```
qos-profile-id-mapping profile-id id_num { [ description desc ] | [ downlink-bw dl_bw] | [ drop-rate drop_percentage ] | [ latency latency_duration ] | [ qos-class { class-A | class-B | class-C | class-D | class-E | class-F } ] | [ uplink-bw ul_bw ] } +
[ default | no ] qos-profile-id-mapping profile-id id_num
```

**default**

Configures the specified QoS profile ID for QoS mapping with default values in this PDSN service.

**no**

Removes the configured QoS profile ID mapping in this PDSN service.

**profile-id id_num**

Specifies the profile identifier for QoS parameters to be used as the customized profile ID or modifies the QoS parameters in a profile ID (id_num) coming from RAN.

*id_num* must be an integer between 0 and 65535.

**description desc**

Specifies the user defined description for profile identifier.

*desc* must be an alpha and/or numeric string between 1 and 32 characters.

**downlink-bw dl_bw**

Default: 32
Specifies the downlink (towards the MN) data traffic bandwidth in kilo-bits per second for this QoS profile.

*dl_bw* must be an integer value between 0 and 100000.

**drop-rate drop_percentage**

Default: 0
Specifies the permitted packet drop rate in percentage for traffic flow to this QoS profile. 
\textit{drop\_percentage} must be an integer value between 0 and 1000.

\textbf{latency} \textit{latency\_duration}

Default: 1000

Specifies the permitted latency duration in milli-seconds for this QoS profile. 
\textit{latency\_duration} must be an integer value between 0 and 1000.

\textbf{qos-class \{class-A | class-B | class-C | class-D | class-E | class-F\}}

Default: Class-C

Specifies the type of QoS class associated with this QoS profile

- class-A: Specifies the A type of QoS class.
- class-B: Specifies the B type of QoS class.
- class-C: Specifies the C type of QoS class.
- class-D: Specifies the D type of QoS class.
- class-E: Specifies the E type of QoS class.
- class-F: Specifies the F type of QoS class.

\textbf{uplink-bw ul\_bw}

Default: 32

Specifies the uplink (from the MN) data traffic bandwidth in kilo-bits per second for this QoS profile. 
\textit{ul\_bw} must be an integer value between 0 and 100000.

More than one of the above keywords can be entered within a single command.

\textbf{Usage}

Use this command to define the values associated with the profile ID on the PDSN. This profile ID is used during the mapping to and from the authorized QoS to the QoS parameters for the A10 link. This mapping is required because the PDSN only knows the profile IDs and not the actual configured values for the profile ID in the RAN. Also this configuration allows the use of custom profile IDs for the subscribers.

If no values are defined with a QoS profile ID, the values from matching QoS profile ID from RAN will be applicable to the subscriber traffic.

\textbf{Example}

The following command sets the downlink bandwidth to 32 kbps, latency duration as 1000 ms, uplink bandwidth to 32 kbps, and QoS class to Class-C for the QoS profile ID 11 in a PDSN service:

\begin{verbatim}
default qos-profile-id-mapping profile-id 11
\end{verbatim}
**qos update**

Sets QoS update parameters for policy mismatches or wait timeouts.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PDSN Service Configuration

```
configure > context context_name > pdsn-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pdsn-service)#
```

**Syntax**

```
qos-update { policy-mismatch | wait-timeout seconds action { disconnect-session | downgrade-to-best-effort | drop-packets } }
[ no | default ] qos-update { policy-mismatch | wait-timeout }
```

**no**


**default**

Sets / Restores default value for `qos-update [ policy-mismatch | wait-timeout ]`.

**policy-mismatch**

PDSN raises a TFT violation if there is a QoS policy mismatch.

**wait-timeout seconds action { disconnect-session | downgrade-to-best-effort | drop-packets }**

Sets the wait time for A11 RRQ for QoS changes. `seconds` must be an integer from 1 through 1000.

**action:** configures the action on the wait-timeout

- **disconnect-session:** Drops the call if the A11 RRQ has not been received for the QoS update. This includes all of the IP flows for the session.

- **downgrade-to-best-effort:** Drops packets if the A11 RRQ has not been received for the QoS update. Sends the forward traffic over best effort (flow FF or FE if available).

- **drop-packets:** Drops packets if the A11 RRQ has not been received for the QoS update.

**Usage**

This command provides a PDSN service level configurable to configure an action, if the PCF ignores the QoS Update request from PDSN. It sets the amount of time to wait and the action to take, if no RRQ is received before the timeout. The action can be to drop packets for the flow, disconnect the session or to downgrade to best effort.
Example

```
qos-update policy-mismatch
```

The following command sets `wait-timeout` to 60 seconds and invokes `downgrade-to-best-effort` if the A11 RRQ has not been received for the QoS update:

```
qos-update wait-timeout 60 action downgrade-to-best-effort
```
registration-accept

Allows the PDSN to accept registration requests when a handoff disconnect is in progress. When the PDSN is tearing
down a session and the MN moves over to a new PCF and initiates a new session, the PDSN by default does not accept
the handoff until it tears down the old session.

Product
PDSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PDSN Service Configuration
configure > context context_name > psdn-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-psdn-service)#

Syntax

[ no | default ]registration-accept handoff session-disconnect-in-progress

<table>
<thead>
<tr>
<th>no</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable accepting of registration requests when a handoff disconnect is still in progress.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default is disabled.</td>
</tr>
<tr>
<td>Sets / Restores default value assigned for registration-accept handoff session-disconnect-in-progress.</td>
</tr>
</tbody>
</table>

Usage
Use this command to allow the PDSN service to accept registration requests when a handoff disconnect is still in progress.

Example
registration-accept handoff session-disconnect-in-progress
registration-ack-deny terminate-session-on-error

Configures the PDSN service to terminate an A11 session when a Registration ACK received from the PCF has an error status.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PDSN Service Configuration
configure > context context_name > psdn-service service_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-psdn-service)#
```

**Syntax**

```
[ no | default ] registration-ack-deny terminate-session-on-error
```

- **no**
  Disable terminating A11 sessions on a Registration ACK error from the PCF.

- **default**
  Sets / Restores default value assigned to `registration-ack-deny terminate-session-on-error`.

**Usage**

Use this command to enable the PDSN service to terminate A11 sessions on a Registration ACK error from the PCF.

**Example**

Use the following command to enable this functionality in the PDSN:

```
registration-ack-deny terminate-session-on-error
```
registration-deny

Configures parameters related to registration rejection.

Product
PDSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PDSN Service Configuration

configure > context context_name > pdsn-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pdsn-service)#

Syntax

registration-deny { handoff { closedrp-rp handoff-in-progress | connection-setup-record-absent [ use-deny-code { poorly-formed-request | reason-unspecified } | max-deny-reply-limit num | mismatched-coa-source-address | new-call { connection-setup-record-absent | reverse-tunnel-unavailable } | session-already-active | session-already-closed | session-already-dormant | terminate-session-on-error | use-zero-gre-key}]

[ default | no ] registration-deny { handoff { closedrp-rp handoff-in-progress | connection-setup-record-absent } | mismatched-coa-source-address | new-call | connection-setup-record-absent | reverse-tunnel-unavailable } | session-already-active | session-already-closed | session-already-dormant | terminate-session-on-error | use-zero-gre-key}

default
Sets / Restores default value for registration-deny.

no
Disables the specified option.

handoff { closedrp-rp handoff-in-progress | connection-setup-record-absent [ use-deny-code { poorly-formed-request | reason-unspecified }]

This command configures the handoff behavior.

closedrp-rp handoff-in-progress: Configures parameters related to denying handoffs from Closed-RP to RP systems. When enabled the PDSN rejects retransmitted handoff R-P requests when a handoff is already in progress from Closed RP to RP. The deny code used is 'Reason Unspecified'. The default is disabled meaning that the PDSN simply discards such requests.

connection-setup-record-absent [ use-deny-code { poorly-formed-request | reason-unspecified }]: When enabled the PDSN denies or discards handoff R-P sessions that do not have an Airlink Connection Setup record in the A11 Registration Request. Default is disabled. Default PDSN behavior is to accept such requests.

[ use-deny-code { poorly-formed-request | reason-unspecified }]: Sets the specified Registration Deny Code when denying a handoff because of a missing connection setup record.
max-deny-reply-limit  \texttt{num}

Default: 3

Configures max number of retries of erroneous registration request message from PCF for a session before PDSN terminates the session. \texttt{num} can be from 1 to 10.

mismatched-coa-source-address

Default: disabled

Denies RP requests which have a care-of-address field that is different from the request source address.

new-call \{ connection-setup-record-absent \} \{ use-deny-code \{ poorly-formed-request \} \{ reason-unspecified \} \{ reverse-tunnel-unavailable \}

connection-setup-record-absent: Configures the PDSN to reject calls that do not have the airlink connection setup record in the RRQ.

use-deny-code \{ poorly-formed-request \} \{ reason-unspecified \} When rejecting calls that do not have the airlink setup record, use the specified deny code.

reverse-tunnel-unavailable: Configures the PDSN to reject calls if the GRE key for a user collides with that of another user.

session-already-active

PDSN denies Registration requests for sessions that are already active with the error code “poorly formed request”.

session-already-closed

PDSN denies RP renew and dereg requests with error code 0x8E for absent R-P sessions.

session-already-dormant

PDSN denies Registration requests for sessions that are already dormant with the error code “poorly formed request”.

terminate-session-on-error

Default: Disabled.

Configures PDSN to terminate session if erroneous registration request message is received for the session.

use-zero-gre-key

Configures the PDSN to set the GRE key to zero (0) when denying a new R-P session.

Usage

Use this command to configure parameters relating to the rejection of registration requests.

Example

To reject calls that do not have the airlink setup record in the RRQ, enter the following command:

\texttt{registration-deny new-call connection-setup-record-absent}

To reject calls if the GRE key collides with that of another user, enter the following command:

\texttt{registration-deny new-call reverse-tunnel-unavailable}
To set the GRE key to 0 (zero) when a new R-P session is denied, enter the following command:

```
registration-deny new-call use-zero-gre-key
```
registration-discard

Configures the PDSN service to discard any Registration Request message containing multiple information elements of the same type or a different GRE key for existing IMSI session.

Product
PDSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PDSN Service Configuration

configure > context context_name > pdsn-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pdsn-service)#

Syntax

[ default | no ] registration-discard { bad-extension | gre-key-change | handoff-connection-setup-record-absent }

default
Sets / Restores default value assigned for registration-discard.

no
Disables the discarding of Registration request messages containing multiple information elements or different GRE keys.

bad-extension
Default: Disabled
Configures the PDSN to discard Registration Request message containing multiple information elements of same type.

gre-key-change
Default: Disabled
Configures PDSN to discard Registration Request message containing different GRE key for existing IMSI session. Default is disable

handoff connection-setup-record-absent
Default: Disabled
When enabled, discards A11 Handoff requests that do not contain the Airlink Setup record.

Usage
Use this command to configure the PDSN service to discard and Registration Requests that contain multiple information elements of the same type or discard Registration Requests that contain GRE keys that have different GRE keys for the existing IMSI session.
Example

To configure the PDSN service to discard of Registration Requests that have multiple information elements of the same type, enter the following command:

```
registration-discard bad-extension
```

To configure the PDSN service to discard registration Requests that contain a GRE key that is different than the existing one for the existing IMSI session, enter the following command:

```
registration-discard gre-key-change
```
registration-update

Configures registration update related parameters for the PDSN.

Product
PDSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PDSN Service Configuration

configure > context context_name > pdsn-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pdsn-service)#

Syntax

registration-update { pdsn-code-nvse | wait-timeout secs }
[ default | no ] registration-update { pdsn-code-nvse | wait-timeout }

no
If this option is used with the pdsn-code-nvse keyword, then pdsn-code-nvse configuration is disabled. If this option is used with the wait-timeout keyword, a separate A11 timer is not used. The PDSN waits for the ppp retransmit-timeout and then sends the A11 Update. If a value is provided, then the "ppp retransmit-timeout" is ignored and a separate A11 timeout is started immediately upon sending the LCP Term-Ack. The A11 Update is then sent when the timer expires. A value of 0 sends the A11 Update immediately after sending the LCP Term-Ack.

default
Sets / Restores default value assigned for registration-update { pdsn-code-nvse | wait-timeout }

pdsn-code-nvse
Adds the PDSN code NVSE in all A11 registration update messages.

secs
The number of seconds to wait. secs must be an integer in the range from 0 through 16.

wait-timeout
After the Mobile Node terminates a PPP session between the PDSN and the Mobile Node, the PDSN service waits for the specified time period to receive an A11 RRQ from the PCF before it sends out a Registration-Update to clear the Session from the PCF.

Usage
Use this command to configure registration update related
The `wait-timeout` keyword configures the PDSN to wait the specified amount of time before sending out a Registration-Update to clear the Session from the PCF.

**Example**

Use the following command to set the registration wait-timeout to 16 seconds:

```
registration-update wait-timeout 16
```
retransmission-timeout

Configures the maximum allowable time for the PDSN service to wait for a response from the PCF before it a) attempts to communicate with the PCF again (if the system is configured to retry the PCF) or b) marks the PCF as unreachable.

Product: PDSN
Privilege: Security Administrator, Administrator
Mode: Exec > Global Configuration > Context Configuration > PDSN Service Configuration
configure > context context_name > psdn-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-psdn-service)#

Syntax:

retransmission-timeout time

[ default | no ] retransmission-timeout

no

Enables/Disables the retransmission-timeout.

default

Sets / Restores default value assigned for retransmission-timeout.

time

Specifies the maximum allowable time for the PDSN service to wait for a response from the PCF before it a) attempts to communicate with the PCF again (if the system is configured to retry the PCF) or b) marks the PCF as unreachable.

time is measured in seconds and can be configured to any integer value between 1 and 1,000,000.

Usage:

Use the retransmission timeout command in conjunction with the max-retransmissions command in order to configure the PDSN services behavior when it does not receive a response from a particular PCF.
Use the no retransmission-timeout command to delete a previously configured timeout value. If after deleting the lifetime setting you desire to return the lifetime parameter to its default setting, use the default retransmission-timeout command.
The chassis is shipped from the factory with the retransmission timeout set to 3 seconds.

Example:

The following command configures a retransmission timeout value of 5 seconds:

retransmission-timeout 5

The following command deletes a previously configured retransmission-timeout setting:
noretransmission-timeout
service-option

If the service option policy is enabled, this command specifies the service options supported by the PDSN service.

Product
PDSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PDSN Service Configuration

configure > context context_name > pdsn-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pdsn-service)#

Syntax

service-option number
no service-option number

no
Enables/Disables the service-option number

default
Sets / Restores default value assigned for service-option.

number
Default: 7, 15, 22, 23, 24, 25, 33, 59, 67
Specifies a specific Service Option (SO) number that this PDSN service is allowed to support.
number can be configured to any integer value between 1 and 1000.

Usage

Use the service option command in conjunction with the policy service option enforce command to configure specific SO numbers that are supported. If a particular SO number is not configured, then any subscriber session received with that SO number will be rejected and an A11 Registration Reply Code of 86 (poorly formed request) will be sent.

By default, PDSN services are configured to support the following service option numbers:

• 7: PCF specific
• 15: PCF specific
• 22: High Speed Packet Data Service: Internet or ISO Protocol Stack (RS1 forward, RS1 reverse)
• 23: High Speed Packet Data Service: Internet or ISO Protocol Stack (RS1 forward, RS2 reverse)
• 24: High Speed Packet Data Service: Internet or ISO Protocol Stack (RS2 forward, RS1 reverse)
• 25: High Speed Packet Data Service: Internet or ISO Protocol Stack (RS2 forward, RS2 reverse)
• 33: 3G High Speed Packet Data
- 59: High Rate Packet Data
- 67: RP A10 connection

**Important:** Option 67 is used for auxiliary connections for Rev-A calls. PPP encapsulation of data packets does not flow over this service option connection. ROHC can be performed without PPP for this service option.

Use the `no service-option number` command to delete a previously configured service option. If after deleting the service option setting you desire to return the service option parameter to its default setting, use the `default service-option command`.

**Example**

The following command enables a service option of 12:

```
service-option 12
```

The following command disables the default service option 59:

```
no service-option 59
```
**setup-timeout**

Specifies the maximum amount of time allowed for session setup.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PDSN Service Configuration

```
configure > context context_name > pdsn-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pdsn-service)#
```

**Syntax**

```
[ no ] setup-timeout seconds
```

- **default setup-timeout**
  
  ```
  default
  
  Sets / Restores default value assigned for setup-timeout.
  
  seconds
  
  Default: 60 seconds
  
  The maximum amount of time, in seconds, to allow for setup of a session. seconds must be an integer from 1 through 1000000
  ```

**Usage**

Use this command to set the maximum amount of time allowed for setting up a session.

**Example**

Use the following command to set the maximum time allowed for setting up a session to 300 seconds:

```
setup-timeout 300
```
simple-ip allow

Enables or disables Simple-IP sessions from making a connection before authorization takes place.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PDSN Service Configuration

```
configure > context context_name > pdsn-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pdsn-service)#
```

**Syntax**

```
[no | default ] simple-ip allow
```

- **no**
  
  When a session attempts PPP authentication, it is assumed that it is a Simple-IP session and it is disconnected before the user is authenticated (RADIUS or local authentication). Also, if `allow-noauth` is enabled and PPP authentication is not performed, after IPCP the session is disconnected if it is discovered that it is a Simple-IP session.

- **default**
  
  Reset this command to allow Simple-IP sessions to connect.

**Usage**

Use this command to prevent Simple-IP sessions from connecting to a PDSN service.

**Example**

The following command configures the PDSN service so that it will reject any Simple-IP sessions:

```
nosimple-ip allow
```

The following command configures the PDSN service to allow Simple-IP sessions:

```
simple-ip allow
```
spi

Configures the security parameter index (SPI) between the PDSN service and the PCF. This command also configures the redirection of call based on PCF zone.

Product
PDSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PDSN Service Configuration

configure > context context_name > pdsn-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pdsn-service)#

Syntax

```
spi remote-address { pcf_ip_address | ip_addr_mask_combo } spi-number number {
encrypted secret enc_secret | secret secret } [ description string ] [ hash-algorithm { md5 | rfc2002-md5 } ] [ replay-protection { nonce | timestamp } ] [ timestamp-tolerance tolerance ] [ zone zone_id ]
```

no spi remote-address pcf_ip_address spi-number number

remote-address { pcf_ip_address | ip_addr_mask_combo }

pcf_ip_address: Specifies the IP address of the PCF. pcf_ip_address is an IP address expressed in IP v4 dotted decimal notation.

ip_addr_mask_combo: Specifies the IP address of the PCF and specifies the IP address network mask bits. ip_addr_mask_combo must be specified using the form ‘IP Address/Mask Bits’ where the IP address must either be an IPv4 address expressed in dotted decimal notation or an IPv6 address expressed in colon notation and the mask bits are a numeric value which is the number of bits in the subnet mask.

spi-number number

Specifies the SPI (number) which indicates a security context between the PCF and the PDSN in accordance with IOS 4.1 and RFC 2002. number can be configured to any integer value between 256 and 4294967295.

encrypted secret enc_secret | secret secret

Configures the shared-secret between the PDSN service and the PCF. The secret can be either encrypted or non-encrypted.

encrypted secret enc_secret: Specifies the encrypted shared key (enc_secret) between the PCF and the PDSN service. enc_secret must be between 1 and 254 alpha and/or numeric characters and is case sensitive.

secret secret: Specifies the shared key (secret) between the PCF and the PDSN services. secret must be between 1 and 127 alpha and/or numeric characters and is case sensitive.

The encrypted keyword is intended only for use by the chassis while saving configuration scripts. The system displays the encrypted keyword in the configuration file as a flag that the variable following the

secret keyword is the encrypted version of the plain text secret key. Only the encrypted secret key is saved as part of the configuration file.

```
description string
```
This is a description for the SPI. string must be an alpha and or numeric string of from 1 through 31 characters.

```
hash-algorithm { md5 | rfc2002-md5 }
```
Default: md5
Specifies the hash-algorithm used between the PDSN service and the PCF.
- md5: Configures the hash-algorithm to implement MD5 per RFC 1321.
- rfc2002-md5: Configures the hash-algorithm to implement keyed-MD5 per RFC 2002.

```
replay-protection { nonce | timestamp }
```
Default: timestamp
Specifies the replay-protection scheme that should be implemented by the PDSN service.
- nonce: Configures replay protection to be implemented using NONCE per RFC 2002.
- timestamp: Configures replay protection to be implemented using timestamps per RFC 2002.

```
timestamp-tolerance tolerance
```
Default: 60
Specifies the allowable difference (tolerance) in timestamps that is acceptable. If the difference is exceeded, then the session will be rejected. If this is set to 0, then time stamp tolerance checking is disabled at the receiving end.
tolerance is measured in seconds and can be configured to any integer value between 0 and 65535.

```
zone zone_id
```
Specifies the different PCF zones to configure in PDSN service. Mapping of a zone-number to a set of PDSNs can be done per PDSN service basis.
zzone_id must be an integer value between 1 and 32. A maximum of 32 PCF zones can be configured for a PDSN service.

**Usage**

An SPI is a security mechanism configured and shared by the PCF and the PDSN service. Please refer to IOS 4.1 and RFC 2002 for additional information.
Multiple SPIs can be configured if the PDSN service is communicating with multiple PCFs.

**Important:** The SPI configuration on the PCF must match the SPI configuration for the PDSN service on the system in order for the two devices to communicate properly.

Use the `no` version of this command to delete a previously configured SPI.
This command used with `zone zone_id` redirects all calls on the basis of PCF zone to the specific PDSN on the basis of parameters configured at policy pcf-zone-match command.

**Example**

The following command configures the PDSN service to use an SPI of 256 when communicating with a PCF with the IP address 192.168.0.2. The key that would be shared between the PCF and the PDSN service is q397F65.
spi remote-address 192.168.0.2 spi-number 256 secret q397F65

The following command deletes the configured SPI of 400 for an PCF with an IP address of 172.100.3.200:

```
no spi remote-address 172.100.3.200 spi-number 400
```

The following command creates the configured SPI of 400 for an PCF with an IP address of 172.100.3.200 and zone id as 11:

```
spi remote-address 172.100.3.200 spi-number 400 zone 11
```
**tft-validation wait-timeout**

Configures the TFT validation wait timeout value for QoS changes. The QoS update timer triggers automatic QoS updates based on dynamic policies.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PDSN Service Configuration

```plaintext
configure > context context_name > pdsn-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pdsn-service)>
```

**Syntax**

```plaintext
tft-validation wait-timeout seconds
[ default | no ] tft-validation wait-timeout
```

- **no**
  
  Removes the wait-timeout timer.

- **default**
  
  Sets / Restores default value assigned for tft-validation wait-timeout.

**Usage**

Configures the TFT validation wait time value for A11 RRQ for QoS changes. `seconds` must be an integer from 1 through 65535.

**Example**

Use the following command to set the TFT validation wait-timeout to 5 seconds:

```plaintext
tft-validation wait-timeout 5
```
threshold a11-ppp-send-discard

Sets an alarm or alert for the PDSN service based on the number of packets that the PPP protocol processing layer internally discarded on transmit for any reason.

Product
PDSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PDSN Service Configuration
configure > context context_name > pdsn-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pdsn-service)#

Syntax

threshold all-ppp-send-discard high_thresh [ clear low_thresh ]

no threshold all-ppp-send-discard

---

high_thresh

Default: 0
The high threshold number of discarded PPP send packets that must be met or exceeded within the polling interval to generate an alert or alarm. It can be configured to any integer value between 0 and 100000.

---

clear low_thresh

Default: 0
The low threshold number of discarded PPP send packets that must be met or exceeded within the polling interval to clear an alert or alarm. It can be configured to any integer value between 0 and 100000.

---

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Use this command to set an alert or an alarm when the number of discarded PPP send packets is equal to or greater than a specified number. Alerts or alarms are triggered for the number of discarded PPP send packets is based on the following rules:

- **Enter condition:** Actual number of discarded PPP send packets > High Threshold
- **Clear condition:** Actual number of discarded PPP send packets ≤ Low Threshold

Example
The following command configures a number of discarded PPP send packets threshold of 1000 and a low threshold of 500 for a system using the Alarm thresholding model:

```
threshold all-ppp-send-discard 1000 clear 500
```
threshold a11-rac-msg-discard

Sets an alarm or alert based on the number of Discarded A11 Registration Acknowledgements for the PDSN service.

Product
PDSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PDSN Service Configuration

configure > context context_name > pdsn-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pdsn-service)#

Syntax

threshold a11-rac-msg-discard high_thresh [ clear low_thresh ]

no threshold a11-rac-msg-discard

no

Deletes the alert or alarm.

high_thresh

Default: 0

The high threshold number of Discarded A11 Registration Acknowledgements that must be met or exceeded within the polling interval to generate an alert or alarm. It can be configured to any integer value between 0 and 100000.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Use this command to set an alert or an alarm when the number of Discarded A11 Registration Acknowledgements is equal to or greater than a specified number.

Alerts or alarms are triggered for the number of Discarded A11 Registration Acknowledgements based on the following rules:

- **Enter condition:** Actual number of Discarded A11 Registration Acknowledgements > High Threshold
- **Clear condition:** Actual number of Discarded A11 Registration Acknowledgements £ Low Threshold
Example

The following command configures a number of Discarded A11 Registration Acknowledgements threshold of 1000 and a low threshold of 500 for a system using the Alarm thresholding model:

```
threshold all-rac-msg-discard 1000 clear 500
```
threshold a11-rrp-failure

Sets an alarm or alert based on the number of A11 Registration Response failures for the PDSN service.

Product
PDSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PDSN Service Configuration

configure > context context_name > pdsn-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pdsn-service)#

Syntax

threshold a11-rrp-failure high_thresh [ clear low_thresh ]

no threshold a11-rrp-failure

do

Deletes the alert or alarm.

high_thresh

Default: 0

The high threshold number of A11 Registration Response failures that must be met or exceeded within the polling interval to generate an alert or alarm. It can be configured to any integer value between 0 and 100000.

clear low_thresh

Default: 0

The low threshold number of A11 Registration Response failures that must be met or exceeded within the polling interval to clear an alert or alarm. It can be configured to any integer value between 0 and 100000.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Use this command to set an alert or an alarm when the number of A11 Registration Response failures is equal to or greater than a specified number. Alerts or alarms are triggered for the number of A11 Registration Response failures based on the following rules:

- **Enter condition:** Actual number of A11 Registration Response failures > High Threshold
- **Clear condition:** Actual number of A11 Registration Response failures £ Low Threshold

Example
The following command configures a number of A11 Registration Response failures threshold of 1000 and a low threshold of 500 for a system using the Alarm thresholding model:

```
threshold all-rrp-failure 1000 clear 500
```
threshold a11-rrq-msg-discard

Sets an alarm or alert based on the number of Discarded A11 Registration Requests for the PDSN service.

Product
PDSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PDSN Service Configuration

configure > context context_name > pdsn-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pdsn-service) #

Syntax

threshold a11-rrq-msg-discard high_thresh [ clear low_thresh ]

no threshold a11-rrq-msg-discard

no

Deletes the alert or alarm.

high_thresh

Default: 0
The high threshold number of Discarded A11 Registration Requests that must be met or exceeded within the polling interval to generate an alert or alarm. It can be configured to any integer value between 0 and 100000.

clear low_thresh

Default: 0
The low threshold number of Discarded A11 Registration Requests that must be met or exceeded within the polling interval to clear an alert or alarm. It can be configured to any integer value between 0 and 100000.

Important: This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Use this command to set an alert or an alarm when the number of Discarded A11 Registration Requests is equal to or greater than a specified number.
Alerts or alarms are triggered for the number of Discarded A11 Registration Requests based on the following rules:

• Enter condition: Actual number of Discarded A11 Registration Requests > High Threshold
• Clear condition: Actual number of Discarded A11 Registration Requests ≤ Low Threshold

Example
The following command configures a number of Discarded A11 Registration Requests threshold of 1000 and a low threshold of 500 for a system using the Alarm thresholding model:

```
threshold all-rrq-msg-discard 1000 clear 500
```
threshold init-rrq-rcvd-rate

Sets an alarm or alert based on the average number of calls setup per second for the context.

Product
PDSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PDSN Service Configuration

configure > context context_name > psdn-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-psdn-service)#

Syntax

threshold init-rrq-rcvd-rate high_thresh [ clear low_thresh ]

no threshold init-rrq-rcvd-rate

no

Deletes the alert or alarm.

high_thresh

Default: 0

The high threshold average number of calls setup per second must be met or exceeded within the polling interval to generate an alert or alarm. It can be configured to any integer value between 0 and 1000000.

clear low_thresh

Default: 0

The low threshold average number of calls setup per second that must be met or exceeded within the polling interval to clear an alert or alarm. It can be configured to any integer value between 0 and 1000000.

**Important:** This value is ignored for the Alert model. In addition, if this value is not configured for the Alarm model, the system assumes it is identical to the high threshold.

Usage

Use this command to set an alert or an alarm when the average number of calls setup per second is equal to or greater than a specified number of calls per second.

Alerts or alarms are triggered for the number of calls setup per second based on the following rules:

- **Enter condition:** Actual number of calls setup per second $>$ High Threshold
- **Clear condition:** Actual number of calls setup per second $\leq$ Low Threshold

Example
The following command configures a number of calls setup per second threshold of 1000 and a low threshold of 500 for a system using the Alarm thresholding model:

```
threshold init-rrq-rcvd-rate 1000 clear 500
```
Chapter 250
PDSN Service RoHC Configuration Mode Commands

The PDSN Service RoHC Configuration Mode is used to configure RoHC (Robust Header Compression) parameters the PDSN service conveys to the PCF in the initial A11 RRP message before PPP authentication.

Mode

Exec > Global Configuration > Context Configuration > PDSN Service Configuration > PDSN Service ROHC configure > context context_name > psdn-service service_name > ip header-compression rohc

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ip-header-compression-rohc)#

Important: The commands, keywords and variables in this mode are available dependent on platform type, product version, and installed license(s).
cid-mode

Enters the RoHC Profile Compression Options Configuration mode and configures options that apply during RoHC compression for the current RoHC profile.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PDSN Service Configuration > PDSN Service ROHC configure > context context_name > pdsn-service service_name > ip header-compression rohc

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ip-header-compression-rohc)#
```

**Syntax**

cid-mode { large | small } max-cid integer
default cid-mode

**default cid-mode**

- **default**
  Reset all options in the RoHC Profile Compression Configuration mode to their default values.

- **large**
  Use large packets with optional information for RoHC

- **small**
  This is the default packet size.
  Use small RoHC packets.

- **max-cid integer**
  Default: 15
  The highest context ID number to be used by the compressor. integer must be an integer from 0 through 15 when small packet size is selected and must be an integer from 0 through 31 when large packet size is selected.

**Usage**

Use this command to set the RoHC packet size and define the maximum

**Example**

The following command sets large RoHC packet size and sets the maximum CID to 100:

```
cid-mode large max-cid 100
```

The following command sets the cid-mode to the default settings of small packets and max-cid 0:
default cid-mode
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
exit
```

Usage
Use this command to return to the parent configuration mode.
mrru

Sets the size of the largest reconstructed reception unit, in octets, that the decompressor is expected to reassemble from segments. The size includes the CRC. If MRRU is negotiated to be 0, no segment headers are allowed on the channel.

Product
PDSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PDSN Service Configuration > PDSN Service ROHC
configure > context context_name > pdsn-service service_name > ip header-compression rohc

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ip-header-compression-rohc)#

Syntax

mrru num_octets

default mrru

default
reset the value of this command to its default setting

num_octets

Default: 0
This is the number of octets for the maximum size of the largest reconstructed reception unit allowed.
num_octets must be an integer from 0 through 65535.

Usage

Use this command to set the size, in octets, of the largest reconstructed reception unit, in octets, that the decompressor is expected to reassemble from segments.

Example

The following command sets the largest reconstructed reception unit to 1024 octets:

mrru 1024

The following command resets the mrru size to its default of 0 octets:

default mrru
**profile**

Specifies the header compression profiles to use. A header compression profile is a specification of how to compress the headers of a specific kind of packet stream over a specific kind of link. At least one profile must be specified.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PDSN Service Configuration > PDSN Service ROHC configure > context context_name > pdsn-service service_name > ip header-compression rohc

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ip-header-compression-rohc)#
```

**Syntax**

```
profile { [ esp-ip ] [ rtp-udp ] [ udp-ip ] [ uncompressed-ip ] }
```

**default profile**

```
default
Default: esp-ip rtp-udp udp-ip uncompressed-ip
This command sets the RoHC profile configuration back to its default setting.
```

```
esp-ip
This enables RoHC Profile 0x0003 which is for ESP/IP compression, compression of the header chain up to and including the first ESP header, but not subsequent subheaders.
```

```
rtp-udp
This enables RoHC Profile 0x0001 which is for RTP/UDP/IP compression
```

```
udp-ip
This enables RoHC Profile 0x0002 which is for UDP/IP compression, compression of the first 12 octets of the UDP payload is not attempted.
```

```
uncompressed-ip
This enables RoHC Profile 0x0000 which is for sending uncompressed IP packets.
```

**Usage**

Use this command to specify the RoHC header compression profiles to use.

**Example**

The following command sets the profiles to use as esp-ip and rtp-udp:

```
profile esp-ip rtp-udp
```
Chapter 251
Peer Profile Configuration Mode Commands

The Peer Profile Configuration Mode is used to configure the peer profiles for GGSN, P-GW, or S-GW service to allows flexible profile based configuration to accommodate growing requirements of customizable parameters with default values and actions for peer nodes of GGSN, P-GW, or S-GW.

Mode

Exec > Global Configuration > Peer Profile Configuration

configure > peer-profile service-type <service-type> {default | name peer_profile_name}

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-peer-profile-ggsn/pgw/sgw-access/nw)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
description

Sets a relevant descriptive string for the specific peer profile. By default it is blank.

Product

GGSN
P-GW
SAEGW
S-GW

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > Peer Profile Configuration

configure > peer-profile service-type <service-type> {default | name peer_profile_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-peer-profile-ggsn/pgw/sgw-access/nw)#

Syntax

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>description desc_string</td>
<td>Indicates the description for GGSN, P-GW, or S-GW service peer profile configured through this mode; must be an alphanumeric string from 1 through 64 characters.</td>
</tr>
<tr>
<td>no description</td>
<td>Removes the set description for GGSN, P-GW, or S-GW service peer profile configured through this mode.</td>
</tr>
</tbody>
</table>

Usage

Use this command to set a relevant description for GGSN, P-GW, or S-GW peer profile configured through this mode.

Example

The following command sets the description ggsn_gtpc_SGSN_profile1 for a GGSN peer profile:

description ggsn_gtpc_SGSN_profile1
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
dend

Usage
Use this command to return to the Exec mode.
`exit`

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
```
exit
```

**Usage**
Use this command to return to the parent configuration mode.
gtpc

Configure the GTP-C parameters for this peer profile.

Product
GGSN
P-GW
SAEGW
S-GW

Privilege
Administrator

Mode
Exec > Global Configuration > Peer Profile Configuration

configure > peer-profile service-type <service-type> {default | name peer_profile_name}

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-peer-profile-ggsn/pgw/sgw-access/nw)#

Syntax

gtpc { echo { interval inter_dur | retransmission-timeout echo_retrans_dur } | max-retransmission retrans_num | retransmission-timeout retrans_dur }

default gtpc { echo [ interval | retransmission-timeout ] | max-retransmissions | retransmission-timeout }

no gtpc echo

---

default
Resets the specified parameter to its default value.

---

no
Disables or removes the configured GTP-C echo settings.

---

echo interval inter_dur
Default: 60
Configures the duration, in seconds, between the sending of echo request messages. inter_dur must be an integer from 60 through 3600.

---

echo retransmission-timeout echo_retrans_dur
Default: 3
Configures the echo retransmission timeout, in seconds, for the this peer profile. echo_retrans_dur must be an integer ranging from 1 to 20.
max-retransmissions retrans_num
retransmission-timeout retrans_dur
retransmission-timeout-ms retrans_dur

Usage
Use this command to configure GTP-C parameters for GGSN, P-GW, or S-GW peer profile.

Example
The following command sets the GTP-C echo parameters to default values:

  default gtpc echo

The following command sets the GTP-C retransmission timeout parameters to 4 seconds:

  default gtpc retransmission-timeout-ms
lawful-intercept

Refer to the *Cisco ASR 5x00 Lawful Intercept Configuration Guide* for a description of this command.
Chapter 252
Peer-Server Configuration Mode Commands

The Peer-Server configuration mode provides the commands to define and manage the peer server configuration part of the SS7 routing on an SGSN.

Mode

Exec > Global Configuration > SS7 Routing Domain Configuration > Peer-Server Configuration

configure > ss7-routing-domain rd_id variant variant_type > peer-server id server_id

Entering the above command sequence results in the following prompt:

[local]host_name(config-ss7-rd-ss7rd_id-ps-id-peer-server_id)#

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
end

Exits the configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Change the mode back to the Exec mode.
exit

Exits the configuration mode and returns to the Global configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

exit

Usage
Return to the Global configuration mode.
mode

Configures the operational mode of the peer-server.

Product

SGSN

HNB-GW

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > SS7 Routing Domain Configuration > Peer-Server Configuration

cfg mode ( loadshare | standby )

loadshare

Sets the peer-server to load share. This is the default.

standby

Sets the peer-server to be in standby mode.

Usage

Configure the operational mode of the peer-server.

Example

Configure the peer-server for standby mode.

    mode standby
**name**

Defines the unique identification - the name - of the peer-server in the SS7 routing domain.

**Product**

SGSN

HNB-GW

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > SS7 Routing Domain Configuration > Peer-Server Configuration

configure > ss7-routing-domain rd_id variant variant_type > peer-server id server_id

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ss7-rd-ss7rd_id-ps-id-peer-server_id)#
```

**Syntax**

```
name name

no name
```

**no**

Removes the peer server’s name from this configuration instance.

**name**

```
name name
```

name: Must be a string of 1 to 64 alphanumeric characters to define a unique identification for the peer-server within the specific SS7 routing domain. Double quotes must be used to create a name that includes spaces.

**Usage**

Create peer server names that are easy to remember and uniquely identify the PSP.

**Example**

Use this command to create an easily remembered alphanumeric name for the peer-server:

```
name "Berlin West"
```
**psp**

Creates the peer-server-process (PSP) instance and enters the PSP configuration mode. See the PSP Configuration Mode chapter in this guide for information on the configuration commands.

![Important:](Image) This command configures a mandatory parameter in the configuration of the peer server.

**Product**
- SGSN
- HNB-GW

**Privilege**
- Security Administrator, Administrator

**Mode**
Exec > Global Configuration > SS7 Routing Domain Configuration > Peer-Server Configuration

```
configure > ss7-routing-domain rd_id variant variant_type > peer-server id server_id
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-ss7-ss7-ss7rd_id-ps-id-peer-server_id)#
```

**Syntax**

```
[ no ] psp instance id
```

no

Removes the PSP instance from the peer server configuration.

```
id
```

id Uniquely identifies the specific peer-server-process configuration. The Id must be an integer from 1 to 4 or for SGSN with Release 15.0 or higher, the value range is 1 to 12.

**Usage**

Use this command to define the peer-server-process (PSP) instance ID number for the SGSN configuration.

**Example**

Use this command to create instance #3 for the PSP configuration:

```
psp instance 3
```
routing-context

Defines the ID of the routing context for the peer-server to use.

Important: This command configures a mandatory parameter in the configuration of the peer server.

Product
SGSN
HNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > SS7 Routing Domain Configuration > Peer-Server Configuration
configure > ss7-routing-domain rd_id variant variant_type > peer-server id server_id

Entering the above command sequence results in the following prompt:

[local]host_name(config-ss7-ss7rd_id-ps-ps-id-peer-server_id)#

Syntax

routing-context id
no routing-context

id

id Uniquely identifies a specific routing context for the peer-server-process to use. The Id must be an integer from 1 to 65535.

no

Removes the routing-context definition from the peer server configuration.

Usage
Use this command to define routing contexts for the peer server.

Example
Define routing-context instance 15:

routing-context 15
self-point-code

This command defines the point-code to identify the SGSN as a peer server.

Product
SGSN
HNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > SS7 Routing Domain Configuration > Peer-Server Configuration
configure > ss7-routing-domain rd_id variant variant_type > peer-server id server_id

Entering the above command sequence results in the following prompt:

[local]host_name(config-ss7-ss7rd_id-ps-id-peer-server_id)#

Syntax

self-point-code point-code

no self-point-code

point-code

Point-code is an SS7-type address for an element in the SS7 network. Point-codes must be defined in dotted-decimal format in a string of 1 to 11 digits. Options include:

• 0.0.1 to 7.255.7 for point-code in the ITU range.
• 0.0.1 to 255.255.255 for point-code in the ANSI range.
• 0.0.1 to 15.31.255 for point-code in the TTC Range.
• A string of 1 to 11 digits in dotted-decimal to represent a point-code in a different range.

no

Removes the self-point-code configuration for this linkset in the peer server.

**Important:** Removing the self-point-code will result in the termination of all traffic on this link.

Usage

Use this command to define the point-code to identify the SGSN.

Example

Use the following command to remove the self-point-code definition from the peer-server configuration:

no self-point-code
Chapter 253
P-GW Service Configuration Mode Commands

The P-GW (PDN Gateway) Service Configuration Mode is used to create and manage the relationship between specified services used for either GTP or PMIP network traffic.

**Mode**

Exec > Global Configuration > Context Configuration > P-GW Service Configuration

```
configure > context context_name > pgw-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pgw-service)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
associate

Associates the P-GW service with specific pre-configured services and/or policies configured in the same context.

Product
P-GW
SAEGW

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > P-GW Service Configuration
configure > context context_name > pgw-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pgw-service)#

Syntax

associate { egtp-service name [ lma-service name ] | ggsn-service name | lma-service name [ egtp-service name ] | peer-map map_name ] | qci-qos-mapping name }

no associate { egtp-service | lma-service | peer-map | qci-qos-mapping }

no
Removes the selected association from this service.

egtp-service name [ lma-service name ] | lma-service name [ egtp-service name ]

egtp-service name [ lma-service name ]: Specifies that the P-GW service is to be associated with an existing eGTP service within this context.
Name must be an alphanumeric string of 1 through 63 characters and be an existing eGTP service.
Configure an associated LMA service name to support handoffs between PMIPv6 and GTP. Name must be an alphanumeric string of 1 through 63 characters and be an existing LMA service.
lma-service name [ egtp-service name ]: Specifies that the P-GW service is to be associated with an existing LMA service within this context.
Name must be an alphanumeric string of 1 through 63 characters and be an existing LMA service.
Configure an associated eGTP service name to support handoffs between PMIPv6 and GTP. Name must be an alphanumeric string of 1 through 63 characters and be an existing eGTP service.

ggsn-service name

Specifies that the P-GW service is to be associated with an existing GGSN service within this context.
Name must be an alphanumeric string of 1 through 63 characters and be an existing GGSN service.

peer-map map_name

Specifies that the P-GW service is to be associated with an existing peer map within this context.
map_name must be an alphanumeric string of 1 through 63 characters and be an existing peer map.
Refer to the LTE Policy Configuration Mode Commands chapter for more information on peer map creation.
associate

qci-qos-mapping name

Specifies that the P-GW service is to be associated with an existing QCI-QoS mapping configuration within this context.

*name* must be an alphanumeric string of 1 through 63 characters and be an existing QCI-QoS mapping configuration.

QCI-QoS mapping is typically configured in a AAA context. Refer to the *QCI-QoS Mapping Configuration Mode Commands* chapter for more information.

**Important:** If a GGSN service is associated with a P-GW service, then the GGSN service will use the QCI-QoS mapping tables specified in the *qci-qos-mapping* command and assigned to its associated P-GW service.

**Usage**

Use this command to associate the P-GW service with other pre-configured services and/or policies configured in the same context.

**Example**

The following command associates this service with an eGTP service called *egtp1*:

```
associate egtp-service egtp1
```
authorize-with-hss

This command enables or disables subscriber session authorization via a Home Subscriber Server (HSS) over an S6b Diameter interface. This feature is required to support the interworking of GGSN with P-GW and HA.

**Product**
P-GW
SAEGW

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > P-GW Service Configuration

```
configure > context context_name > pgw-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pgw-service)#
```

**Syntax**

```
authorize-with-hss [ egtp | lma [ s6b-aaa-group aaa-group-name | report-ipv6-addr ] | report-ipv6-addr ]
[ default | no ] authorize-with-hss
```

- **default | no**
  Disables the default authorization of subscriber over S6b interface. Resets the command to the default setting of “authorize locally” from an internal APN authorization configuration.

- **egtp**
  Enables S6b authorization for eGTP only.

- **lma**
  Enables S6b authorization for LMA only.

- **report-ipv6-addr**
  Enables the IPv6 address reporting through Authorization-Authentication-Request (AAR) towards the S6b interface.

**Usage**

Use this command to enable/disable the authorization support for subscriber over S6b interface, which is used between P-GW and the 3GPP AAA to exchange the information related to charging, GGSN discovery, etc.
**dns-client**

Specifies the DNS client context to use for sending DNS queries.

**Product**
- P-GW
- SAEGW

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > P-GW Service Configuration

```plaintext
configure > context context_name > pgw-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pgw-service)#
```

**Syntax**

```plaintext
dns-client context name

[ default | no ] dns-client context
```

---

**default**

Returns the command to the default setting of targeting the DNS client in the context where the P-GW service resides.

---

**no**

Disables DNS queries.

---

**context name**

Specifies the name of the context where the DNS client is used for the resolution of PCSCF-FQDN received from S6b interface.

*name* must be an existing context expressed as an alphanumeric string of 1 through 79 characters.

**Usage**

Use this command to specify the context where the DNS client resides to perform P-CSF-FQDN resolution from the S6b interface.

**Example**

The following command identifies the *egress1* context as the context where the DNS client resides:

```plaintext
dns-client context egress1
```
**egtp**

Configures handling of eGTP related procedures.

**Product**
P-GW
SAEGW

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > P-GW Service Configuration

```bash
configure > context context_name > pgw-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pgw-service)#
```

**Syntax**

```bash
egtp { cause-code temp-fail timeout sec retry retries | modify-bearer-cmd-negotiate-qos | overcharge-protection | sgw-restoration session-hold timeout seconds }
```

**default egtp { cause-code temp-fail | modify-bearer-cmd-negotiate-qos | overcharge-protection | sgw-restoration session-hold }**

**no egtp { cause-code temp-fail | modify-bearer-cmd-negotiate-qos | overcharge-protection | sgw-restoration session-hold }**

**default**

 Resets the command to the default setting.

**no**

 Disables the configuration statement.

- **cause-code temp-fail timeout sec retry retries**

  Enables EGTP Cause Code Handling for when the P-GW receives a temporary failure response from peer (cause code 110). All transactions that were moved to pending queue because of temporary cause failure would be reattempted after temporary failure timer expires. After timer expiry, the P-GW informs PCRF about the transient failure. PCRF sends new RAR and CBR/MBR/UBR would succeed.

  - **timeout sec**: Specifies the time to wait (in seconds) before reattempting the Create Bearer Request (CBR)/Modify Bearer Request (MBR)/Update Bearer Request (UBR).
  - **sec** must be an integer from 1 to 100.
  - **retry retry**: Specifies the maximum number of retries. The P-GW discards CBR/MBR/UBR after the maximum number of retries are exceeded.
  - **retries** must be an integer from 1 to 4.
modify-bearer-cmd-negotiate-qos
This configuration only impacts the PGW QoS negotiation behavior when PCRF is unreachable or event trigger is not registered while handling Modify Bearer Command. By default, this configuration is disabled. When enabled, P-GW will always enforce old QoS values authorized by the PCRF. When disabled, the P-GW will always accept new QoS values (APN-AMBR/Def-EPS-Bearer-QoS) received in Modify Bearer Command.

overcharge-protection
Configures overcharging protection by temporarily not charging during loss of radio coverage. By default, this configuration is disabled.

sgw-restoration session-hold timeout seconds
Enables S-GW restoration functionality and configure session hold timeout on a P-GW service. By default, S-GW restoration is disabled. seconds must be an integer from 1 to 3600. Default: 0 (disabled). On S-GW failure indication, P-GW shall check if S-GW restoration feature is enabled or not. If enabled, P-GW shall maintain all the affected sessions for session-hold timeout. After session-hold timeout, P-GW shall clear all the sessions which are not recovered yet.

Usage
Use this command to configure the behavior of the P-GW/SAEGW for eGTP procedures.

Example
The following command sets the temporary failure timer to 30 seconds and 2 retries:

```
   egtp cause-code temp-fail timeout 30 retry 2
```

The following command configures the P-GW to accept new QoS values from the modify bearer command while the PCRF is not reachable:

```
   egtp modify-bearer-cmd-negotiate-qos
```

The following command enables S-GW restoration functionality and configures session hold timeout on a P-GW service:

```
   sgw-restoration session-hold timeout seconds
```
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
end

**Usage**
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

`exit`

**Usage**

Use this command to return to the parent configuration mode.
fqdn

Configures a Fully Qualified Domain Name for this P-GW service used in messages between the P-GW and a 3GPP AAA server over the S6b interface.

Product
P-GW
SAEGW

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > P-GW Service Configuration

configure > context context_name > pgw-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pgw-service)#

Syntax

fqdn host domain_name realm realm_name

[ default | no ] fqdn

<table>
<thead>
<tr>
<th>default</th>
</tr>
</thead>
</table>
| Returns the command to the default setting of “null”.

<table>
<thead>
<tr>
<th>no</th>
</tr>
</thead>
</table>
| Removes the configured FQDN from this service configuration.

<table>
<thead>
<tr>
<th>host domain_name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the domain name of the P-GW service.</td>
</tr>
<tr>
<td>domain_name must be an alphanumeric string of 1 through 255 characters.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>realm realm_name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the realm name of the P-GW service.</td>
</tr>
<tr>
<td>realm_name must be an alphanumeric string of 1 through 255 characters.</td>
</tr>
</tbody>
</table>

Usage
Use this command to identify the P-GW service using an FQDN required when sending messages over the S6b interface to a 3GPP AAA server.

Important: In order to properly interact with other nodes in the network, the FQDN should be less than or equal to 96 alphanumeric characters.
Topology Matching (eHRPD only)

You may specify which P-GW you wish an HSGW interface to connect with by enabling topology matching within the FQDNs for both the HSGW service and P-GW service. Topology matching selects geographically closer nodes and reduces backhaul traffic for a specified interface.

The following optional keywords enable or disable topology matching when added to the beginning of an FQDN:

- **topon.**`interface_name`
  
  Beginning an FQDN with topon initiates topology matching with available HSGWs in the network. Once this feature is enabled, the rest of the FQDN is processed from right to left until a matching regional designator is found on a corresponding HSGW FQDN.

- **topoff.**`interface_name`
  
  By default, topology matching is disabled. If you enable topology matching for any interfaces within a node, however, all interfaces not using this feature should be designated with topoff.

**Example**

The following command configures the FQDN for this P-GW service as 123abc.all.com with a realm name of all.com:

```plaintext
fqdn host 123abc.all.com realm all.com
```

The following command configures this P-GW service with an FQDN that enables topology matching:

```plaintext
fqdn host topon.interface_name.pgw01.bos.ma.node.epc
    .mnc<value>.mcc<value>.3gppnetwork.org realm
node.epc.mnc.mcc.3gppnetwork.org
```

**Important:** The associated HSGW service must have a corresponding FQDN similar to the following:

```plaintext
topon.interface_name.hsgw01.bos.ma.node.epc.mncvalue.mccvalue.3gppnetwork.org
```
gx-li

Refer to the *Lawful Intercept Configuration Guide* for a description of this command.
newcall

Configures the P-GW to accept or reject requests for a static IP address if the address is already in use by another session.

Product
P-GW
SAEGW

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > P-GW Service Configuration

```bash
configure > context context_name > pgw-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pgw-service)#
```

Syntax

```
newcall duplicate-subscriber-requested-address { accept | reject }

no newcall duplicate-subscriber-requested-address
```

no

Returns the command to the default setting of “reject”.

```
duplicate-subscriber-requested-address { accept | reject }
```

Default: reject
accept: Specifies that the old session with the requested address will be ended to accept the new session with the same address.
reject: Specifies that the new session requesting the same address will be rejected.

Usage

Use this command to configure the behavior of the P-GW service when receiving requests for static IP address already in use by other sessions.

Important: This command is only applicable to sessions using services supporting duplicate address abort. These services include HA, GGSN, and P-GW.

Example

The following command allows for the acceptance of requests for static IP addresses already in use by other sessions:

```
newcall duplicate-subscriber-requested-address accept
```
plmn

Configures Public Land Mobile Network identifiers used to determine if a mobile station is visiting, roaming, or belongs to this network.

Product
P-GW
SAEGW

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > P-GW Service Configuration
configure > context context_name > pgw-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pgw-service)#

Syntax

plmn id mcc number mnc number [ primary ]

<table>
<thead>
<tr>
<th>id mcc number mnc number</th>
</tr>
</thead>
<tbody>
<tr>
<td>mcc number: Specifies the mobile country code (MCC) portion of the PLMN identifier.</td>
</tr>
<tr>
<td>number is the PLMN MCC identifier and must be an integer from 100 through 999.</td>
</tr>
<tr>
<td>mnc number: Specifies the mobile network code (MNC) portion of the PLMN identifier.</td>
</tr>
<tr>
<td>number is the PLMN MNC identifier and can be configured to a 2- or 3-digit integer from 00 through 999.</td>
</tr>
</tbody>
</table>

primary

When multiple PLMN IDs are configured, the primary keyword can be used to designate one of the PLMN IDs to be used for the AAA attribute.

Usage

The PLMN identifier is used to aid the P-GW service in the determination of whether or not a mobile station is visiting, roaming, or home. Multiple P-GW services can be configured with the same PLMN identifier. Up to five PLMN IDs can be configured for each P-GW Service.

Example

The following command configures the PLMN identifier with an MCC of 462 and MNC of 02:

plmn id mcc 462 mnc 02
**session-delete-delay**

Configures a delay in terminating a session.

**Product**
- P-GW
- SAEGW

**Privilege**
- Administrator

**Mode**
- Exec > Global Configuration > Context Configuration > P-GW Service Configuration
- `configure > context context_name > pgw-service service_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-pgw-service)#
```

**Syntax**

```
session-delete-delay timeout [ msec ]
[ default | no ] session-delete-delay timeout
```

**Usage**

Use this command to set a delay to provide session continuity in break-before-make scenarios.

**Example**

The following command sets the session delete delay to the default setting of 10,000 milliseconds:

```
session-delete-delay timeout
```
setup-timeout

Configures the maximum amount of time the P-GW service takes for creating a session.

Product

P-GW

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > Context Configuration > P-GW Service Configuration

configure > context context_name > pgw-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-pgw-service)#

Syntax

setup-timeout setup_time

default setup-timeout

default

Configures the default guard timer value for session creation.

setup-time

Default: 60

Specifies the maximum amount of time taken by P-GW for service creation.

setup_time is measured in seconds and can be configured to an integer from 1 through 120.

Usage

Use this command to limit the amount of time allowed for creating a session. If a “Create Session Request” is received and the setup-timeout is configured, the timer starts with the configured value. If the setup timeout is not configured, the timer starts with the default value of 60 seconds.

Example

The following command allows a maximum of 120 seconds for creating a session:

setup-timeout 120
Chapter 254
Plugin Configuration Mode Commands

This chapter describes the commands available in the Plugin Configuration Mode. This mode is associated with the Dynamic Software Upgrade (DSU) process described in the System Administration Guide.

You enter this mode using the plugin command in the Global Configuration mode.

Mode

Exec > Global Configuration > Plugin Configuration
configure > plugin plugin_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-plugin-plugin_name)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
**attribute**

This command is not supported in this release.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Plugin Configuration

```bash
configure > plugin plugin_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-plugin-plugin_name)#
```

**Syntax**

```bash
attribute attribute_name attribute_value
```

**Usage**

The command is not supported in this release.
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
exit

**Usage**
Use this command to return to the parent configuration mode.
module priority

Configures the priority in the Version Priority List (VPL) for a specified version of a plugin module.

Product
ADC

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Plugin Configuration

configure > plugin plugin_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-plugin-plugin_name)#

Syntax

module priority number version plugin_version attribute attribute_name attribute_value

no module priority number

no

Removes the configured priority in the module priority list.

priority number

Specifies the priority of the plugin module as an integer from 1 through 100. Priority “1” has the highest priority.

version plugin_version

Specifies the version number of the plugin module. The version number is derived from the filename of the downloaded plugin.

attribute attribute_name attribute_value

Specifies an attribute value pair.
attribute_name specifies the name of an attribute value pair as an alphanumeric string from 1 through 255 characters.
attribute_value specifies the value of an attribute value pair as an alphanumeric string from 1 through 255 characters.

Usage

Assign a priority number to a specific version of patch for the corresponding plugin. The priority number in the module priority list determines which version will be loaded when the update module command is used.

The show plugin command displays the VPL configuration status of this plugin module.

Example
The following command sets the priority of p2p plugin module version 1.17.4340 to 2 where the filename was **libp2p-1.2.0.so.tgz**:

```
module priority 2 version 1.2.0
```
Chapter 255
Policy Control Configuration Mode Commands

Policy Control Configuration mode is used to configure the Diameter dictionary, origin host, host table entry and host selection algorithm for IMS Authorization service.

Mode
Exec > Global Configuration > Context Configuration > IMS Authorization Configuration > Policy Control Configuration

configure > context context_name > ims-auth-service service_name > policy-control

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-imsa-dpca)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
**apn-name-to-be-included**

This command configures the APN name to be included in CCR Gx messages.

**Product**
GGSN
IPSG
P-GW
SAEGW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > IMS Authorization Configuration > Policy Control Configuration
`configure > context context_name > ims-auth-service service_name > policy-control`

Entering the above command sequence results in the following prompt:
`[context_name]host_name(config-imsa-d pca)#`

**Syntax**

```
apn-name-to-be-included { gn | virtual }
default apn-name-to-be-included
```

`gn | virtual`
Specifies which APN name must be sent in the Gx messages.
`gn`: Specifies to send the real APN name.
`virtual`: Specifies to send the virtual APN name if present, else to send the real APN name.

`default`
Applies the default setting for this command.
Default: `gn`

**Usage**
This feature is developed to implement a single global APN for the Enterprise services with the ability to have separate virtual APNs per single Enterprise, group of Enterprises sharing the same service group or per department.

To implement this feature, a configurable option is introduced per interface Rf, Gx, Gy and per APN. That is, a service specific CLI "apn-name-to-be-included" is configured for interfaces Rf, Gx, Gy separately. It can take values ‘gn’ or ‘virtual’. Based on the value configured for this command, the Called-Station-Id AVP is populated.

This command is used to configure the APN name to be included in the CCR Gx messages to the PCRF — the real APN name or the virtual APN name.

The name of the virtual APN and the IP pool are signaled during the UE attach to the Enterprise PDN from the 3GPP AAA server over S6b interface with a new vendor-specific AVP “Virtual-APN-Name”. The
RADIUS Start, Gy CCR to OFCS and Rf ACR to OCS messages contain the Virtual APN name instead of the Enterprise APN. This feature provides customers the desired granularity per enterprise and per department. This also allows bundling of number of small enterprises under the umbrella of single APN and logically separating them by virtual APN.

**Example**

The following command configures sending the real APN name in Gx messages:

```
apn-name-to-be-included gn
```
arp-priority-level

This command enables mapping of the ARP priority-level value received from PCRF to inter-user-priority value and be sent in A11 session update.

Product
PDSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > IMS Authorization Configuration > Policy Control Configuration

configure > context context_name > ims-auth-service service_name > policy-control

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-imsa-dpca)#

Syntax

arp-priority-level map-to inter-user-priority

{ default | no } arp-priority-level map-to

  default
  Configures the default setting for this command.
  Default: arp-priority-level to inter-user-priority mapping not applicable

  no
  Disables arp-priority-level to inter-user-priority mapping.

Usage

Important: This command is for a customer-specific implementation to support IP-CAN policy control via Gx interface in PDSN, wherein the PCRF informs the subscriber’s subscription level (such as gold, silver, bronze) to PDSN/PCEF via Priority-Level AVP, then PDSN maps the subscriber’s subscription level to inter-user-priority and transmits it to PCF via A11 session update message. For more information on the use of this command contact your Cisco account representative.
associate

This command associates/disassociates a failure handling template or a local policy template with the IMS authorization service.

Product

GGSN
HA
HSGW
IPSG
PDSN
P-GW
SAEGW
S-GW

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > Context Configuration > IMS Authorization Configuration > Policy Control Configuration

configure > context context_name > ims-auth-service service_name > policy-control

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-imsa-dpca)#

Syntax

associate { failure-handling-template template_name | local-policy-service service_name }

no associate { failure-handling-template | local-policy-service }

no

Disassociates a failure handling template or local policy template with the IMS authorization service.

failure-handling-template template_name

Associates a previously created failure handling template with the IMS authorization service.

template_name specifies the name for a pre-configured failure handling template. template_name must be an alphanumeric string of 1 through 63 characters.

For more information on failure handling templates, refer to the failure-handling-template command in the Global Configuration Mode Commands chapter.

local-policy-service service_name

Associates a previously created local policy service with the IMS authorization service. service_name specifies the name for a pre-configured local policy service. service_name must be an alphanumeric string of 1 through 63 characters.
For more information on local policy service configuration, refer to the `local-policy-service` command in the *Global Configuration Mode Commands* chapter.

### Usage

Use this command to associate a configured failure handling template or local policy service with the IMS authorization service.

The failure handling template defines the action to be taken when the Diameter application encounters a failure supposing a result-code failure, tx-expiry or response-timeout. The application will take the action given by the template. For more information on failure handling template, refer to the *Failure Handling Template Configuration Mode Commands* chapter.

**Important:** Only one failure handling template can be associated with the IMS authorization service. The failure handling template should be configured prior to issuing this command.

If the association is not made to the template then failure handling behavior configured in the application with the `failure-handling` command will take effect.

To support fallback to local policy in case of failure at PCRF for CCFH continue, the local policy service should be associated with an IMS authorization service. In case of any failures, the local policy template associated with the ims-auth service will be chosen for fallback.

### Example

The following command associates a pre-configured failure handling template called `fht1` to the IMS authorization service:

```
associate failure-handling-template fht1
```
cc-profile

This command configures the value of the **Offline** AVP sent to the PCRF based on the Charging Characteristics (CC) profile received from the SGSN.

**Product**

GGSN

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > IMS Authorization Configuration > Policy Control Configuration

```bash
configure > context context_name > ims-auth-service service_name > policy-control
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-imsa-dpca)#
```

**Syntax**

```bash
cc-profile cc_profile_number [to cc_profile_number_range_end] map-to offline-avp { 0 | 1 }
{ default | no } cc-profile
```

<table>
<thead>
<tr>
<th><strong>Argument</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Configures the default setting for this command. Default: Deletes all previously configured mappings.</td>
</tr>
<tr>
<td>no</td>
<td>Deletes all previously configured mappings.</td>
</tr>
<tr>
<td>cc_profile_number</td>
<td>Specifies the CC profile number to map. For example, 1 for Hot Billing.</td>
</tr>
<tr>
<td>cc_profile_number_range_end</td>
<td>Specifies, for a range of CC profile numbers to map, the end number. That is, from cc_profile_number through cc_profile_number_range_end. cc_profile_number_range_end must be an integer from 1 through 15.</td>
</tr>
<tr>
<td>map-to offline-avp</td>
<td>Specifies to map the CC profile number(s) to the <strong>Offline</strong> AVP value sent to the PCRF.</td>
</tr>
</tbody>
</table>

- 0: Corresponds to the value DISABLE_OFFLINE (0).
- 1: Corresponds to the value ENABLE_OFFLINE (1).
Usage

Use this command to configure the CC Profile to Offline AVP value mapping. The Offline AVP’s value (DISABLE_OFFLINE (0), ENABLE_OFFLINE (1)) is derived based on the CC profile received from the SGSN as specified by this mapping.

The following example shows how this command can be configured multiple times:

```
cc-profile 1 to 2 map-to offline-avp 1
cc-profile 4 map-to offline-avp 0
cc-profile 8 map-to offline-avp 1
```

On configuring the above set of commands, the Offline AVP value is sent as 1 (Offline enabled) for the CC profiles 1 (Hot Billing), 2 (Flat Rate), and 8 (Post-Paid). And, as 0 (Offline disabled) for the CC profile 4 (Pre-paid).

When configuring this command, overlapping of CC profile numbers is not permitted. In the following example, after configuring the first command, which specifies to send the Offline AVP’s value as 1 (Offline enabled) for the CC profiles 1 through 15, the second command, which specifies to map CC profile 7, is not permitted:

```
cc-profile 1 to 15 map-to offline-avp 1
cc-profile 7 map-to offline-avp 0
```

Example

The following command specifies to send Offline AVP value as 1 (Offline enabled) for the CC profile 1 (Hot Billing):

```
cc-profile 1 map-to offline-avp 1
```

The following command specifies to delete all previously configured mappings:

```
no cc-profile
```
# custom-reauth-trigger

This command enables custom reauthorization event triggers.

## Product

All

## Privilege

Security Administrator, Administrator

## Mode

Exec > Global Configuration > Context Configuration > IMS Authorization Configuration > Policy Control Configuration

```bash
configure > context context_name > ims-auth-service service_name > policy-control
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-imsa-dpca)#
```

## Syntax

```
custom-reauth-trigger { none | { preservation-changed | reactivation-changed } + }
```

```bash
default custom-reauth-trigger
```

- **default**
  
  Configures the default setting for this command. The default setting is to enable all the event triggers.

- **none**
  
  Disables all custom event triggers.

- **preservation-changed**
  
  Enables preservation-changed event trigger.

- **reactivation-changed**
  
  Enables reactivation-changed event trigger.

**Important:** This keyword is for use with a customer-specific implementation, and will be available only if a valid license is installed.

- **reactivation-changed**
  
  Enables reactivation-changed event trigger.

**Important:** This keyword is for use with a customer-specific implementation, and will be available only if a valid license is installed.

## Usage

Use this command to enable/disable custom reauth event triggers.
It is recommended that the preservation-changed and reactivation-changed triggers both be enabled. As, when the bearer goes into preservation mode with the preservation-changed trigger, the reactivation-changed trigger must also be enabled for the bearer to get reactivated subsequently.

Example

The following command disables all custom event triggers:

```
custom-reauth-trigger none
```
diameter dictionary

This command specifies the Diameter Policy Control Application dictionary to be used by the IMS Authorization Service for the policy control application.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > IMS Authorization Configuration > Policy Control Configuration

configure > context context_name > ims-auth-service service_name > policy-control

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-imsa-dpca)#

Syntax


default diameter dictionary

---

dpca-custom1

Custom-defined Diameter dictionary for the Gx interface.

---

dpca-custom2

Custom-defined Diameter dictionary for Rel. 7 Gx interface.

---

dpca-custom3

Custom-defined Diameter dictionary for the Gx interface in conjunction with IP Services Gateway (IPSG).

---

dpca-custom4

Standard Diameter dictionary for 3GPP Rel. 7 Gx interface.

---

dpca-custom5

Custom-defined Diameter dictionary for Rel. 7 Gx interface.

---

dpca-custom6 ... dpca-custom30

Custom-defined Diameter dictionaries.
diameter dictionary

Configures the dynamically loaded Diameter dictionary. The dictionary name must be an alphanumeric string of 1 through 15 characters.
For more information on dynamic loading of Diameter dictionaries, see the \textit{diameter dynamic-dictionary} in the \textit{Global Configuration Mode Commands} chapter of this guide.

gx-wimax-standard
Gx WiMAX standard dictionary.

gxa-3gpp2-standard
Gxa 3GPP2 standard dictionary.

gxc-standard
Gxc standard dictionary.

pdsn-ty
This keyword is restricted.

r8-gx-standard
R8 Gx standard dictionary.

Standard
Standard Diameter dictionary for the 3GPP Rel. 6 Gx interface.
Default: Enabled for Gx support in 3GPP networks.

std-pdsn-ty
This keyword is restricted.

ty-plus
This keyword is restricted.

ty-standard
This keyword is restricted.

default
Sets the default Diameter dictionary.
Default: Standard

Usage
Use this command to specify the Diameter dictionary for IMS Authorization Service.

Example
The following command sets the \texttt{Standard} dictionary for Diameter Policy Control functions in 3GPP network:

\begin{verbatim}
diameter dictionary Standard
\end{verbatim}
diameter encode-event-avps

This command enables encoding of all the event-related information AVPs in CCR-U messages.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > IMS Authorization Configuration > Policy Control Configuration

```
configure > context context_name > ims-auth-service service_name > policy-control
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-imsa-dpca)#
```

**Syntax**

```
[ default ] diameter encode-event-avps { always | local-fallback }
```

- **default**
  
  Applies the default setting for this command.
  
  Default: Sends AVPs relevant to the Event-Trigger subscribed by the PCRF.

- **always**
  
  This keyword option always sends the event-related AVPs in all CCR messages.

- **local-fallback**
  
  This keyword option sends the event-related AVPs in CCR-U messages in the event of local fallback scenario.

**Usage**

Use this command to facilitate sending of all the event-related information AVPs in CCR-U messages. In releases prior to 14.0, per the 3GPP standards for Gx, AVPs relevant to the Event-Trigger subscribed by the PCRF were always sent in the CCR messages. This release onwards, sending of event-related AVPs for all update (both access side and internal) and terminate requests is CLI controlled. Note that the QoS-Info AVP will be encoded in all CCR messages if the CLI command “diameter encode-event-avps always” is enabled. This implementation impacts only the dpca-custom15 dictionary.

**Example**

The following command enables to always send the event-related AVPs in all CCR messages:

```
diameter encode-event-avps always
```
**diameter encode-supported-features**

This command enables/disables encoding and sending of Supported-Features AVP.

**Product**

GGSN
P-GW

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > IMS Authorization Configuration > Policy Control Configuration

```shell
configure > context context_name > ims-auth-service service_name > policy-control
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-imsa-dpca)#
```

**Syntax**

```
diameter encode-supported-features sponsored-connectivity

{ default | no } diameter encode-supported-features
```

- **sponsored-connectivity**

  Enables the Sponsored (data) Connectivity feature.
  With sponsored data connectivity, the sponsor has a business relationship with the operator and the sponsor reimburses the operator for the user's data connectivity in order to allow the user access to an associated Application Service Provider's (ASP) services. Alternatively, the user pays for the connectivity with a transaction which is separate from the subscriber's charging. It is assumed the user already has a subscription with the operator.
  The purpose of this feature is to identify the data consumption for a certain set of flows differently and charge it to sponsor. To support this, a new reporting level “SPONSORED_CONNECTIVITY_LEVEL” is added for reporting at Sponsor Connection level and two new AVPs “Sponsor-Identity” and “Application-Service-Provider-Identity” have been introduced at the rule level.
  This CLI command “diameter encode-supported-features” has been added in Policy Control Configuration mode to send Supported-Features AVP with Sponsor Identity.
  Sponsored Connectivity feature will be supported only when both P-GW and PCRF support 3GPP Rel. 10. P-GW advertises release as a part of supported features in CCR-I to PCRF. If P-GW supports Release 10 and also Sponsored Connectivity but PCRF does not support it (as a part of supported features in CCA-I), this feature is turned off.
  This feature implementation impacts only the Gx dictionary “dpca-custom15”.

- **default | no**

  This keyword removes the previously configured supported features.

**Usage**

This command is used to enable encoding and sending of Supported-Features AVP.
diameter host-select reselect

This command controls pacing of the reselection or switching of the PCRF after a change occurs in the table configuration for an IMS Authorization Service.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > IMS Authorization Configuration > Policy Control Configuration

```plaintext
configure > context context_name > ims-auth-service service_name > policy-control
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-imsa-dpca)#
```

**Syntax**

```plaintext
diameter host-select reselect subscriber-limit subs_limit time-interval duration
```

```plaintext
{ default | no } diameter host-select reselect
```

### subscriber-limit subs_limit

Specifies the limit of subscribers to switch or reselect the PCRF for subscribers not more than `subs_limit` in time duration of `duration` second(s).

- `subs_limit` must be an integer from 1 through 1000000.

### time-interval duration

Specifies the time duration, in seconds, to reselect PCRF for subscribers not more than `subs_limit` in time duration of `duration` second(s).

- `duration` must be an integer from 1 through 3600.

### default

Applies the default setting for this command.

Sets the PCRF reselection or switching to default state.

### no

Removes the configured PCRF reselection method and disables the reselection or switching of PCRF.

**Usage**

Use this command to specify the pacing of reselection or switching of the PCRF in an IMS authorization service..

In case IMS authorization session have been opened on certain PCRF on the basis of the current selection table, and the current active table configuration is changed, the IMSA starts selection procedure for the PCRF. Existing sessions on current PCRF from earlier table is required to close and reopened on the selected
PCRF from the new table. This reselection periodicity is controlled by this command and it indicates the number of subscriber sessions `subs_limit` to be reselected or moved in `duration` seconds.
For example, if this command is configured with 100 subscribers and 2 seconds, then the system reselects the PCRF for no more than 100 subscribers per 2 seconds.

Example

The following command sets the system to reselect the new PCRF for no more than 1000 subscriber in 15 seconds:

```
diameter host-select reselect subscriber-limit 1000 time-interval 15
```
diameter host-select row-precedence

This command adds/appends rows with precedence to a Diameter host table or MSISDN prefix range table.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > IMS Authorization Configuration > Policy Control Configuration
configure > context context_name > ims-auth-service service_name > policy-control

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-imsa-dpca)#

Syntax

diameter host-select row-precedence precedence_value table { { { 1 | 2 } host host_name [ realm realm_id ] [ secondary host host_name [ realm realm_id ] ] } | { prefix-table { 1 | 2 } msisdn-prefix-from msisdn-prefix_from msisdn-prefix-to msisdn_prefix_to host host_name [ realm realm_id ] [ secondary host sec_host_name [ realm sec_realm_id ] algorithm { active-standby | round-robin } ] } } [ -noconfirm ]

no diameter host-select row-precedence precedence_value table { { 1 | 2 } | prefix-table { 1 | 2 } }

diameter host-select row-precedence precedence_value table { { 1 | 2 } host host_name [ realm realm_id ] [ secondary host sec_host_name [ realm sec_realm_id ] ] }

This command adds/appends a row in the specified Diameter host table.

In 8.0, a maximum of 16 rows can be added to a table. In 8.1 and later releases, a maximum of 128 rows can be added per table.

row-precedence precedence_value: Specifies precedence of the row in the Diameter host table.

Important: In 8.1 and later releases, precedence_value must be an integer from 1 through 128. In 8.0 and previous releases, precedence_value must be an integer from 1 through 100.

table { 1 | 2 }: Specifies the Diameter host table to add/append the primary and secondary Diameter host addresses.
host host_name: Specifies the primary host name. host_name must be an alphanumeric string of 1 through 127 characters in length.
realm realm_id: Specifies the primary realm ID. realm_id must be an alphanumeric string of 1 through 127 characters in length.
secondary host sec_host_name [ realm sec_realm_id ]: Specifies the secondary host name and realm ID:
host sec_host_name: Specifies the secondary host name. host_name must be an alphanumeric string of 1 through 127 characters in length.
**Policy Control Configuration Mode Commands**

**diameter host-select row-precedence**

```plaintext
realm sec Realm_id: Specifies the secondary realm ID. realm_name must be an alphanumeric string of 1 through 127 characters in length.
```

```plaintext
no diameter host-select row-precedence precedence_value table prefix-table { 1 | 2 }
```

Removes the row with the specified precedence from the specified MSISDN prefix range table.

```plaintext
diameter host-select row-precedence precedence_value table prefix-table { 1 | 2 }
msisdn-prefix-from msisdn_prefix_from msisdn-prefix-to msisdn_prefix_to host
host_name [ realm realm_id ] [ secondary host sec_host_name [ realm sec Realm_id ]
algorithm { active-standby | round-robin } ] [ -noconfirm ]
```

Use this command to configure the MSISDN prefix range based PCRF selection mechanism for Rel. 7 Gx interface support, wherein the PCEF is required to discover and select an appropriate PCRF to establish control relationship at primary PDP context activation.

This command adds a row in the specified MSISDN prefix range table. A maximum of 128 rows can be added per prefix range table.

```plaintext
row-precedence precedence_value: Specifies precedence of the row in the table.
```

**Important:** In 8.1 and later releases, precedence_value must be an integer from 1 through 128. In 8.0 and previous releases, precedence_value must be an integer from 1 through 100.

```plaintext
prefix-table { 1 | 2 }: Specifies the MSISDN prefix range table to add the primary and/or secondary Diameter host addresses.
msisdn-prefix-from msisdn_prefix_from: For a range of MSISDNs, specifies the starting MSISDN.
msisdn-prefix-to msisdn_prefix_to: For a range of MSISDNs, specifies the ending MSISDN.
```

**Important:** To enable the Gx interface to connect to a specific PCRF for a range of MSISDNs/subscribers configure msisdn prefix from and msisdn prefix to with the starting and ending MSISDNs respectively. The MSISDN ranges must not overlap between rows. To enable the Gx interface to connect to a specific PCRF for a specific MSISDN/subscriber, configure both msisdn prefix from and msisdn prefix to with the same MSISDN.

```plaintext
host host_name: Specifies the primary host name. host_name must be an alphanumeric string of 1 through 127 characters in length.
realm realm_id: Specifies the primary realm ID. realm_id must be an alphanumeric string of 1 through 127 characters in length.
secondary host sec_host_name [ realm sec Realm_id ]: Specifies the secondary host name and realm ID: host sec_host_name: Specifies the secondary host name. sec_host_name must be an alphanumeric string of 1 through 127 characters in length.
realm sec Realm_id: Specifies the secondary realm ID. sec Realm_id must be an alphanumeric string of 1 through 127 characters in length.
algorithm { active-standby | round-robin }: Specifies the algorithm for selection between primary and secondary servers in the MSISDN prefix range table.
Default: active-standby
active-standby: Specifies selection of servers in the Active-Standby fashion.
round-robin: Specifies selection of servers in the Round-Robin fashion.
```

**Important:** The Round Robin algorithm for PCRF selection is effective only over a large number of PCRF selections, and not at a granular level.
no diameter host-select row-precedence precedence_value table { 1 | 2 }
Removes the row with the specified precedence from the specified Diameter host table.

Usage
Use this command to add, update, or delete rows specified with a precedence from a Diameter host table or MSISDN prefix range table.
In the Rel. 7 Gx implementation, when the Gateway interworks with multiple PCRFs, the Gateway can configure the primary and secondary server based on the MSISDN-prefix range in the MSISDN prefix range table. Using this command, you can add a new prefix row into the MSISDN prefix table.
If a row with the precedence that you add already exists in a table, the existing prefix row is removed and the new row is inserted with the same precedence.

Example
The following command adds a row with precedence 12 in table 2 with primary host name as star_ims1 and secondary host name as star_ims2 to Diameter host table.

diameter host-select row-precedence 12 table 2 host star_ims1 secondary host star_ims2
diameter host-select table

This command selects the Diameter host table or the MSISDN prefix range table, and the algorithm to select rows from the Diameter host table.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > IMS Authorization Configuration > Policy Control Configuration

configure > context context_name > ims-auth-service service_name > policy-control

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-imsa-dpca)#

Syntax

diameter host-select table { { 1 | 2 } algorithm { ip-address-modulus [ prefer-ipv4 | prefer-ipv6 ] | msisdn-modulus | round-robin } | prefix-table { 1 | 2 } }

{ default | no } diameter host-select table

diameter host-select table { 1 | 2 } algorithm { ip-address-modulus | msisdn-modulus | round-robin }
table { 1 | 2 }: Specifies the Diameter host table to obtain the primary and secondary host names for PCRF.
algorithm { ip-address-modulus [ prefer-ipv4 | prefer-ipv6 ] | msisdn-modulus | round-robin }: Specifies the algorithm to select row from the Diameter host table.
Default: round-robin
•ip-address-modulus [ prefer-ipv4 | prefer-ipv6 ]: This algorithm divides the IP address, in binary, of the subscriber by the number of rows in the table, and the remainder is used as an index into the specified table to select the row.
•prefer-ipv4: Specifies that IPv4 addresses are to be used, if an IPv4v6 call is received, for selecting the rows in the host table.
•prefer-ipv6: Specifies that IPv6 addresses are to be used, if an IPv4v6 call is received, for selecting the rows in the host table.
•msisdn-modulus: This algorithm divides the MSISDN value in binary without the leading “+” of the subscriber by the number of rows in the table, and the remainder is used as an index in the specific table to select the row.
•round-robin: This algorithm rotates all rows in the active table for selection of the row in round-robin fashion. If no algorithm is specified this is the default behavior.

**Important:** The Round Robin algorithm is effective only over a large number of selections, and not at a granular level.
diameter host-select table prefix-table { 1 | 2 }

Specifies the MSISDN Prefix Range table to be used in case of MSISDN prefix range based PCRF discovery mechanism.

**default**

Applies the default setting for this command.

**no**

Removes previous configuration.

When no table is selected, the system will not communicate with any PCRF for new sessions.

**Usage**

Use this command to configure the Diameter host table and row selection methods to select host name or realm for PCRF.

When this command is used to change which table the system should be using, user must re-determine which E-PDF the system should be using for each subscriber. If a different E-PDF results from the configuration change in the table, the system will wait for all of the IMS sessions for the subscriber to be no longer active and then the system either closes/opens Gx sessions with the old/new PDFs respectively, or the system deactivates the PDP contexts of the subscriber.

Here is an example of how row selection is configured for three hosts that the system will use for load-balancing. Operator can configure six rows in a table, as follows.

<table>
<thead>
<tr>
<th>Modulo 6</th>
<th>Primary Host</th>
<th>Secondary Host</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>5</td>
<td>3</td>
<td>2</td>
</tr>
</tbody>
</table>

In the above table, the three hosts are named 1, 2, and 3. When all hosts are working, the load will be distributed among all the three hosts. If host 1 fails, then the load will be distributed between the remaining two hosts. In this scenario, the modulo 6 results of 2 and 4 will return rows that have primary hosts but no working back-up host.

In the Rel. 7 Gx implementation, the GGSN/PCEF is required to discover and select an appropriate PCRF to establish control relationship at primary PDP context activation. The ip-address-modulus, msisdn-modulus, and round-robin algorithms are supported by the GGSN/PCEF for PCRF discovery. In addition, the active/standby and round-robin algorithms are used for selection between primary and secondary servers based on the MSISDN Prefix Range Table.

**Example**

The following command specifies **table 1** with **round-robin** algorithm to select the rows with host name for E-PDF in Diameter host table.

```
diameter host-select table 1 algorithm round-robin
```
diameter host-select-template

This command specifies the Diameter host server template to be associated with this IMS Authorization service. The service uses the specified template (and associated host-select table) to select a Diameter peer server. It then uses the returned host name(s) to contact the PCRF and establish the call.

Product
GGSN
HA
HSGW
IPSG
PDSN
P-GW
SAEGW
S-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > IMS Authorization Configuration > Policy Control Configuration

configure > context context_name > ims-auth-service service_name > policy-control

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-imsa-d pca)#

Syntax

diameter host-select-template tmplt_name

no diameter host-select-template

no

Removes the binding of the Diameter host select template with the IMS Authorization service.

__tmplt_name__

Specifies the name of an existing Diameter host server template (configured in Global Configuration mode) to bind with the IMS Authorization service. It is an alphanumeric string of 1 through 255 characters.

Usage

Use this command to bind a configured Diameter host select template to the IMS Authorization service for DPCA. This IMS authorization service searches the associated host select table to select a Diameter peer server. For additional information refer to the Diameter Host Select Configuration Mode Commands chapter and the description of the diameter-host-template command in the Global Configuration Mode Commands chapter.
Important: Prior to issuing this command, the Diameter host select template should be configured using the `diameter-host-template` command in the Global Configuration mode.

Important: If no association is made to the template then the `diameter peer-select` command configured at the application level will be used for peer selection.

Example

The following command binds a configured Diameter host select template named `diamtemplate` to the IMS authorization service:

```
diameter host-select-template diamtemplate
```
diameter map

This command enables selecting the value to which the USAGE_REPORT and APN_AMBR_MOD_FAILURE Event-Trigger should be mapped to.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > IMS Authorization Configuration > Policy Control Configuration

```bash
configure > context context_name > ims-auth-service service_name > policy-control
```

Entering the above command sequence results in the following prompt:

```
[context_name] host_name(config-imsa-dpca)#
```

**Syntax**

```bash
diameter map usage-report { 29 | 26 | 33 }
default diameter map usage-report
```

Maps the USAGE_REPORT of Event-Trigger AVP to one or a combination of these values.

- 26 – Event-Trigger 26 will mapped to USAGE_REPORT. Note this will not affect any other Event-Trigger.
- 29 – Event-Trigger 29 will mapped to USAGE_REPORT, and 33 to APN_AMBR_MOD_FAILURE.
- 33 – Event-Trigger 33 will mapped to USAGE_REPORT, and 29 to APN_AMBR_MOD_FAILURE.

**default**

The default behavior is to configure the Event-Trigger USAGE_REPORT to be mapped to 26.

**Usage**

The Event-Trigger AVP’s USAGE_REPORT has been given different values in the 3GPP TS 29.212 standard spec. As a result of that, the releases of TS 29.212 are not backward compatible. To address this, this CLI command has been introduced in Policy Control configuration mode to map the USAGE_REPORT to either 26/29/33 in order to be flexible enough to interoperate with various operators.

- TS 29.212 v9.5.0 - USAGE_REPORT (26)
- TS 29.212 v9.6.0 - USAGE_REPORT (29)
- TS 29.212 v9.7.0 - USAGE_REPORT (33)

If this CLI command `diameter map usage-report 29` is configured in the chassis and PCRF sends 29 event-trigger then on volume threshold breach CCR-U with volume-report and event-trigger 29 will be sent to the PCRF. Same is the case with the values 26 and 33.
Example

The following command maps the Event-Trigger USAGE_REPORT to 29 and APN_AMBR_MOD_FAILURE to 33:

```
diameter map usage-report 29
```
**diameter origin endpoint**

This command binds the origin endpoint configured in Context Configuration mode to the IMS Authorization service for Diameter Policy Control Application (DPCA).

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > IMS Authorization Configuration > Policy Control Configuration

```
configure > context context_name > ims-auth-service service_name > policy-control
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-imsa-dpca)#
```

**Syntax**

```
diameter origin endpoint endpoint_name

no diameter origin
```

`endpoint endpoint_name`

`endpoint_name` is the Diameter endpoint configured in Context Configuration Mode to bind with IMS authorization service, and must be an alpha/numeric string of 1 through 63 characters in length.

```
no
```

Removes the binding of Diameter origin endpoint with IMS Authorization service.

**Usage**

Use this command to bind a configured Diameter origin endpoint to the IMS Authorization service for DPCA. This IMS authorization service searches all system contexts until it finds one with a matching Diameter origin endpoint name specified.

**Example**

The following command binds a configured endpoint named test to the IMS authorization service:

```
diameter origin endpoint test
```
**diameter request-timeout**

This command configures the request-timeout setting for Diameter-IMSA Gx interface.

**Product**

GGSN  
P-GW  
SAEGW

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > IMS Authorization Configuration > Policy Control Configuration  
\texttt{configure > context \ context_name > ims-auth-service \ service_name > policy-control}

Entering the above command sequence results in the following prompt:

\texttt{[context_name]host_name(config-imsa-dpca)\#}

**Syntax**

\texttt{diameter request-timeout \ timeout}

\texttt{default \ diameter request-timeout}

\begin{verbatim}
timeout
\end{verbatim}

Specifies the timeout duration (in seconds). The value must be an integer from 1 through 300. Default: 10 seconds

\begin{verbatim}
default
\end{verbatim}

Applies the default setting for this command.

**Usage**

Use this command to configure the request-timeout setting for Diameter-IMSA Gx interface. At the request-timeout value, DPCA will apply failure-handling to the subscriber. Action will be taken based on the failure-handling configuration (terminate/retry-terminate/continue).

**Example**

The following command configures the Diameter request-timeout setting to 20 seconds:

\texttt{diameter request-timeout 20}
diameter update-dictionary-avps

This command enables dictionary control of the AVPs that need to be added based on the version of the specification to which the PCEF is compliant with.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > IMS Authorization Configuration > Policy Control Configuration

configure > context context_name > ims-auth-service service_name > policy-control

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-imsa-dpca)#

Syntax

diameter update-dictionary avps { 3gpp-r8 | 3gpp-r9 | 3gpp-r10 }

{ default | no } diameter update-dictionary avps

default | no

Configures this command with the default setting.
The default behavior is that R9 support will not be indicated as part of Supported-Features AVP in a R7/R8 dictionary and R8 support will not be indicated as part of Supported-Features AVP in a R7 dictionary.

3gpp-r8
Specifies to select the 3GPP Rel. 8 AVPs for encoding.

3gpp-r9
Specifies to select the 3GPP Rel. 9 AVPs for encoding.

3gpp-r10
Specifies to select the 3GPP Rel. 10 AVPs for encoding.

Usage

Important: This command is applicable only to Diameter dictionaries that support standard based volume reporting over Gx feature.

Use this command to encode the AVPs in the dictionary based on the release version of the specification to which the PCEF is compliant with.
Release 12.0 onwards, if a 3GPP Rel. 7 based dictionary is already configured with diameter dictionary dpca-custom4 command, and then if the diameter update-dictionary-avps 3gpp-r9 command is
applied, the Supported-Features AVP with feature bit 1 being set will be sent in the CCR-I to indicate that 3GPP Rel. 9 AVPs are also supported.

Both default and no command have the same behavior, as if the CLI command is not configured. Hence, in the output of show configuration verbose command, the default and no command is shown as no diameter update-dictionary-avps.

This CLI command when configured results in behavioral changes as indicated in the following table.

<table>
<thead>
<tr>
<th>Possible Upgrade Scenarios</th>
<th>Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>3GPP Rel. 7 based dictionary upgraded to 3GPP Rel. 9&lt;br&gt;For example:&lt;br&gt;<strong>diameter dictionary dpca-custom4 diameter update-dictionary-avps 3gpp-r9</strong></td>
<td>In the CCR-I, Supported-Features AVP will be encoded with value 2 for the Feature-List AVP.&lt;br&gt;[$V$] [$M$] Supported-Features:&lt;br&gt;[$M$] Vendor-Id: 10415&lt;br&gt;[$V$] [$M$] Feature-List-ID: 1&lt;br&gt;[$V$] [$M$] Feature-List: 2&lt;br&gt;The Feature-List AVP value suggest that it is 3GPP Rel. 9 compliant. But, it is not fully compliant to 3GPP Rel. 9.&lt;br&gt;In the current release, for this upgrade scenario (3GPP Rel. 7 to 3GPP Rel. 9), only volume reporting related AVPs mentioned in the 3GPP Rel. 9 will be supported.</td>
</tr>
<tr>
<td>3GPP Rel. 7 based dictionary upgraded to 3GPP Rel. 8&lt;br&gt;For example:&lt;br&gt;<strong>diameter dictionary dpca-custom4 diameter update-dictionary-avps 3gpp-r8</strong></td>
<td>In the CCR-I, Supported-Features AVP will be encoded with value 1 for the Feature-List AVP.&lt;br&gt;[$V$] [$M$] Supported-Features:&lt;br&gt;[$M$] Vendor-Id: 10415&lt;br&gt;[$V$] [$M$] Feature-List-ID: 1&lt;br&gt;[$V$] [$M$] Feature-List: 1&lt;br&gt;The Feature-List AVP value suggest that it is 3GPP Rel. 8 compliant. But, it is not fully compliant to 3GPP Rel. 8.&lt;br&gt;In the current release, for this upgrade scenario (3GPP Rel. 7 to 3GPP Rel. 8), none of the features mentioned in 3GPP Rel. 8 will be supported.</td>
</tr>
<tr>
<td>3GPP Rel. 8 based dictionary upgraded to 3GPP Rel. 9&lt;br&gt;For example:&lt;br&gt;<strong>diameter dictionary r8-gx-standard diameter update-dictionary-avps 3gpp-r9</strong></td>
<td>In the CCR-I, value for the Feature-List AVP in the Supported-Features AVP will be 2.&lt;br&gt;[$V$] [$M$] Supported-Features:&lt;br&gt;[$M$] Vendor-Id: 10415&lt;br&gt;[$V$] [$M$] Feature-List-ID: 1&lt;br&gt;[$V$] [$M$] Feature-List: 2&lt;br&gt;The Feature-List AVP value suggest that it is 3GPP Rel. 9 compliant. But, it is not fully compliant to 3GPP Rel. 9.&lt;br&gt;Currently for this upgrade scenario (3GPP Rel. 8 to 3GPP Rel. 9), only volume reporting related AVPs mentioned in 3GPP Rel. 9 will be supported.</td>
</tr>
<tr>
<td>3GPP Rel. 9 based dictionary upgraded to 3GPP Rel. 10&lt;br&gt;For example:&lt;br&gt;<strong>diameter dictionary r8-gx-standard diameter update-dictionary-avps 3gpp-r10</strong></td>
<td>In the CCR-I, value for the Feature-List AVP in the Supported-Features AVP will be 8.&lt;br&gt;[$V$] [$M$] Supported-Features:&lt;br&gt;[$M$] Vendor-Id: 10415&lt;br&gt;[$V$] [$M$] Feature-List-ID: 1&lt;br&gt;[$V$] [$M$] Feature-List: 8&lt;br&gt;The Feature-List AVP value suggest that it is 3GPP Rel. 10 compliant. But, it is not fully compliant to 3GPP Rel. 10.</td>
</tr>
</tbody>
</table>

In 14.1 and later releases, Supported-Features AVP is extended to support 3GPP Rel. 10 in EPS 3.0 in addition to 3GPP Rel. 8 and Rel. 9. If the **diameter update-dictionary-avps 3gpp-r10** command is applied, the Supported-Features AVP with feature bit 1 being set will be sent in the CCR-I / CCA to indicate that 3GPP Rel. 10 AVPs are also supported. The 'M' bit setting for the Feature-List AVP and Feature-List-ID AVP must be the same as defined in 3GPP TS 29.229 and must not be affected by the 'M' bit setting of the Supported-Features AVP.

Example
The following command enables encoding of AVPs in the dictionary based on 3GPP Rel. 9:

```
diameter update-dictionary-avps 3gpp-r9
```
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**
Use this command to return to the Exec mode.
endpoint-peer-select

This command enables Diabase to select the Diameter peers in all failure scenarios.

Product
- GGSN
- PGW

Privilege
- Security Administrator, Administrator

Mode
- Exec > Global Configuration > Context Configuration > IMS Authorization Configuration > Policy Control Configuration
  - configure > context context_name > ims-auth-service service_name > policy-control

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-imsa-dpca)#

Syntax

endpoint-peer-select [ on-host-select-failure | on-inactive-host ]

{ default | no } endpoint-peer-select

- on-host-select-failure
  Specifies to perform server selection at Diabase when the hosts could not be selected by IMS Authorization application.

- on-inactive-host
  Specifies to perform server selection at diabase when the hosts selected by application are inactive.

{ default | no }
Default/no behavior is to terminate the call when the hosts could not be selected by application or when the hosts selected by application are inactive.

Usage

Use this command to perform server selection at Diabase when the hosts could not be selected by application or when the hosts selected by the IMS Authorization application is inactive. For example, host table is not configured in IMSA service, host table is configured but not activated, none of the rows in prefix table match the subscriber, host template is not associated with IMSA service, host template could not select the hosts. This CLI command is added in policy control configuration mode to maintain backward compatibility with the old behavior of terminating the call when server selection fails at application.

Example

The following command enables Diabase to select peers when the hosts selected by application are inactive.

endpoint-peer-select on-inactive-host
event-report-indication

This command enables event report indication.

Product
P-GW
SAEGW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > IMS Authorization Configuration > Policy Control Configuration

configure > context context_name > ims-auth-service service_name > policy-control

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-imsa-dpca)#

Syntax

event-report-indication { all | pgw-trace-control | qos-change | rai-change | rat-change
| sgsn-change | ue-timezone-change | user-loc-change } [ pgw-trace-control ] [ qos-change
] [ rai-change ] [ rat-change ] [ sgsn-change ] [ ue-timezone-change ] [ user-loc-change ]

{ default | no } event-report-indication

all | pgw-trace-control | qos-change | rai-change | rat-change | sgsn-change |
ue-timezone-change | user-loc-change

 Specifies which types of changes will trigger an event report from the PCRF.
• all: all triggers
• pgw-trace-control: P-GW trace control change trigger
• qos-change: QoS change trigger
• rai-change: RAI change trigger
• rat-change: RAT change trigger
• sgsn-change: SGSN change trigger
• ue-timezone-change: UE time zone change trigger
• user-loc-change: User location change trigger

default | no

Disables event report indication.

Usage
Use this command to determine what type of event changes are reported from the PCRF.

Example
The following command enables event report indication for all triggers.

```
event-report-indication all
```
event-update

This command configures sending usage monitoring information in event updates either for all event triggers or for a specific event trigger.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > IMS Authorization Configuration > Policy Control Configuration

configure > context context_name > ims-auth-service service_name > policy-control

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-imsa-dpca)#

Syntax


{ default | no } event-update

default
Configures the default setting for this command.
Default: Usage report is not sent in event update.

no
Disables sending usage report in event update.

reset-usage
Resets the usage at PCEF after reporting in event update.


Sends the custom usage report based on the following event triggers:
- an-gw-change — AN GW change event trigger
• apn-ambr-mod-failure — APN AMBR Modification Failure event trigger
• bearer-loss — Loss of bearer trigger
• bearer-rcvry — Recovery of bearer trigger
• charging-correlation-exchange — Charging Correlation Exchange trigger
• default-bearer-qos-change — Default EPS bearer QoS change event trigger
• default-bearer-qos-mod-failure — Default EPS Bearer QOS Modification Failure event trigger
• ip-can-change — IP-CAN Change trigger
• out-of-credit — Out of credit trigger
• pgw-trace-control — P-GW Trace Control
• plmn-change — PLMN change trigger
• qos-change — QoS change trigger
• qos-excess-change — QoS Change Exceeding Authorization trigger
• rai-change — RAI Change trigger
• rat-change — RAT change trigger
• reallocation-of-credit — Reallocation of credit trigger
• resource-modification-request — Resource modification trigger
• revalidation-timeout — Revalidation timeout trigger
• sgsn-change — SGSN change trigger
• successful-resource-alloc — Successful Resource Allocation event trigger
• tft-change — TFT change trigger
• ue-ip-addr-allocate — UE IP address allocate trigger
• ue-ip-addr-release — UE IP address release trigger
• ue-timezone-change — UE Time Zone Change event trigger
• user-loc-change — User Location Change trigger

Usage
Use this command to send volume usage information when an event change is reported to the PCRF in a CCR-U message.
To send customized usage information based on specific event triggers, the event should be accordingly configured with the `event-update send-usage-report events` command. For example, if the usage report is required whenever RAT change occurs, this can be accomplished using the `event-update send-usage-report events rat-change` command.

Example
The following command specifies to send volume usage report in event updates to the PCRF for all event triggers:

```
event-update send-usage-report reset-usage
```

The following command specifies to send volume usage report in event updates to the PCRF for RAT change scenarios:

```
event-update send-usage-report reset-usage events rat-change
```
The following command specifies to send volume usage report in event updates to the PCRF if either RAT change or QOS change occurs:

```
event-update send-usage-report reset-usage events rat-change qos-change
```
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Use this command to return to the parent configuration mode.
failure-handling

This command configures Diameter failure handling behavior.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > IMS Authorization Configuration > Policy Control Configuration

```plaintext
configure > context context_name > ims-auth-service service_name > policy-control
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-imsa-dpca)#
```

**Syntax**

In Release 8.0:

```plaintext
failure-handling { continue | retry-and-terminate | terminate | diameter-result-code { any-error | result_code } ccfh { continue | retry-and-terminate | terminate } [ cc-request-type { initial-request | terminate-request | update-request } ] }

no failure-handling diameter-result-code { any-error | integer result_code } [ cc-request-type { initial-request | terminate-request | update-request } ]
```

In 8.1 and later releases:

```plaintext
failure-handling cc-request-type { any-request | initial-request | terminate-request | update-request } [ diameter-result-code { any-error | result_code [ to end_result_code ] } ] [ continue [ retry-server-on-event | send-ccrt-on-call-termination ] | retry-and-terminate | terminate ]

no failure-handling cc-request-type { any-request | initial-request | terminate-request | update-request } [ diameter-result-code { any-error | result_code [ to end_result_code ] } ] [ continue [ send-ccrt-on-call-termination ] ]
```

---

**no**
Disables previous failure-handling configuration.

---

**retry-and-terminate**

Specifies that in the event of a failure the user session continues for the duration of one retry attempt with the server. If this retry attempt also fails, the session is terminated.

---

**terminate**

Specifies that in the event of a failure the user session be terminated.
Policy Control Configuration Mode Commands

---

**diameter-result-code** { any-error | result_code [ to end_result_code ] }

Specifies failure handling behavior for any/specific result-code(s) to identify the type of failure and failure handling action for specific credit control request type.
- **any-error**: Specifies failure handling behavior for those result-codes for which failure-handling behavior has not been specified.
- **result_code**: Specifies a Diameter failure result code. `result_code` is the code returned for a failure handling action and must be an integer from 3000 through 4999.
- **to end_result_code**: Use to specify a range of Diameter failure result codes. `end_result_code` must be an integer from 3000 through 4999, and must be greater than `result_code`.

---

**continue** [ retry-server-on-event | send-ccrt-on-call-termination ] | retry-and-terminate | terminate

**As in 8.1 and later releases:**

Specifies the credit control failure handling action.
- **continue**: In the event of a failure the user session continues. DPCA/Diameter will make periodic request and/or connection retry attempts and/or will attempt to communicate with a secondary peer depending on the peer config and session-binding setting.
- **retry-server-on-event**: This optional keyword enables reconnecting with PCRF server on update and termination requests or re-authorization from server, for failure-handling CONTINUE sessions.

---

**Important**: This keyword is valid only for `update-request` though it is allowed to configure for all the requests. The `failure-handling` command configuration will throw an error/warning message if it is configured for any request other than the update request.

---

**Important**: Failure handling action “continue retry-server-on-event” will be taken only if failure happens to CCR-U message, not for CCR-I messages.

---

**send-ccrt-on-call-termination**: This optional keyword enables to send CCR-T on call termination if the failure action is `continue`.

---

**Important**: This keyword is valid only for `update-request` though it is allowed to configure for all the requests. The `show configuration errors` command will throw an error/warning message if it is configured for any request other than the update request.

---

- **retry-and-terminate**: In the event of a failure the user session continues for the duration of one retry attempt with the server. If this retry attempt also fails, the session is terminated.
- **terminate**: In the event of a failure the user session is terminated.

---

**ccfh** { continue | retry-and-terminate | terminate }

**As in 8.0 release:**

Specifies the credit control failure handling (CCFH) action with or without credit control request type.

---
• **continue**: In the event of a failure the user session continues. DPCA/Diameter will make periodic request and/or connection retry attempts and/or will attempt to communicate with a secondary peer depending on the peer config and session-binding setting.

• **retry-and-terminate**: In the event of a failure the user session continues for the duration of one retry attempt with the server. If this retry attempt also fails, the session is terminated.

• **terminate**: In the event of a failure the user session is terminated.

---

**cc-request-type**

**As in 8.0 release:**

This optional keyword defines the type of credit control request with failure result code and credit control failure handling action for a session.

• **any-request**: Specifies the request type as any request for a new session.

• **initial-request**: Specifies the request type as initial request for a new session.

• **terminate-request**: Specifies the request type as terminate request for a session.

• **update-request**: Specifies the request type as update request for an active session.

---

**Usage**

Use this command to configure the Diameter Policy Control Application (DPCA) failure handling behavior. When an unknown rulebase comes in CCA, changing of rulebase and failure handling is managed in the following manner:

• If the new and existing rulebases have the same CCA policy, then switch to the new rulebase is successful.

• If the new rulebase is valid and has CCA-enabled, in CCA-Initial/Update request, switch to the new rulebase is successful.

• If the new rulebase is valid and does NOT have CCA enabled, whereas the existing rulebase has credit enabled, or vice versa, in CCA-Initial/Update request:
  
  • CCFH-Continue: Goes offline immediately after sending the CCR-T with termination cause as BAD_ANSWER.
  
  • CCFH-RETRY&TERMINATE: Goes offline immediately after sending the CCR-T with termination cause as BAD_ANSWER.
  
  • CCFH-TERMINATE: Goes offline immediately after sending the CCR-T with termination cause as BAD_ANSWER.

• If the new rulebase is invalid, in CCA-Initial/Update request:
  
  • CCFH-Continue: Goes offline immediately after sending the CCR-T with termination cause as BAD_ANSWER.
  
  • CCFH-RETRY&TERMINATE: Terminates on successful CCA-T, or terminates after successful/failed retry to secondary.
  
  • CCFH-TERMINATE: Terminates on successful/failed CCR-T to Primary.

The default failure handling behavior is:

**failure-handling diameter-result-code any-error ccfh terminate**

In StarOS release 14.1 and earlier, when an IP CAN session is up, if any CCR-U message delivery fails due to timeout or TCP link failure, the failure-handling action “**continue**” will be taken for the session and there will not be any further interaction with PCRF and RAR from PCRF is also not accepted (result code 5002 is
sent in RAA). If the CCR-U that is triggered for reporting Usage-Monitoring-Information AVP fails, then the usage information is lost.

In 15.0 and later releases, after the IP-CAN session is up, if CCR-U message delivery fails due to timeout or TCP link failure, the failure-handling action “continue retry-server-on-event” will be taken at PCEF. Any request coming from session manager will be forwarded to PCRF, and if message delivery again fails session manager will be notified with status “SN_STATUS_NO_ACTIONS_TAKEN”.

If CCR-U for reporting Usage-Monitoring-Information fails, then the unreported usage information is given back to ECS and the usage information is stored at ECS. Usage will be reported in CCR-T or in the next CCR-U (if CLI “event-update send-usage-report” is configured). Also, RAR message from PCRF will be processed and responded with result-code success in RAA.

**Important:** Unreported usage will be lost, if CCR-U message delivery fails for last rule removal or usage reporting for monitoring stop indication from PCRF. Also, note that preserving unreported usage monitoring information is currently not supported for dpca-custom9 dictionary.

**Example**

The following command sets the DPCA failure handling to retry-and-terminate and return a result code of 3456 for credit control request type initial-request:

As in 8.0 release:

```plaintext
failure-handling diameter-result-code 3456 ccfh retry-and-terminate cc-request-type initial-request
```

As in 8.1 and later releases:

```plaintext
failure-handling cc-request-type initial-request diameter-result-code 3456 retry-and-terminate
```
li-secret

Refer to the *Cisco ASR 5000 Lawful Intercept Configuration Guide* for a description of this command.
re-auth-trigger

This command configures the Event-Trigger AVP with the value “CHARGING_CORRELATION_EXCHANGE (28)”.

Product
GGSN
HA
HSGW
IPSG
PDSN
P-GW
S-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > IMS Authorization Configuration > Policy Control Configuration

configure > context context_name > ims-auth-service service_name > policy-control

Entering the above command sequence results in the following prompt:

[context_name] host_name(config-imsa-dpca)#

Syntax

re-auth-trigger charging-correlation-exchange

{ default | no } re-auth-trigger

default
Applies the default setting for this command.

no
Disables the event trigger “CHARGING_CORRELATION_EXCHANGE (28)”.

charging-correlation-exchange
This keyword enables the event trigger “CHARGING_CORRELATION_EXCHANGE (28)”.

Usage
Use this command to configure the Event-Trigger AVP with the value “CHARGING_CORRELATION_EXCHANGE (28)”. When this trigger is configured, the Access-Network-Charging-Identifier-Gx AVP will be encoded in all CCR messages and sent to PCRF. Unless configured, the Event-Trigger AVP will not contain the value “CHARGING_CORRELATION_EXCHANGE (28)”. The PCRF will use this event trigger value in CCA and RAR commands to indicate that the PCEF will report the access network charging identifier associated to one or more dynamic PCC rules through the Access-
Network-Charging-Identifier-Gx AVP. The Charging-Correlation-Indicator AVP with the value CHARGING_IDENTIFIER_REQUIRED will be provided. When used in a CCR command, this value indicates that an access network charging identifier has been assigned. The actual value will be reported through the Access-Network-Charging-Identifier-Gx AVP. In releases prior to 15.0, the Access-Network-Charging-Identifier-Gx AVP was always included in CCR-I/CCR-U messages sent from the system to PCRF and contains default bearer's charging ID. Now in 15.0 and later releases, it is sent only if the event trigger “CHARGING_CORRELATION_EXCHANGE (28)” is enabled and a new AVP “Charging-Correlation-Indicator 0 (identifier required)” is sent by PCRF to the system. This behavioral change is introduced to conform to the 3GPP TS 29.212 V10.5.0, and it is important to be noted that this CLI command helps to retain the old behavior, that is, send the Access-Network-Charging-Identifier-Gx AVP in all CCR messages. PCRF can install the event trigger (28) and request for the charging correlation while installing/modifying a dynamic rule in RAR/CCA. PCRF can install the trigger and request for charging correlation alone without modifying the rule in RAR/CCA message. Earlier, this AVP “Access-Network-Charging-Identifier-Gx” was included in the RAA message. But, in 15.0 and later releases, this AVP is not sent in RAA but a new CCR-U is triggered if the system receives Charging-Correlation-Indicator AVP in RAR message and the trigger is enabled.

**Example**

The following command enables the CHARGING_CORRELATION_EXCHANGE event trigger.

```
re-auth-trigger charging-correlation-exchange
```
subscription-id service-type

This command enables required subscription-id types for various services. The Subscription-ID AVP will be encoded based on the configured subscription-ID type.

Product
- GGSN
- HA
- IPSG
- PDSN
- P-GW

Privilege
- Security Administrator, Administrator

Mode
- Exec > Global Configuration > Context Configuration > IMS Authorization Configuration > Policy Control Configuration
- configure > context context_name > ims-auth-service service_name > policy-control

Entering the above command sequence results in the following prompt:

```
{context_name}@host_name(config-imsa-dpca)#
```

Syntax

```
subscription-id service-type { closed_rp | ggsn | ha | ipsg | l2tpls | mipv6ha | pdsn | pgw } { e164 | imsi | nai }
```

```
{ default | no } subscription-id service-type { closed_rp | ggsn | ha | ipsg | l2tpls | mipv6ha | pdsn | pgw } { e164 | imsi | nai }
```

```
default | no
```

Configures this command with the default setting.
The default behavior is that Subscription-ID AVP will be encoded based on service-type and Diameter dictionary.

```
{ closed_rp | ggsn | ha | ipsg | l2tpls | mipv6ha | pdsn | pgw } { e164 | imsi | nai }
```

Controls the encoding of Subscription-ID AVP based on the following service-types associated with services such as GGSN, HA, IPSG, PDSN, etc.

- E164
- IMSI
- NAI

Usage

In releases prior to 15.0, Subscription-ID AVP is encoded based on service-type and Diameter dictionary.
In 15.0 and later releases, when IMS Authorization service encodes the Subscription-ID AVP, IMSA will first check whether or not this CLI command `subscription-id service-type` is configured. If the CLI is configured for the current service, then IMSA will encode the Subscription-ID AVP based on the configured subscription-ID type. This CLI command takes more precedence than the default behavior. If the CLI configuration does not encode any Subscription-ID AVP, then IMSA will encode this AVP based on the default behavior. For example, in GGSN/IPSG service, NAI support is not available. If this CLI command is configured for GGSN/IPSG service with NAI type, then based on CLI IMSA cannot encode any subscription-ID AVP. By this time default behavior (old behavior based on service-type and dictionary) will add the subscription-ID.

**Example**

The following command enables encoding of the Subscription-ID AVP based on IMSI parameter for GGSN service:

```
subscription-id service-type ggsn imsi
```
Chapter 256
PVC Configuration Mode Commands

The Permanent Virtual Connection (PVC) configuration mode commands bind IP interfaces or SS7-Frame Relay links a PVC as well as configure PVC operational parameters for a specific port.

Mode

Exec > Global Configuration > ATM Port Configuration > PVC Configuration

```
configure > port atm slot_number/port_number > pvc vpi vpi_number vci vci_number
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-port-slot_number/port_number-pvc-pvc_number/vci_number)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, version, and installed license(s).
bind

This command binds an IP interface or an SS7 link to the PVC.

**Important:** Prior to attempting the binding, the interface and context or the SS7 routing information and link must have been configured.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > ATM Port Configuration > PVC Configuration

```bash
configure > port atm slot_number/port_number > pvc vpi vpi_number vci vci_number
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-port-slot_number/port_number-pvc-pvc_number/vci_number)#
```

**Syntax**

```bash
[ no ] bind { interface interface_name context_name | link ss7-routing-domain rd_id linkset-id id link-id id }
```

- **no**
  Removes the binding from the configuration.

- **interface_name**
  Defines the name of the virtual interface to be bound to the PVC. *interface_name:* Must be a unique string consisting of 1 to 79 alphanumeric characters.

- **context_name**
  Specifies the name of the context to be bound to the virtual interface. *context_name:* Must be a unique string consisting of 1 to 79 alphanumeric characters.

- **ss7-routing-domain rd_id**
  Identifies a specific SS7 routing domain. *rd_id:* must be an integer from 1 to 12

- **linkset-id id**
  Identifies a specific linkset within the routing domain. *id:* must be an integer from 1 to 33

- **link-id id**
  Identifies a specific link within the linkset. *id:* must be an integer value 1 - 16
Usage
Use this command to bind the PVC to an interface or a specific link.

Example
Use a command similar to the following to bind a PVC to a link ID #2:

```
bind ss7-routing-domain 1 linkset-id 23 link-id 2
```
encapsulation aal5

Specify the data encapsulation type for the ATM adaptation layer 5 (AAL5) frames for the PVC.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > ATM Port Configuration > PVC Configuration

configure > port atm slot_number/port_number > pvc vpi vpi_number vci vci_number

Entering the above command sequence results in the following prompt:

[local]host_name(config-port-slot_number/port_number-pvc-pvc_number/vci_number)#

Syntax

encapsulation aal5 { llc-snap | vc-mux }

<table>
<thead>
<tr>
<th>llc-snap</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frames protocol is identified in the AAL5 using logical link control (LLC) encapsulation.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>vc-mux</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frames are not encapsulated and use virtual circuit multiplexing (VC-MUX) to identify the protocols used for the AAL5 frames.</td>
</tr>
</tbody>
</table>

Usage
Use this command to identify the protocol type for the circuit.

Example

encapsulation aal5 vc-mux
end

Exits the PVC configuration mode and returns to the Exec mode.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**
end

**Usage**
Change the mode back to the Exec mode.
**exit**

Exits the PVC configuration mode and returns to the ATM port configuration mode.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
exit
```

**Usage**

Return to the port configuration mode.
shaping

Specify the type of traffic shaping (rates) for this PVC.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > ATM Port Configuration > PVC Configuration
configure > port atm slot_number/port_number > pvc vpi vpi_number vci vci_number

Entering the above command sequence results in the following prompt:

[local]host_name(config-port-slot_number/port_number-pvc-pvc_number/vci_number)#

Syntax

shaping { cbr pcr pcr_num | ubr pcr pcr_num | ubr+ pcr pcr_num mrc mrc_num | vbr pcr pcr_num scr src_num mbs mbs_num }

---

cbr

Constant bit rate
pcr - peak cell rate = cells per second
pcr_num: Must be an integer from 75 to 1412830

---

ubr

Unspecified Bit Rate
pcr - peak cell rate = cells per second
pcr_num: Must be an integer from 75 to 1412830

---

ubr+

Unspecified Bit Rate with Minimum Cell Rate.
The PCR and MCR values should be set to maintain the following relationship: PCR >= (MCR + minRate), where the current recommended minRate is 75.
pcr - peak cell rate = cells per second
pcr_num: Must be an integer from 75 to 1412830
mcr - minimum cell rate
mcr_num: Must be an integer from 75 to 1412830

---

vbr

Variable Bit Rate, NRT (not real time) type.
The PCR and MCR values should be set to maintain the following relationship: PCR >= (MCR + minRate), where the current recommended minRate is 75.
pcr - peak cell rate = cells per second
pcr_num must be an integer from 75 to 1412830
scr - sustained cell rate
scr_num must be an integer from 75 to 1412830
mbs - maximum burst size

mbs_num must be an integer from 75 to 1412830

Usage
Use this command to configure the shaping for egress traffic on this PVC.

Example

    shaping cbr pcr 56000
**shutdown**

Disables/enables traffic over the current VLAN.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > ATM Port Configuration > PVC Configuration

```
configure > port atm slot_number/port_number > pvc vpi vpi_number vci vci_number
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-port-slot_number/port_number-pvc-pvc_number/vci_number)#
```

**Syntax**

```
shutdown

no shutdown
```

Enables the VLAN. When omitted the VLAN is non-functional.

**Usage**

Enables/ Disables specified VLAN.

This command is necessary to bring a VLAN into service by enabling it via the `no` keyword.

**Example**

To disable a VLAN from sending or receiving network traffic use the following command:

```
shutdown
```

To enable a VLAN use the following command:

```
no shutdown
```
The PVC (permanent virtual connection) Interface configuration mode is used to create and manage the IP parameters for PVC interface(s) associated with an OLC (ATM-type) for a specific context.

**Mode**

```
Exec > Global Configuration > Context Configuration > PVC Interface Configuration

configure > context context_name > interface interface_name point-to-point
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-pvc)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
description

Defines descriptive text to provide useful information about the current interface.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PVC Interface Configuration

```
configure > context context_name > interface interface_name point-to-point
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-pvc)#
```

**Syntax**

```
description text
```

```
no description
```

**no**
Erases the port’s description from the configuration file.

**text**
```
text: Must be a string of 1 to 79 alphanumeric characters with no spaces or a string within double quotes that includes printable characters. The description is case-sensitive.
```

**Usage**
Set the description to provide helpful information, for example the port’s primary function, services, end users. Define any information, the only limit is the number of characters, 79.

**Example**

```
description "PVC12 connects server 1 to home office."
```
end

Exits the PVC interface configuration mode and returns to the Exec mode.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

end

Usage
Change the mode back to the Exec mode.
exit

Exits the interface configuration mode and returns to the context configuration mode.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

exit

Usage
Return to the context configuration mode.
ip

The commands in this section are used to configure the IP parameters for the PVC interface.

Important: Before configuring the OSPF parameters in this section, you need to enable OSPF using the router command and OSPF configuration sub-mode commands accessed in the Context configuration mode and documented in the Context Configuration Mode chapter of this Command Line Interface Reference.
ip access-group

This command identifies the access control list (ACL) to be associated with this PVC interface in this context.

**Important:** Prior to using this command, the access list must be created for this context with the `ip access-list` command in the Context configuration mode and then the ACL must be configured using the commands described in CLI chapter ACL Configuration Mode.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PVC Interface Configuration

command: `configure > context context_name > interface interface_name point-to-point`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-pvc)#
```

**Syntax**

```
ip access-group name { in | out }

no ip access-group name { in | out }
```

**no**
Indicates the specified access group to be removed from the access list.

**name**
Specifies the access control list (ACL) rule to be added or removed from the group.

**name:** Must be a string of 1 to 79 alphanumeric characters with no spaces.

**Important:** Up to 8 ACLs can be applied to a group provided that the number of rules configured within the ACL(s) does not exceed the 128 rule limit for the interface.

**in | out**

**in:** Specifies list is for in-bound access control.

**out:** Specifies the list is for out-bound access control.

**Important:** Even though “in” or “out” can be specified, context-level ACL rules are automatically applied to both directions.
Usage
Use this command to add IP access lists configured for the same context to an IP access-group. The list can be configured to apply to all inbound and/or outbound traffic.

Example
The following adds ACL access-list-1 to the IP access-group associated with this PVC for this context.

```
ip access-group access-list-1 in
```
**ip address**

Defines the primary IP address and the network mask to be associated with this PVC interface for this context. This command can also be used to configure the secondary IP address.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PVC Interface Configuration

`configure > context context_name > interface interface_name point-to-point`

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-if-pvc)#`

**Syntax**

```plaintext
ip address ip_address ip_mask [ secondary ]

no ip address ip_address
```

**Usage**

Configures or deletes the IPv4 or IPv6 addresses and subnet mask to be associated with this PVC.

**Example**

The following configures the secondary IP address to associate with the interface.

```plaintext
ip address 131.2.3.4 255.255.255.0 secondary
```

The following set of commands removes the primary IP address from the PVC interface configuration for this context.

```plaintext
no ip address secondary address
```
no ip address primary address
**ip mtu**

Configures the maximum transmission unit (MTU) to be supported on this interface.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PVC Interface Configuration

```
configure > context context_name > interface interface_name point-to-point
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-pvc)#
```

**Syntax**

```
ip mtu value

no ip mtu
```

- **no**
  - Disables and/or restores the option to the system default.

- **mtu value**
  - Configures the maximum transmission unit in octets.
  - **value**: Enter an integer between 576 and 1600. Default is 1500.

**Usage**

Change the maximum transmission unit size to 1300.

**Example**

```
ip mtu 1300
```
**ip ospf authentication-key**

This command configures the password or key to be used for OSPF (Open Shortest Path First) authentication with neighboring routers.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PVC Interface Configuration
configure > context context_name > interface interface_name point-to-point

Entering the above command sequence results in the following prompt:

([context_name]host_name(config-if-pvc)#

**Syntax**

```
ip ospf authentication-key [ encrypted ] password auth_key
no ip ospf authentication-key
```

**Usage**

Use this command to set the authentication key used when authenticating with neighboring routers.

**Example**

To set the authentication key to 123abc, use the following command;

```
ip ospf authentication-key password 123abc
```

Use the following command to delete the authentication key;

```
no ip ospf authentication-key
```
**ip ospf authentication-type**

This command configures the OSPF authentication method to be used with OSPF neighbors over the logical interface.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PVC Interface Configuration

`configure > context context_name > interface interface_name point-to-point`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-pvc)#
```

**Syntax**

```
ip ospf authentication-type { message-digest | null | text }
no ip ospf authentication-type { message-digest | null | text }
```  

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>message-digest</strong></td>
<td>Set the OSPF authentication type to use the message digest (MD) authentication method.</td>
</tr>
<tr>
<td><strong>null</strong></td>
<td>Set the OSPF authentication type to use no authentication, thus disabling either MD or clear text methods.</td>
</tr>
<tr>
<td><strong>text</strong></td>
<td>Set the OSPF authentication type to use the clear text authentication method.</td>
</tr>
</tbody>
</table>

**Usage**

Use this command to set the type of authentication to use when authenticating with neighboring routers.

**Example**

To set the authentication type to use clear text, enter the following command;

```
ip ospf authentication-type text
```
ip ospf cost

This command configures the cost associated with sending a packet over this logical interface.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PVC Interface Configuration

configure > context context_name > interface interface_name point-to-point

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-if-pvc)#

Syntax

ip ospf cost value

no ip ospf cost

no

Disable this function.

value

Default: 10

The cost to assign to OSPF packets. This must be an integer from 1 through 65535.

Usage

Use this command to set the cost associated with routes from the interface.

Example

Use the following command to set the cost to 20;

    ip ospf cost 20

Use the following command to disable the cost setting;

    no ip ospf cost
**ip ospf dead-interval**

This command configures the dead-interval and the delay time in seconds, for OSPF communications.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PVC Interface Configuration

configure > context context_name > interface interface_name point-to-point

Entering the above command sequence results in the following prompt:

\[\text{context_name}\text{host_name(config-if-pvc)}\#$

**Syntax**

`ip ospf dead-interval value`

`no ip ospf dead-interval`

- **no**
  Deletes the value set and returns the value to its default.

- **value**
  The interval, in seconds, that the router should wait. During this interval, if no packets are received then the system considers the neighboring router to be off-line. This interval is typically 4 times the duration of the hello-interval.
  Value must be an integer from 1 through 65535. Default: 40

**Usage**

Use this command to set the dead-intervals or delays for OSPF communications.

**Example**

To set the dead-interval to 100, use the following command;

```
ip ospf dead-interval 100
```

To delete the setting for the dead-interval and reset the dead-interval value to its default of 40, use the following command:

```
oip ospf dead-interval
```
ip ospf hello-interval

This command configures the delay time in seconds, for OSPF hello interval.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PVC Interface Configuration

\texttt{configure > context context\_name > interface interface\_name point-to-point}

Entering the above command sequence results in the following prompt:

\texttt{[context\_name]\host\_name(config-if-pvc)#}

Syntax

\texttt{ip ospf hello-interval value}

\texttt{no ip ospf hello-interval}

\texttt{no}

Deletes the value set and returns the value to its default.

\texttt{value}

The interval, in seconds, between sending hello packets. This value is typically set to be 1/4 of the value of the dead-interval. \texttt{value} must be an integer from 1 through 65535. Default: 10

Usage

Use this command to set the delays for the hello-interval.

Example

To set the hello-interval to 25, use the following command;

\texttt{ip ospf hello-interval 25}

To delete the setting for the hello-interval and reset the hello-interval value to its default of 10, use the following command:

\texttt{no ip ospf hello-interval}
ip ospf message-digest-key

This command enables the use of MD5-based OSPF authentication.

Product
- SGSN

Privilege
- Security Administrator, Administrator

Mode
- Exec > Global Configuration > Context Configuration > PVC Interface Configuration
  configure > context context_name > interface interface_name point-to-point

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-if-pvc)#

Syntax

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip ospf message-digest-key key_id md5 [ encrypted ] password authentication_key</td>
<td>Creates an authentication key. Use this command to create an authentication key that uses MD5-based OSPF authentication.</td>
</tr>
<tr>
<td>no ip ospfmessage-digest-key key_id</td>
<td>Deletes the key.</td>
</tr>
</tbody>
</table>

Usage

Use this command to create an authentication key that uses MD5-based OSPF authentication.

Example

To create a key with the ID of 25 and a password of 123abc, use the following command;

    ip ospf message-digest-key 25 md5 password 123abc

To delete the same key, enter the following command;

    no ip ospf message-digest-key 25
**ip ospf network**

Configures the OSPF network type.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PVC Interface Configuration

```
configure > context context_name > interface interface_name point-to-point
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-pvc)#
```

**Syntax**

```
ip ospf network { broadcast | non-broadcast | point-to-multipoint | point-to-point }
no ip ospf network
```

**Usage**

Use this command to specify the OSPF network type.

**Example**

To set the OSPF network type to broadcast, enter the following command;

```
ip ospf network broadcast
```

To disable the OSPF network type, enter the following command;

```
no ip ospf network
```
ip ospf priority

This command designates the OSPF router priority.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > PVC Interface Configuration

configure > context context_name > interface interface_name point-to-point

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-if-pvc)#

Syntax

ip ospf priority value

no ip ospf priority value

no
Disable this function.

value
The priority value to assign. This must be an integer from 0 through 255.

Usage

Use this command to set the OSPF router priority.

Example

To set the priority to 25, enter the following command:

   ip ospf priority 25

To disable the priority, enter the following command:

   no ip ospf priority
**ip ospf retransmit-interval**

This command configures the retransmit-interval and the delay time in seconds, for OSPF communications.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PVC Interface Configuration

```bash
configure > context context_name > interface interface_name point-to-point
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-pvc)#
```

**Syntax**

```bash
ip ospf dead-interval value

no ip ospf dead-interval
```

- **no**
  - Deletes the value set and returns the value to its default.

- **value**
  - The interval, in seconds, between LSA (Link State Advertisement) retransmissions. Value must be an integer from 1 through 65535. Default: 5

**Usage**

Use this command to set the retransmit-intervals or delays for OSPF communications.

**Example**

To set the dead-interval to 25, use the following command;

```bash
ip ospf retransmit-interval 25
```
**ip ospf transmit-delay**

This command configures the transmit-delay the OSPF communications parameters.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > PVC Interface Configuration

```
configure > context context_name > interface interface_name point-to-point
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-pvc)#
```

**Syntax**

```
ip ospf transmit-delay value

no ip ospf transmit-delay
```

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>value</td>
<td>The interval, in seconds, that the router should wait before transmitting a packet. Value must be an integer from 1 through 65535. Default: 1</td>
</tr>
<tr>
<td>no</td>
<td>Deletes the value set and returns the value to its default.</td>
</tr>
</tbody>
</table>

**Usage**
Use this command to set the transmit-delay.

**Example**
To set the transmit delay to 5 seconds, use the following command:

```
ip ospf transmit-delay 5
```

To delete the setting for the transmit-delay or reset the transmit-delay value to its default of 1, use the following command:

```
no ip ospf transmit-delay
```
Chapter 258
QCI - QoS Mapping Configuration Mode Commands

The QoS Class Index (QCI) to QoS Mapping Configuration Mode is used to map QoS Class Indexes to enforceable QoS parameters. Mapping can occur between the RAN and the Serving Gateway (S-GW), the Mobility Management Entity (MME), and/or the PDN Gateway (P-GW) in an LTE network or between the RAN and the eHRPD Serving Gateway (HSGW) in an eHRPD network.

Mode

Exec > Global Configuration > QCI-QoS Mapping Configuration
configure > qci-qos-mapping name

Entering the above command sequence results in the following prompt:

[local]host_name(config-qci-qos-mapping)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

exit

**Usage**

Use this command to return to the parent configuration mode.
qci

Creates and maps standard QCI values to enforceable QoS parameters.

Product
HSGW
P-GW
SAEGW
S-GW

Privilege
Administrator

Mode
Exec > Global Configuration > QCI-QoS Mapping Configuration
configure > qci-qos-mapping name

Entering the above command sequence results in the following prompt:

[llocal]host_name(config-qci-qos-mapping)#

Syntax information

- Syntax for releases 15 and earlier

Syntax for releases 15 and earlier

```plaintext
qci num [ delay-class num precedence-class num reliability-class num [ downlink | uplink ] ]


qci num [ gbr [ delay-class | downlink | max-packet-delay | traffic-policing | uplink ] ]

qci num [ max-packet-delay num max-error-rate num [ downlink | uplink ] ]

qci num [ non-gbr [ delay-class | downlink | max-packet-delay | traffic-policing | uplink ] ]

qci num [ traffic-policing interval interval [ delay-class | downlink | max-packet-delay | uplink ] ]

```
QCI - QoS Mapping Configuration Mode Commands

[ default | no ] qci num

**Important:** The optional keywords associated with each of the initial optional keywords are abbreviated in the syntax examples above for clarity. Refer to the definitions below for the full keyword paths and associated descriptions for each keyword string in this command.

**default**
Resets the default values for the select standards-based QCI value.

**no**
Disables the selected standards-based QCI value.

**num**
Specifies the standards-based QCI value to be enabled.

**Important:** Only standards-based QCI values of 1 through 9 are supported.

QCI values 1 through 9 are defined in 3GPP Specification TS 23.203 "Policy and charging control architecture".

**delay-class** num precedence-class num reliability-class num

delay-class num: Specifies the pre-release 8 value for configuring packet delay.

**precedence-class** num: Specifies the pre-release 8 value for configuring packet precedence.

**reliability-class** num: Specifies the pre-release 8 value for configuring packet reliability.


Configures parameters for downlink traffic.

802.1p-value priority: Maps the qci value to the priority value set in the Ethernet frame header.

**encaps-header:** Specifies that the DSCP marking must be set on the encapsulation header for IP-in-IP, GRE, or GTP encapsulation.

**user-datagram dscp-marking hex:** Specifies that the IP DSCP marking is to be defined by this keyword.

**Important:** The optional keywords associated with each of the initial optional keywords are abbreviated in the syntax examples above for clarity. Refer to the definitions below for the full keyword paths and associated descriptions for each keyword string in this command.

**copy-inner**

• copy-inner: Specifies that the DSCP marking is to be acquired from the UDP headers within the encapsulation.

• dscp-marking hex: Specifies that the DSCP marking is to be defined by this keyword.

hex is expressed as a hexadecimal number from 0x00 through 0x3F.
**gbr**

Specifies that this QCI type is Guaranteed Bit Rate (GBR).

**max-packet-delay num max-error-rate num**

**max-packet-delay num**: Specifies the maximum packet delay (in milliseconds) that can be applied to the data with the QCI.

* num must be an integer from 10 through 100.

**max-error-rate num**: Specifies the maximum error loss rate of non-congestion related packet loss.

* num must be an integer from 1 through 6, specifying 10-1 through 10-6.

---

**Important**: Defaults for standards-based QCI values are defined in *3GPP Specification TS 23.203 “Policy and charging control architecture”*.

---

**non-gbr**

Specifies that this QCI type is non-Guaranteed Bit Rate (non-GBR).

**traffic-policing interval interval**

Specifies the traffic policing interval associated with the this QCI.

* interval must be an integer from 1 through 100.


Configures parameters for uplink traffic.

**802.1p-value priority**: Maps the qci value to the priority value set in the Ethernet frame header.

* priority is an integer value from 0 through 7.

**encaps-header**: Specifies that the DSCP marking must be set on the encapsulation header for IP-in-IP, GRE, or GTP encapsulation.

**mpls-exp-value value**: Sets EXP bits for MPLS for mobile to egress side traffic.

* value is an integer value from 0 through 7.

**user-datagram dscp-marking hex**: Specifies that the IP DSCP marking is to be defined by this keyword.

* hex is expressed as a hexadecimal number from 0x00 through 0x3F.

{ copy-inner | dscp-marking hex }

- **copy-inner**: Specifies that the DSCP marking is to be acquired from the UDP headers within the encapsulation.

- **dscp-marking hex**: Specifies that the DSCP marking is to be defined by this keyword.

* hex is expressed as a hexadecimal number from 0x00 through 0x3F.

---

**Usage**

Use this command to create and map QCI values to enforceable QoS parameters.
Non-standard QCI values are only supported with the license-enabled operator-defined qci command.

Example

The following command creates a QCI value of 8 and defines the uplink encapsulation header as using the DSCP marking from the encapsulated UDP header:

```plaintext
qci 8 uplink encaps-header copy-inner
```
Chapter 259
QCI - RAN ID Mapping Configuration Mode Commands

The QoS Class Index (QCI) Mapping Configuration Mode is used to map RAN profile IDs to QoS Class Indexes via the HRPD Serving Gateway (HSGW) in an eHRPD network.

Mode

Exec > Global Configuration > QCI - RAN ID Mapping Configuration

configure > profile-id-qci-mapping-table name

Entering the above command sequence results in the following prompt:

[local]host_name(config-profile-id-qci-mapping-table)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
end

Exits the current mode and returns to the Exec Mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
end

**Usage**
Change the mode back to the Exec mode.
exit

Exits the current mode and returns to the previous mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
``` 

**Usage**
Return to the previous mode.
profile-id

Maps a QCI ID to a RAN profile ID and modifies data flow bit rate ranges.

**Product**
HSGW

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > QCI - RAN ID Mapping Configuration

```console
configure > profile-id-qci-mapping-table name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-profile-id-qci-mapping-table)#
```

**Syntax**

```bash
profile-id id qci num [ uplink { gbr rate [ mbr rate ] | mbr rate [ gbr rate ] } downlink { gbr rate [ mbr rate ] | mbr rate [ gbr rate ] } ]
no profile-id id
```

**no profile-id id**

Removes the specified profile ID entry from this map.

**id**

Specifies the profile ID to which a QCI ID will be mapped. `id` must be an integer value from 1 to 65535.

**qci num**

Specifies the QCI number to which the profile ID will be mapped. `num` must be an integer value from 1 to 255.

**uplink**

Specifies that the guaranteed bit rate (GBR) and/or maximum bite rate (MBR) setting that follow this keyword will be applied to the uplink data flow.

**downlink**

Specifies that the guaranteed bit rate (GBR) and/or maximum bite rate (MBR) settings that follow this keyword will be applied to the downlink data flow.

**gbr rate**

Specifies the guaranteed bit rate for the uplink or downlink data flow. `rate` must be an integer value from 0 to 4294967295.
mbr rate

Specifies the maximum bit rate for the uplink or downlink data flow. rate must be an integer value from 0 to 4294967295.

Usage

Use this command to map a QCI ID to a RAN profile ID and, optionally, modify data flow bit rate ranges.

Example

The following command maps a QCI ID (1) to a profile ID (10) and sets the uplink guaranteed bite rate to 10000 and the downlink guaranteed bit rate to 20000:

```
profile-id 10 qci 1 uplink gbr 10000 downlink gbr 20000
```
Chapter 260
Remote Address List Configuration Mode Commands

The Remote Address List Configuration Mode is used to configure address lists for the Remote Address-based Accounting feature on a per-context basis.

Mode

Exec > Global Configuration > Context Configuration > Remote Address List Configuration

configure > context context_name > radius accounting ip remote-address list list_number

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx-remaddr-list)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
address

Configures addresses within a Remote Address List.

Product

- PDSN
- HA

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > Context Configuration > Remote Address List Configuration

```
configure > context context_name > radius accounting ip remote-address list list_number
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-remaddr-list)#
```

Syntax

```
[ no ] address ip_address netmask subnet
```

<table>
<thead>
<tr>
<th>no</th>
<th>Removes a previously configured address.</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip_address</td>
<td>Specifies the IP address of the remote device.</td>
</tr>
<tr>
<td>netmask subnet</td>
<td>Specifies the subnet mask of the remote device.</td>
</tr>
</tbody>
</table>

Usage

Use this command to configure remote address lists for use with the Remote Address-based accounting feature. A maximum of 10 address can be configured per list.

Example

The following command adds an IP address of 192.168.100.1 with a subnet mask of 255.255.255.0 to the list:

```
address 192.168.100.1 netmask 255.255.255.0
```
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
```
end
```

**Usage**
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**
Use this command to return to the parent configuration mode.
The Remote Secret List Configuration Mode manages the list of remote secrets based on ID type.

Mode

Exec > Global Configuration > Remote Secret List Configuration

> crypto remote-secret-list listname

[local_context]host_name(config-remote-server-list)#
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
```
end
```

**Usage**
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Use this command to return to the parent configuration mode.
remote-id

Configures the remote pre-shared key based on the ID type.

**Product**
WSG

**Privilege**
Security Administrator

**Mode**
Exec > Global Configuration > Remote Secret List Configuration
> crypto remote-secret-list listname
[local_context]host_name(config-remote-server-list)#

**Syntax**

```plaintext
remote-id id-type { der-asn1-dn | fqdn | ip-addr | key-id | rfc822-addr } id id_value
secret [ encrypted ] key key_value

no remote-id id-type { der-asn1-dn | fqdn | ip-addr | key-id | rfc822-addr } id id_value
```

**Usage**

Use this command to enter up to 1000 entries in the remote secret list. Each entry is designated by ID type and ID value. Repeat the command sequence to add entries to the list.

**Example**

The following command enters an ip address in the remote secret list:
remote-id id-type ip-addr id 10.1.1.1
Chapter 262
Remote Server List Configuration Mode Commands

The Remote Server List Configuration Mode manages the list of server addresses to which a context has access.

Mode

Exec > Global Configuration > Remote Server List Configuration

configure > context context_name > remote-server-list name list_name

[context_name]host_name(config-remote-server-list)#

Important: Available commands or keywords/variables vary based on platform type, product version, and installed license(s).
address

Configures or removes an IP address to a remote server.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Remote Server List Configuration
configure > context context_name > remote-server-list name list_name

[context_name]host_name(config-remote-server-list)#

Syntax

address remote-ip-address netmask ip_netmask

no address remote-ip-address netmask ip_netmask

Usage
Removes the specified IP address from the Remote Server List.

remote-ip-address netmask ip_netmask

Specifies the IP address and netmask of the remote server in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

Example

Use this command to create and maintain a list of remote servers accessible by this context.

address 193.154.78.9 netmask 255.255.255.0
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
```
end
```

**Usage**
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
exit

**Usage**
Use this command to return to the parent configuration mode.
Chapter 263
RLF Template Configuration Mode Commands

Rate Limiting Function (RLF) Template Configuration Mode is accessed from the Global Configuration Mode. This mode allows an operator to configure the RLF template that can be associated with Diameter and other applications for throttling and rate controlling of messages sent to external network interfaces.

**Important:** Rate Limiting Function (RLF) is a license-controlled feature. A valid feature license must be installed prior to configuring this feature. Contact your Cisco account representative for more information.

Mode

Exec > Global Configuration > RLF Template Configuration

```
configure > rlf-template rlf_template_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-rlf-template)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
**delay-tolerance**

Defines the maximum number of seconds a control plane signaling message can be queued before being processed. After exceeding this delay, the message is dropped.

**Product**

GGSN

P-GW

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > RLF Template Configuration

`configure > rlf-template rlf_template_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-rlf-template)#
```

**Syntax**

```
delay-tolerance tolerance_value [ -noconfirm ]
```

**default delay-tolerance**

```
default
```

Removes the configuration associated with the RLF template. Default value is 2.

```
tolerance_value
```

Specifies the maximum number of seconds a message can be queued in the RLF module. The message must be sent after expiry of “delay-tolerance” seconds. `tolerance_value` must be an integer from 0 through 10. Default value is 2.

```
[ -noconfirm ]
```

Specifies that the command must execute without any prompts and confirmation from the user.

**Usage**

Use this command to define the maximum number of seconds a message can be queued in the RLF module before being processed. After exceeding this delay, the message is dropped.

**Example**

The following command sets the value of delay tolerance to 4 seconds:

```
delay-tolerance 4
```
**end**

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
```
end
```

**Usage**
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax

exit

Usage

Use this command to return to the parent configuration mode.
**msg-rate**

Sets the maximum number of messages that can be processed per second.

**Product**

GGSN
P-GW

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > RLF Template Configuration

```
configure > rlf-template rlf_template_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(cfg-rlf-template)#
```

**Syntax**

```
msg-rate tps_value burst-size size [ -noconfirm ]
```

- **tps_value**

  Specifies the number of messages that can be processed per second. This is the maximum number of allowed transactions per second (TPS) for an external interface.

- **Important**: The TPS value (configured per external interface) is at a chassis-level and is distributed appropriately to all session managers, AAA manager, Diamproxy, or any other applications that use RLF. RLF employs the Token Bucket Algorithm to achieve the rate limiting.

  - **tps_value** must be an integer from 1 through 100000.

- **burst_size**

  Defines the maximum number of messages (burst) that can be sent out together at any instant of time. If this setting is not configured, the default value is the current message rate. Burst size is used to derive the shaping interval in such a way that it splits the 1000 ms in N slots, where N can be 1, 2, 4, 5, 10, 20, 50, and 100.

  - **size** must be an integer from 1 through 100000.

  - **[-noconfirm]**

  Specifies that the command must execute without any prompts and confirmation from the user.

**Usage**

Use this command to define the number of messages that can be processed per second. This is the maximum number of allowed transactions per second (TPS) for an external interface. The RLF ensures that the maximum configured TPS rate is not exceeded on the interface.
If burst-size is not configured, the messages are sent without delay when they arrive in RLF. For example, if the CLI command `msg-rate 1000 burst-size 100` is configured, then all 1,000 messages are sent to an external interface in bursts of 100 messages (burst-size). If the burst size is not configured, then all 1,000 messages are sent as they arrive in RLF (regardless of TPS).

**Example**

The following command sets the value of message rate to 20:

```
msg-rate 20
```
threshold

Configures the threshold for rate-limiting the outgoing messages.

Product

GGSN
P-GW

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > RLF Template Configuration
configure > rlf-template rlf_template_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(cfg-rlf-template)#

Syntax

threshold { lower lowerThreshold_value | upper upperThreshold_value } [ -noconfirm ]

default threshold

default

Returns the command to its default settings.

lower lowerThreshold_value

This threshold indicates that the application has message-rate control enabled. Default is 30%. If the number of outstanding messages in the RLF queue drops below 30% of msg-rate, RLF will transition to READY state.

upper upperThreshold_value

This threshold indicates that action will be taken when the message-rate reaches the maximum limit. Default is 80%. If the number of outstanding messages in the RLF queue exceeds 80% of msg-rate, RLF will transition to OVER_THRESHOLD state.

Usage

Use this command to configure the desired threshold value for rate limiting the outgoing messages. The configurable threshold value of TPS for an interface is used to notify applications of corrective actions when the threshold criteria is met.

Example

The following command configures the upper threshold to 80 and the lower threshold to 60 for throttling and rate control:

    threshold upper 80 lower 60
Chapter 264
RNC Configuration Mode Commands

The RNC (radio network controller) configuration mode defines the parameters related to the SGSN connection with an RNC.

Mode

Exec > Global Configuration > Context Configuration > luPS Service Configuration > RNC Configuration

configure > context context_name > iups-service service_name > rnc id rnc_id

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx-iups-service-rnc)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
associate-gtpu-bind-address

This command defines the GTP-U loopback address and associates (binds) this address with a particular interface (non-loopback) address.

Product

SGSN

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > Context Configuration > luPS Service Configuration > RNC Configuration

configure > context context_name > iups-service service_name > rnc id rnc_id

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx-iups-service-rnc)#

Syntax

[ no ] associate-gtpu-bind-address ip_address to-interface-address ip_address

- **no**
  - Removes the loopback address definition and interface association from the current RNC configuration.

- **ip_address**
  - **ip_address**: Must be specified using the standard IPv4 dotted decimal notation.

Usage

Use this command to setup associations between loopback GTP-U addresses and a non-loopback addresses.

Example

Bind the GTP-U loopback address of 123.1.1.1 to interface address 222.1.1.1:

associate-gtpu-bind-address 123.1.1.1 to-interface-address 222.1.1.1
description

This command defines an alphanumeric string that is intended to provide descriptive information about the radio network controller (RNC). This is used for operator reference only.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > IuPS Service Configuration > RNC Configuration

configure > context context_name > iups-service service_name > rnc id rnc_id

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx-iups-service-rnc)#

Syntax

description string

no description

no

Removes the description string from the current RNC configuration.

string

Specifies the alphanumeric string that is stored. must be from 1 through 255 alphanumeric characters. Strings with spaces must be enclosed in double-quotes. See the example below.

Usage

Use this command to set a description for reference by operators.

Example

The following command sets the description to identify a particular RNC and carrier in Uganda "RNC1 Carrier2 Uganda":

description "RNC1 Carrier2 Uganda"
**direct-tunnel**

This command enables/disables the direct tunnel feature through the interface to the radio network controller (RNC).

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > luPS Service Configuration > RNC Configuration

```plaintext
configure > context context_name > iups-service service_name > rnc id rnc_id
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service-rnc)#
```

**Syntax**

```plaintext
direct-tunnel not-permitted-by-rnc

default direct-tunnel
```

**default**

Sets the direct tunnel support on RNC to default mode; i.e. enabling direct tunnel.

**not-permitted-by-rnc**

Default: enabled

Disables the direct-tunnel support on radio network controller (RNC).

**Usage**

Use this command to disable/enable the direct-tunnel function through the interface to the RNC.

**Example**

Following command disables the direct tunnel support to the RNC:

```plaintext
direct-tunnel not-permitted-by-rnc
```
**dual-address-pdp**

This command enables the SGSN to work with an RNC with functioning dual address (IPv4v6) bearer support capability. By default, it is assumed that the RNC does not support dual PDP-type addressing.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > LuPS Service Configuration > RNC Configuration

`configure > context context_name > iups-service service_name > rnc id rnc_id`

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-ctx-iups-service-rnc)#`

**Syntax**

```
dual-address-pdp { not-supported | supported }

default dual-address-pdp
```

---

**default**

Resets the SGSN to function with an RNC that is not supporting dual PDP addressing.

---

**not-supported**

Default

Enables the SGSN to work with an RNC that does not support dual PDP-type addressing. It allows a single address bearer PDP-type to be activated with a configured PDP-type.

---

**supported**

Enables the SGSN to work with an RNC that does support dual PDP-type addressing.

---

**Usage**

This command enables the SGSN to support dual PDP-type addressing (IPv4v6) per RNC. For a dual PDP context to be activated, the RNC should support the PDP-type IPv4v6 in the RAB assignment request. For an RNC that does support the dual PDP-type addressing, use this command to change the default configuration and to configure the SGSN to work with the RNC’s dual address bearer support capability. If the RNC does not support this functionality, then the `default` form of this command should be configured to enable the SGSN to activate a single-address bearer PDP context even if (1) the UE requests PDP type IPv4v6 and if (2) the subscription allows this PDP type. The single address bearer PDP type will be activated with a configured PDP type.

When a UE moves from an RNC that supports dual PDP-type addressing to another RNC that does not support dual PDP-type addressing, then the SGSN will deactivate the PDP context. This is done because, even if we preserve the PDP contexts, the UE would be unaware of the preserved PDP context. This would lead to non-synchronized behavior in the network. So the SGSN deactivates the PDP context with cause code...
"reactivation-required" to ensure the UE, RNC, SGSN, and GGSN are in synch. As well, this gives the UE the opportunity to activate a PDP context again without dual bearers.

The `sgsn-rnc-no-dual-pdp-init-pdp-deact` disconnect reason is used to indicate that a PDP context has been deactivated because of roaming into an RNC that does not support this feature.

**Important:** For this configuration to function, support for dual PDP-type addressing must be enabled at the global level (the default). To confirm the functionality is enabled, issue the `show sgsn-mode` command from the Exec mode. If the PDP-type addressing is not enabled, then refer to the instructions for the `dual-address-pdp` command in the `SGSN Global Configuration Mode Commands` section.

**Example**

Use the following command to enable dual PDP-type addressing with a supporting RNC:

```
dual-address-pdp supported
```
enb-direct-data-forward

Selects the setup of indirect data forwarding tunnels (IDFT) between the eNodeB and the RNC via the SGW during SRNS relocation, or, selects the use of direct data forwarding.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > luPS Service Configuration > RNC Configuration

```bash
configure > context context_name > iups-service service_name > rnc id rnc_id
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service-rnc)#
```

**Syntax**

```
[no] enb-direct-data-forward
```

- **[no]**
  Disables direct data forwarding and enables the setup of indirect data forwarding tunnels between the eNodeB and the RNC via the SGW during SRNS relocation. This allows the S4-SGSN to support connected mode handovers between the UTRAN and E-UTRAN networks across the S3 interface. This is the default setting.

- **enb-direct-data-forward**
  Enables the use of direct data forwarding between the eNodeB and the RNC via the SGW. If this setting is configured and the SGSN receives a Relocation Required message from this RNC for a subscriber with target node as an eNodeB, then the SGSN will set the indication->DFI (direct forwarding indicator) flag in the Forward Relocation Request message sent across the S3 interface. Use of this command disables the setup of indirect data forwarding tunnels.

**Usage**

Use this command to enable the setup of direct data forwarding tunnels between the eNodeB and the RNC during inter RAT connected mode handover. Enabling direct data forwarding tunnels allows the S4-SGSN to support connected mode handovers between the UTRAN and E-UTRAN networks across the S3 interface without the use of indirect data forwarding tunnels through SGW. Once direct data forwarding is enabled, indirect data forwarding is automatically disabled.

**Example**

Enable the setup of indirect data forwarding tunnels between the eNodeB and RNC via the SGW during SRNS relocation. This command also disables direct data forwarding.

```
no enb-direct-data-forward
```
end

Exits the configuration mode and returns to the Exec mode.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**
end

**Usage**
Change the mode to the Exec mode.
exit

Exits the current configuration mode and returns to the IuPS Service configuration mode.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**
Return to the previous configuration mode.
**lac**

This command identifies a Local Area Concentrator (LAC) and a Remote Area Concentrator (RAC) and associates them with this RNC definition.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > luPS Service Configuration > RNC Configuration
configure > context context_name > iups-service service_name > rnc id rnc_id

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service-rnc)#
```

**Syntax**

```
[ no ] lac lac_id rac rac_id
```

- **no**
  Deletes the LAC and RAC information from the system configuration.

- **lac_id**
  A unique numeric identifier for the LAC associated with the RNC.
  **lac_id** must be an integer between 1 and 65535.

- **rac_id**
  A unique numeric identifier for the RLAC associated with the RNC.
  **rac_id** must be an integer between 1 and 255.

**Usage**

Creates an association with a specific LAC and RAC.

**Example**

Associate LAC 545 and RAC 23 with this RNC:

```
lac 545 rac 23
```
mbms

Configures RNC options for multimedia broadcast multicast service.

Important: This feature and command are currently under development and are not supported.

Product

SGSN
overload-action disable

This command maps an action to be taken if traffic reaches or exceeds defined levels.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > luPS Service Configuration > RNC Configuration

configure > context context_name > iups-service service_name > rnc id rnc_id

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service-rnc)#
```

**Syntax**

```
overload-action disable { activate | attach | auth-challenge | modify-request | paging-downlink-data | ptmsi-reallocation | service-request-data | sms | srns } traffic-level

[ no | default ] overload-action disable { activate | attach | auth-challenge | modify-request | paging-downlink-data | ptmsi-reallocation | service-request-data | sms | srns }
```

- **no**
  Removes the defined overload action from configuration.

- **default**
  Resets the traffic level to the default level for the associated overload action.

```
activate traffic-level traffic-level
```

The system rejects new requests to activate PDP contexts if the defined traffic-level is exceeded.

*traffic-level*: An integer 1 to 15.
Default: 14

```
attach traffic-level traffic-level
```

The system rejects new requests for GPRS attach if the defined traffic-level is exceeded.

*traffic-level*: An integer 1 to 15.
Default: 15

```
auth-challenge traffic-level traffic-level
```

The system skips performing authentication challenges if the defined traffic-level is exceeded.

*traffic-level*: An integer 1 to 15.
Default: 4
modify-request traffic-level

The system rejects requests to modify a PDP context if the defined traffic-level is exceeded.

traffic-level: An integer 1 to 15.
Default: 12

paging-downlink-data traffic-level traffic-level

If the defined traffic-level is exceeded, then paging is not performed for data during downlinks if RABs are not available.

traffic-level: An integer 1 to 15.
Default: 11

ptmsi-reallocation traffic-level traffic-level

The system skips performing ptmsi-reallocation if the defined traffic-level is reached or exceeded.

traffic-level: An integer from 1 to 15.
Default: 4

service-request-data traffic-level traffic-level

The system rejects service requests to accept data and establish new RABs if the defined traffic-level is reached or exceeded.

traffic-level: An integer from 1 to 15.
Default: 10

sms traffic-level traffic-level

The system rejects SMS signaling if the defined traffic-level is reached or exceeded.

traffic-level: An integer 1 to 15.
Default: 8

srns traffic-level traffic-level

The SGSN rejects/disables SRNS if the target RNC is in overload at the specified traffic level. This keyword setting is effective for both Inter-SGSN SRNS and Intra-SGSN SRNS.

traffic-level: An integer 1 to 15.
Default: 15

Usage

This command defines traffic levels and the actions to take if traffic exceeds the defined levels. The command can be re-entered multiple times to create individual definitions for each type of traffic level and action.

Example

Use the following to instruct the system to reject service requests to establish new RABs if the traffic level reaches 3:

overload-action disable service-request-data traffic-level 3
paging-non-searching-indication

This command instructs the SGSN to include the non-searching indicator flag in the page-request message.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > luPS Service Configuration > RNC Configuration
configure > context context_name > iups-service service_name > rnc id rnc_id
Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx-iups-service-rnc)#

Syntax

paging-non-searching-indication { non-searching | searching }

[ no | default ] paging-non-searching-indication

<table>
<thead>
<tr>
<th>no</th>
<th>default</th>
</tr>
</thead>
</table>
| This is the default. Entering no or default with this command disables the inclusion of the flag.

<table>
<thead>
<tr>
<th>non-searching</th>
</tr>
</thead>
</table>
| Set the non-searching-indication to non-searching in the page-request message.

<table>
<thead>
<tr>
<th>searching</th>
</tr>
</thead>
</table>
| Set the non-searching-indication to searching in the page-request message.

Usage

Use this command to determine which type of search indicator flag will be included in the page-request message.

Example

Use this command to include the non-searching flag in page-request messages:

    paging-non-searching-indication non-searching
pointcode

Configures the point code of the RNC.

The access protocol that is part of the IuPS Service configuration mode must be configured prior to defining the RNC’s point code.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > IuPS Service Configuration > RNC Configuration

configure > context context_name > iups-service service_name > rnc id rnc_id

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx-iups-service-rnc)#

Syntax

pointcode pt_code

no pointcode

no

Deletes the RNC’s point code information from the system configuration.

pt_code

Point code in dotted-decimal format:

•ITU Range 0.0.1 to 7.255.7
•ANSI Range 0.0.1 to 255.255.255
•TTC Range 0.0.1 to 15.31.255
•string of 1 to 11 characters

Usage

Use this command to identify the point code of the associated RNC.

Example

Identify the pointcode for this RNC as 1.234.2:

pointcode 1.234.2
pooled

Configure an RNC as either ‘pooled’ or ‘non-pooled’.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > luPS Service Configuration > RNC Configuration

\[ \text{configure} \] > context context_name > iups-service service_name > rnc id rnc_id

Entering the above command sequence results in the following prompt:

\[[context_name]host_name(config-ctx-iups-service-rnc)\#

**Syntax**

\[ \text{pooled} \]

\[ \text{[default | no] pooled} \]

\[ \text{default | no} \]

Entering either \text{default} or \text{no} returns the RNC configuration to the default ‘non-pooled’ state.

**Usage**

Each RNC, one-at-a-time, can be identified as ‘pooled’ -- as participating within an SGSN pool -- or ‘non-pooled’. Pooled RNCs can co-exist with non-pooled RNCs.

**Example**

Identify this RNC as being part of an SGSN pool:

\[ \text{pooled} \]
rab-asymmetry-indicator

Configures the SGSN to force “Asymmetric-Bidirecitonal” as the RAB Asymmetry Indicator when uplink/downlink bitrates are equal.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > 1uPS Service Configuration > RNC Configuration

configure > context context_name > iups-service service_name > rnc id rnc_id

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx-iups-service-rnc)#

Syntax

rab-asymmetry-indicator symmetric-bidirectional force-asymmetric-bidirectional

no rab-asymmetry-indicator symmetric-bidirectional force-asymmetric-bidirectional

default rab-asymmetry-indicator

    default | no

Disables the override and sets the indicator based on the symmetry of the bitrates as described for the Default Functionality below.

Usage

This command defines an override that uses “Asymmetric-Bidirecitonal” as the RAB Asymmetry Indicator when uplink/downlink bitrates are equal (default functionality item #1). This overrides the default functionality (see below) for the RAB indicator in the RAB Assignment Request. As a result of using this override command, two sets of bitrates, one for downlink and one for uplink, will be included in RAB Assignment Requests for establish or modify per 3GPP TS 25.413.

Default Functionality: The SGSN sets the value of the RAB Asymmetry Indicator based on symmetry of negotiated maximum bitrates in the following manner:

• If the uplink and downlink bitrates are equal, then it is set to “Symmetric-Bidirectional”.
• If uplink bitrate is set to 0 kbps, then it is set to “Asymmetric-Unidirectional-Downlink”.
• If downlink bitrate is set to 0 kbps, then it is set to “Asymmetric-Unidirectional-Uplink”.
• If the uplink and downlink bitrates are non-zero and different, then it is set to “Asymmetric-Bidirectional”.

Example

Override the use of the “Symmetric-Bidirecitonal” RAB Asymmetry Indicator for equal up/downlink bitrates with the following command:
rab-asymmetry-indicator symmetric-bidirectional force-asymmetric-bidirectional

Disable the override with the following command:

    no rab-asymmetry-indicator symmetric-bidirectional force-asymmetric-bidirectional
rab-modify-procedure

This command configures how the RAB (radio access bearer) assignment procedure will be modified.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > IuPS Service Configuration > RNC Configuration
configure > context context_name > iups-service service_name > rnc id rnc_id

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx-iups-service-rnc)#

Syntax


default rab-modify-procedure

no rab-modify-procedure normal-modify [ data-vol-report-ind-ie | pdp-type-info-ie ]

default

Resets the configuration to use ‘release-and-establish’, the SGSN’s default RAB Assignment modification procedure.

normal-modify

Selects the normal modification procedure for RAB assignment. Either one of two IE options can be included:

*data-vol-report-ind-ie sends the “Data Volume Reporting Indication IE” as part of the modification request of the RAB Assignment Request procedure.

*pdp-type-info-ie sends the "PDP Type Information IE" as part of the modification request of the RAB Assignment Request procedure.

release-and-establish

Instructs the system to release and establish the RAB procedure.

Usage

Set the type of modification procedure to be used to establish the radio access bearer (RAB) assignment. The command can be issued multiple times to configure either or both IEs for ‘normal-modify’ procedure. The effect of adding the no prefix to the command depends on the keyword options included with the command:
• no rab-modify-procedure normal-modify disables a previously configured normal modify procedure and sets the configuration to use the default RAB Assignment modification procedure (i.e., release-an-establish).

• no rab-modify-procedure normal-modify data-vol-report-ind-ie changes the configuration to disable sending "Data Volume Reporting Indication IE" in the RAB Assignment request for modification. NOTE: This command does not change the use of the normal RAB modification procedure (i.e., normal-modify).

• no rab-modify-procedure normal-modify pdp-type-info-ie changes the configuration to disable sending "PDP Type Information IE" in the RAB Assignment request for modification. NOTE: This command does not change the use of the normal RAB modification procedure (i.e.: normal-modify).

Use either of the following commands to verify the current configuration for type of RAB Assignment modification procedure, and if optional IEs are to be used:

• show configuration verbose
• show iups-service

Example

Use the following command to enable ‘normal-modify’ as the modification procedure to be used for RAB Assignment:

    rab-modify-procedure normal-modify

Use the following command to configure ‘release-establish’ as the modification procedure to be used by the SGSN for RAB Assignments:

    default rab-modify-procedure

Use the following command to enable the “Data Volume Reporting Indication IE” as part of the normal modification request of the RAB Assignment Request procedure.

    rab-modify-procedure normal-modify data-vol-report-ind-ie
ranap arp-ie

This command enables or disables the inclusion of ARP-IE in RAB assignment / Relocation request RANAP messages per RNC.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > LuPS Service Configuration > RNC Configuration
configure > context context_name > iups-service service_name > rnc id rnc_id

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx-iups-service-rnc)#

Syntax

    ranap arp-ie

    [ default | no ] ranap arp-ie

---

**default**

Returns the configuration to the default setting, the inclusion of ARP-IE in RAB assignment / Relocation request RANAP messages is disabled.

---

**no**

Disables the inclusion of ARP-IE in RAB assignment / Relocation request RANAP messages per RNC.
ranap eutran-service-handover-ie

Enables/disables the inclusion of the E-UTRAN Service Handover Information Element in RAB Assignment Request messages (during the PDP activation phase) and Relocation Request RANAP messages (during the SRNS relocation phase). This ensures that an SRNS relocation handover to E-UTRAN is not allowed for E-UTRAN capable UEs that have only a UTRAN/GERAN roaming agreement in place.

Product
SGSN

Privilege
Administrator, Security Administrator

Mode
Exec > Global Configuration > Context Configuration > lUPS Service Configuration > RNC Configuration

configure > context context_name > iups-service service_name > rnc id rnc_id

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx-iups-service-rnc)#

Syntax

ranap eutran-service-handover-ie

[ default | no ] ranap eutran-service-handover-ie

---

ranap eutran-service-handover-ie

Enables the inclusion of the E-UTRAN Service Handover Information Element in RAB Assignment Request (during the PDP activation phase) and Relocation Request RANAP messages (during the SRNS relocation phase). The IE in the RAB Assignment Request during the PDP activation phase informs the RNC not to handover the subscriber to E-UTRAN. The IE in Relocation Request is sent when there is an intra-SGSN SRNS or inter-SGSN SRNS relocation within the UTRAN itself so that the target RNC knows that it shall not handover the subscriber to E-UTRAN.

no ranap eutran-service-handover-ie

Specifies that the SGSN will not include the E-UTRAN Service Handover IE in RAB Assignment Request and Relocation Request RANAP messages.

default

Returns the configuration to the default setting. The inclusion of the E-UTRAN Service Handover Information Element in RAB Assignment Request and Relocation Request RANAP messages is disabled.

no

Disables the inclusion of the E-UTRAN Service Handover Information Element in RAB Assignment Request and Relocation Request RANAP messages is disabled.

Usage

Use this feature to prevent handovers to E-UTRAN in the following scenarios:
1. A UE is E-UTRAN capable, the PLMN is E-UTRAN capable, but the UE has not subscribed to EPS services (no 4G subscription available).

2. The VPLMN is E-UTRAN-capable, and the UE of an inbound roamer is E-UTRAN capable, but the UE has only a UTRAN/GERAN roaming agreement in place. Enabling this parameter helps ensure that an SRNS relocation handover to E-UTRAN is not allowed for E-UTRAN capable UEs that have only a UTRAN/GERAN roaming agreement. This results in an elimination of potential service denial or disruption issues, and unnecessary signaling. The following commands and features must be executed before enabling the `ranap eutran-service-handover-ie` setting:

   - The SRNS relocation feature must be configured in Call Control Profile Configuration Mode via the `srns-inter` and/or `srns-intra` commands.
   - The `eutran-not-allowed` flag must be enabled in the access-restriction-data command in Call Control Profile Configuration Mode.
   - The call-control-profile must then be associated with an operator policy via the `associate` command in Operator Policy Configuration Mode.

**Example**

This example enables the inclusion of the E-UTRAN Service Handover IE in RAB Assignment Request and Relocation Request RANAP messages.

```
ranap eutran-service-handover-ie
```
ranap global-cn-id

This command configures the SGSN to use include the Global Core Network ID IE in the various messages.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > luPS Service Configuration > RNC Configuration

```
configure > context context_name > iups-service service_name > rnc id rnc_id
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service-rnc)#
```

**Syntax**

```
ranap global-cn-id { paging-request | relocation-request | reset-procedure | reset-resource-procedure } [ network-sharing selected-plmn ]

[ default | no ] ranap global-cn-id { paging-request | relocation-request }
```

---

**default**

Returns the configuration to the default setting and sends the common-plmn in the Global CN ID IE.

**no**

Disables sending the Global CN ID IE.

**paging-request**

Instructs the SGSN to send the Global CN ID IE in the Paging Request message.

**relocation-request**

Instructs the SGSN to send the Global CN ID IE in the Relocation Request message.

**reset-procedure**

Instructs the SGSN to send the Global CN ID IE in the Reset/Ack message.

**reset-resource-procedure**

Instructs the SGSN to send the Global CN ID IE in the Reset-Resource/Ack message.

**network-sharing selected-plmn**

Instructs the SGSN to send the selected-plmn in the Global CN ID IE if network sharing has been enabled.
### Usage

Use this command to configure the SGSN to use ‘selected-plmn’ in the Global Core Network ID IE in various messages when network sharing is enabled.

### Example

Use the following command to include the global-cn-id IE in a Paging Request with the common PLMN when network sharing is enabled:

```
default ranap global-cn-id paging-request
```

Use the following command to include global-cn-id IE in Relocation Request with the selected-plmn (assumes network sharing has been enabled):

```
ranap global-cn-id relocation-request network-sharing selected-plmn
```
**ranap paging-area-id**

This command configures the SGSN to use include the Paging Area ID IE in the Paging Request message.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > luPS Service Configuration > RNC Configuration

`configure > context context_name > iups-service service_name > rnc id rnc_id`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service-rnc)#
```

**Syntax**

```
ranap paging-area-id paging-request [ network-sharing selected-plmn ]

[ default | no ] ranap paging-area-id paging-request [ network-sharing selected-plmn ]
```

<table>
<thead>
<tr>
<th><strong>default</strong></th>
<th>Returns the configuration to the default setting and sends the common-plmn in the Paging Area ID IE.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>no</strong></td>
<td>Disables sending the Paging Area ID IE.</td>
</tr>
</tbody>
</table>

**Usage**

Use this command to configure the SGSN to use ‘selected-plmn’ in the Paging Area ID IE in the Paging Request message when network sharing is enabled.

**Example**

Use the following command to include the paging-area-id IE in a Paging Request with the common PLMN when network sharing is enabled:

```
default ranap paging-area-id paging-request
```

Use the following command to include global-cn-id IE in Paging Request with the selected-plmn (assumes network sharing has been enabled):

```
ranap global-cn-id paging-request network-sharing selected-plmn
```
ranap paging-cause-ie

This command sets the paging cause value and either includes or suppresses the Paging Cause IE in responses to Paging Requests due to various sources. This command is available in releases 8.1 and higher.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > luPS Service Configuration > RNC Configuration
configure > context context_name > iups-service service_name > rnc id rnc_id

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service-rnc)#
```

**Syntax**

```
```

---

**default**

Resets the specific parameters value to default.

**no**

Suppresses the Paging Cause IE so that it is not included in responses to Paging Requests from respective sources.

**all**

Using **all** sets the action for the Paging Cause IE value for all paging due to all sources.

**background-data [ value ]**

Default: 3 (terminating background call)
Set the Paging Cause IE value for paging due to background data.

\[value\]: Must be an integer from 0 to 5. See Paging Cause value mapping in Usage section.

**conversational-data [ value ]**

Default: 5 (terminating high priority signaling)
Set the Paging Cause IE value for paging due to conversational data.

\[value\]: Must be an integer from 0 to 5. See Paging Cause value mapping in Usage section.
gmm-signalling [ value ]

Default: 5 (terminating high priority signaling)
Set the Paging Cause IE value for paging due to gmm-signaling.
value: Must be an integer from 0 to 5. See Paging Cause value mapping in Usage section.

gs-signalling [ value ]

Default: 5 (terminating high priority signaling)
Set the Paging Cause IE value for paging due to VLR Paging Request.
value: Must be an integer from 0 to 5. See Paging Cause value mapping in Usage section.

interactive-data [ value ]

Default: 2 (terminating interactive call)
Set the Paging Cause IE value for paging due to interactive data.
value: Must be an integer from 0 to 5. See Paging Cause value mapping in Usage section.

mme-signalling [ value ]

Default: 5 (terminating high priority signaling)
Sets the Paging Cause IE value for paging from MME due to Circuit Switch Fallback (CSFB).
value: Must be an integer from 0 to 5. See Paging Cause value mapping in Usage section.

sm-signalling [ value ]

Default: 5 (terminating high priority signaling)
Set the Paging Cause IE value for paging due to SM signaling.
value: Must be an integer from 0 to 5. See Paging Cause value mapping in Usage section.

sms-signalling [ value ]

Default: 4 (terminating low priority signaling)
Set the Paging Cause IE value for paging due to SMS signaling.
value: Must be an integer from 0 to 5. See Paging Cause value mapping in Usage section.

streaming-data [ value ]

Default: 5 (terminating high priority signaling)
Set the Paging Cause IE value for paging due to streaming data.
value: Must be an integer from 0 to 5. See Paging Cause value mapping in Usage section.

Usage

This command can be used to set the value (meaning) of the Paging Cause IE included in responses to Paging Requests or it can be used to suppress the inclusion of the Paging Cause IE in the responses. These actions can be configured for paging for all sources or for a specified source.
The following values are applicable to all Paging Cause IEs:

- **0**: Terminating conversational call
- **1**: Terminating streaming call
- **2**: Terminating interactive call
- **3**: Terminating background call
- **4**: Terminating low priority signaling
- 5 - Terminating high priority signaling

**Example**

Use the following command to set Paging Cause value to 3 for paging due to GMM signaling without affecting cause values for other sources:

```
ranap paging-cause-ie gmm-signalling 3
```

Use the following command to suppress the Paging Cause IE from all Paging Requests to the RNC:

```
no ranap paging-cause-ie all
```

Either of the following commands will cause the Paging Cause IE to be included in Paging Requests with the default value for SM signaling without affecting the cause for other sources:

```
ranap paging-cause-ie sm-signalling
default ranap paging-cause-ie sm-signalling
```
**ranap signalling-indication-ie**

This command enables/disables the inclusion of the Signaling Indication IE in either or both the RAB Assignment Request and/or the Relocation Request RANAP messages.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > luPS Service Configuration > RNC Configuration

```
configure > context context_name > iups-service service_name > rnc id rnc_id
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service-rnc)#
```

**Syntax**

```
ranap signalling-indication-ie { rab-assignment-request [ relocation-request ] | relocation-request [ rab-assignment-request ] }

no ranap signalling-indication-ie

default ranap signalling-indication-ie
```

- **no**
  Sets the configuration so that the SGSN never includes the IE.

- **default**
  Resets the configuration to the default - the SGSN includes the IE in the messages if preconditions are met (see Usage section).

- **rab-assignment-request | relocation-request**
  Including one or both of these keywords configures what type of RANAP message will include the IE.

**Usage**

The command enables the operator to determine whether the signalling indication information element is included in either or both the RAB Assignment Request and Relocation Request messages during the PDP context setup procedure.

For this command configuration to work so that the IE is included, two preconditions must be met:

- Received QoS traffic class for the context must be interactive
- Received QoS has a signalling indication value as optimized

When an RNC receives this IE, the RNC assumes that the customer is using IMS signaling and allocates massive amounts of bandwidth, potentially causing cell congestion. This command enables the operator to determine the usage of this IE which provides the operator with additional session management control.

**Example**
Use the following command to include the signalling indication IE in the RAB Assignment Request:

```
ranap signalling-indication-ie rab-assignment-request
```
**ran-information-management**

Use this command to inform the SGSN which RNC are capable of handling RAN information management (RIM) messages.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > luPS Service Configuration > RNC Configuration

```bash
configure > context context_name > iups-service service_name > rnc id rnc_id
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service-rnc)#
```

**Syntax**

```
[ default | no ] ran-information-management
```

- **default**
  
  Resets the default so RIM is disabled.

- **no**
  
  Disables the RIM support in the configuration file.

**Usage**

By default, handling of RAN information management (RIM) messages is disabled. This command informs the SGSN which RNC are capable of handling RIM messages. This configuration only becomes ‘operational’ if the `ran-information-management` command is enabled in the SGSN global configuration mode.

When RIM support is enabled on both the SGSN and the destination node, then all RIM PDUs are forwarded to the BSC/RNC. If RIM message handling is not enabled on both nodes, then the RIM PDUs are dropped silently.

**Example**

Use the following command to enable RIM support:

```
ran-information-management
```

Use the following command to disable RIM support that has been added to the configuration:

```
no ran-information-management
```
release-compliance

This command allows the SGSN to set support based on the RNC’s 3GPP release compliance and to define per RNC QoS overrides.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > luPS Service Configuration > RNC Configuration

```bash
configure > context context_name > iups-service service_name > rnc id rnc_id
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ctx-iups-service-rnc)#
```

**Syntax**

```bash
release-compliance { pre-release-7 | release-7 } [ gbr-down gbr_dn_val | gbr-up gbr_up_val | mbr-down mbr_dn_val | mbr-up mbr_up_val ] +
```

default release-compliance

<table>
<thead>
<tr>
<th>default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Returns the configuration to the default value, release-7.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>pre-release-7</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enables support for an RNC with capabilities compliant with releases prior to Release 7, such as HSPA in R6.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>release-7</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enables support for RNC with capabilities compliant with 3GPP Release 7 or later, such as HSPA+ available in R7.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>gbr-down gbr_dn_val</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defines a guaranteed kbps bit rate for downlink direction,</td>
</tr>
<tr>
<td>• options for pre-release-7 include: 16, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192, 11500, 16000. Default cap is 16000.</td>
</tr>
<tr>
<td>• options for release-7 include: 16, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192, 11500, 16000, 21000, 28000, 42000. See default cap information below.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>gbr-up gbr_up_val</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defines a guaranteed kbps bit rate for uplink direction,</td>
</tr>
<tr>
<td>• options for pre-release-7 include: 16, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192, 11500, 16000. Default cap is 16000.</td>
</tr>
</tbody>
</table>
• options for `release-7` include: 16, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192, 11500, 16000, 21000, 28000, 42000. See default cap information below.

**mbr-down mbr_dn_val**

Defines a maximum kbps bit rate for downlink direction,

• options for `pre-release-7` include: 16, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192, 11500, 16000. Default cap is 16000.

• options for `release-7` include: 16, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192, 11500, 16000, 21000, 28000, 42000. See default cap information below.

**mbr-up mbr_up_val**

Defines a maximum kbps bit rate for uplink direction,

• options for `pre-release-7` include: 16, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192, 11500, 16000. Default cap is 16000.

• options for `release-7` include: 16, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192, 11500, 16000, 21000, 28000, 42000. See default cap information below.

**Usage**

Use this command to match the 3GPP release support by the RNC. As the 3GPP releases each support differing data rate options - R6 supports HSPA and R7 supports HSPA+ - then selecting the compliance is a method of preforming data rate management on a per RNC basis. Also use this command to set QoS capping overrides for each RNC separately. Default caps for Release 7 RNC will vary depending upon which overrides are set.

**Important:** Once caps are set for an RNC, if the RNC release level changes the capping remains the same until the QoS override values are changed for that RNC. Values do not automatically change to the default values appropriate for that release.

**Example**

Enable HSPA fallback to R6 compliance:

```
release-compliance pre-release-7
```
reset-resource

This command enables the operator to control message length by configuring the number of IuConIDs sent in each RANAP Reset Resource messages.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > IuPS Service Configuration > RNC Configuration

configure > context context_name > iups-service service_name > rnc id rnc_id

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-ctx-iups-service-rnc)#

Syntax

reset-resource max-iuconid-per-msg number

default reset-resource max-iuconid-per-msg

default
Resets the number of Iu connection Ids included in the Reset Resource messages. Default is 250.

max-iuconid-per-msg number
Sets the number of Iu connection Ids to be included in the Reset Resource messages.

number: Integer from 1 to 250.
Default: 250

Usage
Id numbers for each Iu connection are included in the RANAP Reset Resource messages. Including this potentially long stream of numbers can make the message very long. With this command, the operator can control the size of the messages by controlling the number of Id messages included in the messages.

Example
Limit the number of Iu connection IDs to 30:

       reset-resource max-iuconid-per-msg 30
Chapter 265
RoHC Profile Common Options Configuration Mode Commands

The RoHC Profile Common Options Configuration Mode is used to set timers that, upon expiration, release robust header compression contexts.

Mode
Exec > Global Configuration > RoHC Profile Configuration > RoHC Profile Common Options Configuration

configure > rohc-profile profile-name profile_name > compression-options

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-rohcprofile-profile_name-common)#

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
delay-release-hc-context-timer

Sets a delay in releasing Robust Header Compression (RoHC) contexts allowing for context continuation during intra-gateway handoffs.

Product
HSGW
PDSN

Privilege
Administrator

Mode
Exec > Global Configuration > RoHC Profile Configuration > RoHC Profile Common Options Configuration

configure > rohc-profile profile-name profile_name > compression-options

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-rohcprofile-profile_name-common)#

Syntax

delay-release-hc-context-timer seconds

no delay-release-hc-context-timer

no
- Removes previously configured value for this command. No value disables the feature.

seconds
- Specifies the number of seconds the system delays before releasing the header compression context as an integer from 0 to 65535.

Usage

Use this command to set a delay in releasing a header compression context. This command is necessary when employing RoHC and mobility. Typically, when an RP connection is released, the header compression context is also released immediately. However, in mobility situations, such as intra-PDSN handoffs, the header compression context should be preserved. Adding a delay to cover the handoff time allows the context to be maintained.

A header compression context contains the compression/decompression configuration and statistics for the session.

Example

The following command sets the header compression release delay to 20 seconds:

delay-release-hc-context-timer 20
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
end

**Usage**
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Use this command to return to the parent configuration mode.
inactive-traffic-release-hc-context-timer

Sets an inactivity timer that is checked when inactivity is detected on an SO67 A10 bearer connection with negotiated RoHC parameters. When this timer expires, the header compression context is released.

**Product**
HSGW
PDSN

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > RoHC Profile Configuration > RoHC Profile Common Options Configuration

```plaintext
configure > rohc-profile profile-name profile_name > compression-options
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-rohcprofile-profile_name-common)#
```

**Syntax**

```
inactive-traffic-release-hc-context-timer seconds
```

```
o inactive-traffic-release-hc-context-timer
```

**Usage**
Use this command to set a timer that is started upon detecting inactivity on the bearer channel. Upon expiry, the header compression context is released. Enable this feature for more efficient memory utilization.

**Example**
The following command sets the bearer channel inactivity timer to 60 seconds:

```
inactive-traffic-release-hc-context-timer 60
```
Chapter 266
RoHC Profile Compression Configuration Mode Commands

The RoHC Profile Compression Configuration Mode is used to configure RoHC (Robust Header Compression) Compressor parameters. RoHC is not supported on GGSN.

Mode

Exec > Global Configuration > RoHC Profile Configuration > RoHC Profile Compression Configuration

configure > rohc-profile profile-name profile_name > compression-options

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-rohcprofile-profile_name-comp)#

Important: The availability of commands, keywords and variables in this mode are dependent on platform type, product version, and installed license(s).
context-timeout

Context timeout in seconds.

Product

- HSGW
- PDSN

Privilege

Administrator

Mode

Exec > Global Configuration > RoHC Profile Configuration > RoHC Profile Compression Configuration
configure > rohc-profile profile-name profile_name > compression-options

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-rohcafterrofiprofile-name-comp)#

Syntax

context-timeout seconds

default context-timeout

default

Returns the command to its default value.

seconds

Specifies the context timeout value (in seconds) as an integer from 0 through 100.
Default: 20

Usage

Use this command to set the context timeout.

Example

The following command sets the context timeout to 10 seconds:

context-timeout-period 10
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

dend

**Usage**
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Use this command to return to the parent configuration mode.
ipid-history-size

Specifies the number of IP-IDs of previously sent packets to store. An IP ID is a 16-bit header field that stores IPv4 Identification information.

Product
HSGW
PDSN

Privilege
Administrator

Mode
Exec > Global Configuration > RoHC Profile Configuration > RoHC Profile Compression Configuration
configure > rohc-profile profile-name profile_name > compression-options

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-rohcprofile-profile_name-comp)#

Syntax

ipid-history-size number

default ipid-history-size

____________
default
Returns the command to its default value.

____________

number
Specifies the number of IP IDs to store as an integer from 1 through 32.
Default: 8

Usage
Use this command to set the number of IP IDs to store in the history.

Example
The following command sets the history size to 24 IP-IDs:

ipid-history-size 24
max-jitter-cd

Specifies the upper boundary of jitter expected on the communication channel between the compressor and decompressor.

Product

HSGW
PDSN

Privilege

Administrator

Mode

Exec > Global Configuration > RoHC Profile Configuration > RoHC Profile Compression Configuration
configure > rohc-profile profile-name profile_name > compression-options

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-rohcprofile-profile_name-comp)#

Syntax

max-jitter-cd num_ms

default max-jitter-cd

default

Returns the command to its default value.

num_ms

Specifies the number of milliseconds for the maximum jitter setting as an integer from 0 through 999999999. Default: 150

Usage

Use this command to set the maximum amount of jitter allowed on the communication channel between compressor and decompressor.

Example

The following command sets the jitter limit to 1000 ms (1 second):

max-jitter-cd 1000
max-sliding-window

Specifies the width of the sliding window for W-LSB (Windows-based Least Significant Bits) encoded values.

Product
HSGW
PDSN

Privilege
Administrator

Mode
Exec > Global Configuration > RoHC Profile Configuration > RoHC Profile Compression Configuration
configure > rohc-profile profile-name profile_name > compression-options

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-rohcprofile-profile_name-comp)#

Syntax

max-sliding-window size

default max-sliding-window

default
Returns the command to its default value.

size
Specifies the size of the sliding window as an integer from 1 through 1000.
Default: 6

Usage
Use this command to set the size of the sliding window used to compute jitter for W-LSB encoded values.

Example
The following command sets the sliding window size to 500:

max-sliding-window 500
multiple-ts-stride

Enables or disables the use of repeated transmission of RTS_STRIDE for timer-based compression.

**Product**
- HSGW
- PDSN

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > RoHC Profile Configuration > RoHC Profile Compression Configuration
`configure > rohc-profile profile-name profile_name > compression-options`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-rohcrpofile-profile_name-comp)#
```

**Syntax**

```
[ no ] multiple-ts-stride
```

<table>
<thead>
<tr>
<th>no</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disables the use of repeated transmission of RTS_STRIDE for time-based compression.</td>
</tr>
</tbody>
</table>

**Usage**

Use this command to enable or disable a gateway’s ability to repeatedly transmit RTS_STRIDE for timer-based compression.
new-context-blocking-time

Specifies the time period in seconds for blocking the establishment of new contexts after the compressor has received a feedback reject.

Product

HSGW

PDSN

Privilege

Administrator

Mode

Exec > Global Configuration > RoHC Profile Configuration > RoHC Profile Compression Configuration

compress > rohc-profile profile-name profile_name > compression-options

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-rohcprofile-profile_name-comp)#

Syntax

new-context-blocking-time seconds

default context-timeout

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Returns the command to its default value.</td>
</tr>
<tr>
<td>seconds</td>
<td>Specifies the context blocking time (in seconds) as an integer from 0 through 100. Default: 20</td>
</tr>
</tbody>
</table>

Usage

Use this command to set the context blocking time after the compressor has received a feedback reject.

Example

The following command sets the context blocking time to 10 seconds:

```
new-context-blocking-time 10
```
num-pkts-ts

Specifies the number packets per RTP timestamp (TS).

Product
HSGW
PDSN

Privilege
Administrator

Mode
Exec > Global Configuration > RoHC Profile Configuration > RoHC Profile Compression Configuration
configure > rohc-profile profile-name profile_name > compression-options

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-rohcpprofile-profile_name-comp)#

Syntax

num-pkts-ts num_pkts

default num-pkts-ts

---------------------------------------------------------------

default
Returns the command to its default value.

---------------------------------------------------------------

num_pkts
Specifies the number of packets for the timestamp as an integer from 0 through 999.
Default: 6

Usage

Use this command to set the number of packets for each RTP timestamp (TS).

Example

The following command sets the number of packets per timestamp to 50:

num-pkts-ts 50
**num-pkts-u-mode**

Specifies the number of packets sent when operating in U-Mode (unidirectional mode).

**Product**
HSGW
PDSN

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > RoHC Profile Configuration > RoHC Profile Compression Configuration

configure > rohc-profile profile-name profile_name > compression-options

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-rohcprofile-profile_name-comp)#
```

**Syntax**

```
num-pkts-u-mode num_pkts

default num-pkts-u-mode

default

Returns the command to its default value.

```

**num_pkts**

Specifies the number of packets sent in U-Mode as an integer from 0 through 999.
Default: 1

**Usage**

Use this command to set the number of packets sent when in U-Mode.

**Example**

The following command sets the number of packets for U-Mode to 50:

```
um-pkts-u-mode 50```
num-updates-ir

Configures the number of IR (Initiation and Refresh state) updates.

**Product**
- HSGW
- PDSN

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > RoHC Profile Configuration > RoHC Profile Compression Configuration
configure > rohc-profile profile-name profile_name > compression-options

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-rohcprofile-profile_name-comp)#
```

**Syntax**

```
num-updates-ir num_pkts

default num-updates-ir
```

**default**

Returns the command to its default value of 4.

```
num_pkts
```

Specifies the number of IR updates as an integer from 0 through 999.
Default: 4

**Usage**

Use this command to set the number of IR updates.

**Example**

The following command sets the number of IR updates to 30:
```
num-updates-ir 30
```
optimistic-repeats

Specifies the number of repeated packets to send to the decompressor. For transition from the FO (First Order) to the SO (Second Order) state, the compressor should be confident that the decompressor has all the parameters needed to decompress according to a fixed pattern. The compressor obtains its confidence about decompressor status by sending several packets with the same information according to the lower compression state. If the decompressor receives any of these packets, it is in sync with the compressor.

Product
HSGW
PDSN

Privilege
Administrator

Mode
Exec > Global Configuration > RoHC Profile Configuration > RoHC Profile Compression Configuration

configure > rohc-profile profile-name profile_name > compression-options

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-rohcuprofile-profile_name-comp)#

Syntax

optimistic-repeats num_pkts

default optimistic-repeats

default

Returns the command to its default value.

num_pkts

Specifies the number of packets to repeat with the same information to assure synchronization with the decompressor.

num_pkts must be an integer from 0 through 10.
Default: 6

Usage

Use this command to set the number of packets to repeat to the decompressor to assure synchronization before transition states.

Example

The following command sets the number of repeated packets to 5:

optimistic-repeats 5
rtp-sn-p

Specifies the value of p in RTP SN (RTP Sequence Number) calculation. Least Significant Bits (LSB) encoding is used for header fields whose values are usually subject to small changes. With LSB encoding, the k least significant bits of the field value are transmitted instead of the original field value, where k is a positive integer. After receiving k bits, the decompressor derives the original value using a previously received value as reference (v_ref). The scheme is guaranteed to be correct if the compressor and the decompressor each use interpretation intervals as follows:

- In which the original value resides
- And in which the original value is the only value that has the exact same k least significant bits as those transmitted.

The interpretation interval can be described as a function:

\[ f(v_{\text{ref}}, k) = [v_{\text{ref}} - p, v_{\text{ref}} + (2^k - 1) - p] \]

Where p is an integer.

Syntax

```rtp-sn-p p_value
default rtp-sn-p
```

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Returns the command to its default value.</td>
</tr>
<tr>
<td>p_value</td>
<td>Specifies the value of p in the RTP SN calculation as an integer from 0 through 999. Default: 6</td>
</tr>
</tbody>
</table>

Usage

Use this command to set the value for p when performing the RTP SN calculation.

Example

The following command sets the value of p to 100:

```
rtp-sn-p 100
```
**rtp-sn-p-override**

Enables an override of p in the RTP SN calculation. This is disabled by default.

**Product**
- HSGW
- PDSN

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > RoHC Profile Configuration > RoHC Profile Compression Configuration

```plaintext
configure > rohc-profile profile-name profile_name > compression-options
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-rohcprofile-profile_name-comp)#
```

**Syntax**

```
[ default | no ] rtp-sn-p-override
```

- **default**
  Returns the command to its default value of disabled.

- **no**
  Disables overriding p in RTP SN calculation.

**Usage**

Use this command to enable an override of p in RTP SN calculation.

**Example**

The following command enables the override of p in the RTP SN calculation:

```
rtp-sn-p-override
```
rtp-time-stride

Sets the time interval used for one TS (RTP Time Stamp) stride. This interval is used when timer-based encoding is enabled.

Product
HSGW
PDSN

Privilege
Administrator

Mode
Exec > Global Configuration > RoHC Profile Configuration > RoHC Profile Compression Configuration
  configure > rohc-profile profile-name profile_name > compression-options

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-rohcprofile-profile_name-comp)#

Syntax

rtp-time-stride num_ms

default rtp-time-stride

default

Returns the command to its default value.

num_ms

Specifies the number of milliseconds to use for TS_STRIDE as an integer from 0 through 999999999. Default: 20

Usage

Use this command to set the length of the TS_STRIDE in milliseconds.

Example

The following command sets TS_STRIDE to 100ms:

  rtp-time-stride 100
rtp-ts-deviation

Sets the maximum percentage of deviation allowed for input RTP packets for timer-based compression.

Product
HSGW
PDSN

Privilege
Administrator

Mode
Exec > Global Configuration > RoHC Profile Configuration > RoHC Profile Compression Configuration
configure > rohc-profile profile-name profile_name > compression-options

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-rohcprofile-profile_name-comp)#

Syntax

rtp-ts-deviation percentage

default rtp-ts-deviation

default
Returns the command to its default value of 25.

percentage
Specifies the maximum percentage of deviation allowed for input RTP packets for timer-based compression as an integer value from 0 through 100.
Default: 25

Usage

Use this command to set the maximum percentage of deviation allowed for input RTP packets for timer-based compression.

Example

The following command sets the percentage to 30:

rtp-ts-deviation 30
**rtp-ts-stride**

Specifies the amount by which TS (RTP time stamp) is incremented. This value is used for Scaled RTP TS encoding.

**Product**
- HSGW
- PDSN

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > RoHC Profile Configuration > RoHC Profile Compression Configuration
configure > rohc-profile profile-name profile_name > compression-options

Entering the above command sequence results in the following prompt:

```
[context_name] host_name(config-rohcprofile-profile_name-comp)#
```

**Syntax**

```
rtp-ts-stride num_ms
```

```
default rtp-ts-stride
```

**default**
Returns the command to its default value of 160.

```
num_ms
```

Specifies the number of milliseconds to use incrementing TS as an integer from 0 through 999999999. Default: 160

**Usage**

Use this command to set the amount by which TS is incremented for Scaled RTP TS encoding.

**Example**

The following command sets amount by which TS is incremented to 100ms:

```
rtp-ts-stride 100
```
sliding-window-ts

Sets the sliding window used to compute jitter.

Product
HSGW
PDSN

Privilege
Administrator

Mode
Exec > Global Configuration > RoHC Profile Configuration > RoHC Profile Compression Configuration

configure > rohc-profile profile-name profile_name > compression-options

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-rohc-profile-profile_name-comp)#

Syntax

sliding-window-ts size

default sliding-window-ts

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Returns the window to its default value of 4.</td>
</tr>
<tr>
<td>size</td>
<td>Specifies the size of the sliding window as an integer from 1 through 1000. Default: 4</td>
</tr>
</tbody>
</table>

Usage

Use this command to set the size of the sliding window used to compute jitter for the current RoHC profile.

Example

The following command sets the sliding window size to 500:

sliding-window-ts 500
total-jitter-ipv4

Specifies the total jitter allowed after compression for IPv4.

Product
HSGW
PDSN

Privilege
Administrator

Mode
Exec > Global Configuration > RoHC Profile Configuration > RoHC Profile Compression Configuration

configure > rohc-profile profile-name profile_name > compression-options

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-rohcsprofile-profile_name-comp)#

Syntax

total-jitter-ipv4 time

default total-jitter-ipv4

default
default

Returns the command to its default value of 270.

time
time

Specifies the time interval to use (in milliseconds) as an integer from 0 through 999999999. Default: 270

Usage
Use this command to set the jitter limit after compression.

Example
The following command sets the jitter after compression limit to 900 ms:

total-jitter-ipv4 900
total-jitter-ipv6

Specifies the total jitter allowed after compression for IPv6.

Product
HSGW
PDSN

Privilege
Administrator

Mode
Exec > Global Configuration > RoHC Profile Configuration > RoHC Profile Compression Configuration

configure > rohc-profile profile-name profile_name > compression-options

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-rohcprofile-profile_name-comp)#

Syntax

total-jitter-ipv6 time

default total-jitter-ipv6

default
Returns the command to its default value 580.

time
Specifies the total jitter interval allowed (in milliseconds) as an integer from 0 through 999999999. Default: 580

Usage
Use this command to set the jitter limit after compression.

Example
The following command sets the jitter after compression limit to 900 ms:

total-jitter-ipv6 900
unimode-timeout-to-fo-state

Specifies the time period in seconds before falling back to the FO (First Order) state.

Product
HSGW
PDSN

Privilege
Administrator

Mode
Exec > Global Configuration > RoHC Profile Configuration > RoHC Profile Compression Configuration

configure > rohc-profile profile-name profile_name > compression-options

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-rohcprofile-profile_name-comp)#

Syntax

unimode-timeout-to-fo-state num_ms

default unimode-timeout-to-fo-state

default

Returns the command to its default value of 3.

num_ms

Specifies the timeout period (in seconds) as an integer from 0 through 10.
Default: 3

Usage
Use this command to set the timeout before falling back to the FO state when in Unimode.

Example
The following command sets the fall back timeout to 2 seconds:

unimode-timeout-to-fo-state 2
unimode-timeout-to-ir-state

Specifies the time period in seconds before falling back to the IR (Initiation and Refresh) state.

**Syntax**

```
unimode-timeout-to-ir-state num_ms
```

default unimode-timeout-to-ir-state

  default
  Returns the command to its default value of 5.

  num_ms
  Specifies the timeout period in seconds as an integer from 0 through 20.
  Default: 5

**Usage**

Use this command to set the timeout before falling back to the IR state when in Unimode.

**Example**

The following command sets the fall back timeout to 3 seconds:

```
unimode-timeout-to-ir-state 3
```
use-calculated-rtp-time-stride

Overides the configured value of rtp-time-stride with a calculated value.

Product
HSGW
PDSN

Privilege
Administrator

Mode
Exec > Global Configuration > RoHC Profile Configuration > RoHC Profile Compression Configuration

configure > rohc-profile profile-name profile_name > compression-options

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-rohcprofile-profile_name-comp)#

Syntax

[ default | no ] use-calculated-rtp-time-stride

default
Returns the command to its default value of enabled.

no
Disables the use of calculated RTP time stride override.

Usage
This command overrides the configured value of rtp-time-stride with a calculated value.

Example
The following command overrides the configured value of rtp-time-stride.

use-calculated-rtp-time-stride
**use-calculated-rtp-ts-stride**

Overrides the configured value of rtp-ts-stride with a calculated value.

**Product**
- HSGW
- PDSN

**Privilege**
Administrator

**Mode**
- Exec > Global Configuration > RoHC Profile Configuration > RoHC Profile Compression Configuration
- configure > rohc-profile profile-name profile_name > compression-options

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-rohcprofile-profile_name-comp)#
```

**Syntax**

```
[ default | no ] use-calculated-rtp-ts-stride
```

- **default**
  Returns the command to its default value of enabled.

- **no**
  Disables the use of calculated RTP TS time stride override.

**Usage**

This command overrides the configured value of rtp-ts-stride with a calculated value.

**Example**

The following command overrides the configured value of rtp-ts-stride.

```
use-calculated-rtp-ts-stride
```
use-ipid-override

Enables or disables overriding the IP-ID (IPv4 Identification header field).

**Product**

HSGW

PDSN

**Privilege**

Administrator

**Mode**

Exec > Global Configuration > RoHC Profile Configuration > RoHC Profile Compression Configuration

configure > rohc-profile profile-name profile_name > compression-options

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-rohcprofile-profile_name-comp)#`

**Syntax**

```
[ default | no ] use-ipid-override
```

default

Returns the command to its default value of disabled.

no

Disables the IP-ID override.

**Usage**

Use this command to enable overriding of the IP-ID.

**Example**

The following command enables the IP-ID override feature:

```
use-ipid-override
```

The following command disables the IP-ID override feature:

```
no use-ipid-override
```

The following command also disables the IP-ID override feature:

```
default use-ipid-override
```
use-optimized-talkspurt

Enables or disables the use of optimized talkspurt.

**Product**
- HSGW
- PDSN

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > RoHC Profile Configuration > RoHC Profile Compression Configuration

```
configure > rohc-profile profile-name profile_name > compression-options
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-rohcprofile-profile_name-comp)#
```

**Syntax**

```
[ default | no ] use-optimized-talkspurt
```

- **default**
  Returns the command to its default value of enabled.

- **no**
  Disables the use of optimized talkspurt.

**Usage**

Use this command to enable and disable the use of optimized talkspurt.

**Example**

The following command enables the use of optimized talkspurt:

```
use-optimized-talkspurt
```

The following command disables the use of optimized talkspurt:

```
no use-optimized-talkspurt
```
use-optimized-transience

Enables or disables the use of optimized transience.

**Product**
- HSGW
- PDSN

**Privilege**
- Administrator

**Mode**
- Exec > Global Configuration > RoHC Profile Configuration > RoHC Profile Compression Configuration

configure > rohc-profile profile-name profile_name > compression-options

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-rohcprofile-profile_name-comp)#
```

**Syntax**

```
[ default | no ] use-optimized-transience
```

- **default**
  Returns the command to its default value of enabled.

- **no**
  Disables the use of optimized transience.

**Usage**

Use this command to enable or disable the use of optimized transience.

**Example**

The following command enables the use of optimized transience.

```
use-optimized-transience
```

The following command disables the use of optimized transience.

```
no use-optimized-transience
```
use-timer-based-compression

Enables or disables timer-based compression of the RTP time stamp (TS) at the compressor.

**Product**
HSGW
PDSN

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > RoHC Profile Configuration > RoHC Profile Compression Configuration
configure > rohc-profile profile-name profile_name > compression-options

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-rohcprofile-profile_name-comp)#
```

**Syntax**

```
[ default | no ] use-timer-based-compression
```

- **default**
  Returns the command to its default value of enabled.

- **no**
  Disables the use of timer-based compression.

**Usage**
Use this command to enable or disable the use of timer-based compression.

**Example**
The following command enables the use of timer-based compression.

```
use-timer-based-compression
```

The following command disables the use of timer-based compression.

```
no use-timer-based-compression
```
use-uncomp-profile

Enables or disables the use of the Uncompressed Profile (0x0000) if required at the compressor.

**Product**
- HSGW
- PDSN

**Privilege**
- Administrator

**Mode**
- Exec > Global Configuration > RoHC Profile Configuration > RoHC Profile Compression Configuration
- `configure > rohc-profile profile-name profile_name > compression-options`

Entering the above command sequence results in the following prompt:

```
[context_name] host_name(config-rohcpprofile-profile_name-comp)##
```

**Syntax**

```
[default | no ] useS-uncomp-profile
```

- **default**
  - Returns the command to its default value of disabled.

- **no**
  - Disables the use of the Uncompressed Profile.

**Usage**

Use this command to enable or disable the use of the Uncompressed Profile.

**Example**

The following command enables the use of the Uncompressed Profile.

```
use-uncomp-profile
```

The following command disables the use of the Uncompressed Profile.

```
no use-uncomp-profile
```
Chapter 267
RoHC Profile Configuration Mode Commands

The RoHC Profile Configuration Mode is used to configure RoHC (Robust Header Compression) Compressor and Decompressor parameters. The profiles can then be assigned to specific subscriber sessions when RoHC header compression is configured. RoHC is not supported on GGSN.

Mode

Exec > Global Configuration > RoHC Profile Configuration

`configure > rohc-profile profile-name profile_name`

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-rohcprofile-profile_name)#`

Important: The availability of commands, keywords and variables in this mode is dependent on platform type, product version, and installed license(s).
common-options

Enters the RoHC Profile Common Options Configuration Mode where inactivity and delay timers are set to support dynamic header compression contexts and context preservation during handoffs.

Product
HSGW
PDSN

Privilege
Administrator

Mode
Exec > Global Configuration > RoHC Profile Configuration

configure > rohc-profile profile-name profile_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-rohcprofile-profile_name)#

Syntax

[ default ] common-options

default

Reset all parameters in the RoHC Profile Common Options Configuration Mode to default values.

Usage

Use this command to enter the RoHC Profile Common Options Configuration Mode where parameters for maintaining header compression contexts and inactivity timers can be configured.

Entering this command results in the following prompt:

[context_name]host(config-rohcprofile-profile_name-common)#

RoHC Profile Common Options Configuration Mode commands are defined in the RoHC Profile Common Options Configuration Mode Commands chapter.
compression-options

Enters the RoHC Profile Compression Options Configuration Mode allowing configuration of options applied during RoHC compression for the current RoHC profile.

Product
HSGW
PDSN

Privilege
Administrator

Mode
Exec > Global Configuration > RoHC Profile Configuration
configure > rohc-profile profile-name profile_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-rohcprofile-profile_name)#

Syntax

[ default ] compression-options

default
Reset all options in the RoHC Profile Compression Configuration Mode to their default values.

Usage
Use this command to enter RoHC Profile Compression Configuration Mode to set the compression options that are used for subscriber sessions using the current RoHC profile.

Entering this command results in the following prompt:

[context_name]host(config-rohcprofile-profile_name-comp)#

RoHC Profile Compression Options Configuration Mode commands are defined in the RoHC Profile Compression Configuration Mode Commands chapter.

Example

The following command enters RoHC Profile Compression Options Configuration Mode:

compression-options

The following command sets all compression options to their default values:

default compression-options
decompression-options

Enters the RoHC Profile Decompression Options Configuration Mode allowing configuration of options applied during RoHC decompression for the current RoHC profile.

**Product**
- HSGW
- PDSN

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > RoHC Profile Configuration
```
configure > rohc-profile profile-name profile_name
```
Entering the above command sequence results in the following prompt:
```
[context_name]host_name(config-rohcprofile-profile_name)#
```

**Syntax**
```
[default ] decompression-options
```

**Usage**
Use this command to enter RoHC Profile Decompression Options Configuration Mode to set the decompression options used for subscriber sessions using the current RoHC profile.
Entering this command results in the following prompt:
```
[context_name]host(config-rohcprofile<-profile_name>-decomp)#
```
RoHC Profile Decompression Options Configuration Mode commands are defined in the RoHC Profile Decompression Configuration Mode Commands chapter.

**Example**
The following command enters RoHC Profile Decompression Options Configuration Mode:
```
decompression-options
```
The following command sets all decompression options to their default values:
```
default decompression-options
```
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**

Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Use this command to return to the parent configuration mode.
The RoHC Profile Decompression Configuration Mode is used to configure RoHC (Robust Header Compression) Decompressor parameters.

Mode

Exec > Global Configuration > RoHC Profile Configuration >
configure > rohc-profile profile-name profile_name > decompression-options

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-rohcprofile-profile_name-decomp)#

Important: The availability of commands, keywords and variables in this mode are dependent on platform type, product version, and installed license(s).
accept-delayed-pkts

Accepts delayed packets

**Product**
- HSGW
- PDSN

**Privilege**
- Administrator

**Mode**
Exec > Global Configuration > RoHC Profile Configuration >
configure > rohc-profile profile-name profile_name > decompression-options

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-rohcprofile-profile_name-decomp)#
```

**Syntax**

```
[ default ] accept-delayed-pkts
```

- **default**
  
  Returns the command to its default value of disabled.

**Usage**

This command helps reduce packet loss during context repair.

**Example**

Use the following command to enable the system to accept delayed packets:

```
accept-delayed-pkts
```
context-timeout

Ensures that no expired contexts are used for data compression.

Product

HSGW
PDSN

Privilege

Administrator

Mode

Exec > Global Configuration > RoHC Profile Configuration >
configure > rohc-profile profile-name profile_name > decompression-options

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-rohcprofile-profile_name-decomp)#

Syntax

context-timeout seconds

default context-timeout

default
Returns the command to its default value.

seconds
Specifies the context timeout value (in seconds) as an integer from 0 through 100.
Default: 20

Usage

The RoHC stack should periodically clean up expired contexts and release memory in case there is no data activity for the call on this context. The context cleanup period is internally calculated to be set to half of the value of the context-timeout value. This will ensure that no expired contexts are used for data compression.

Example

The following command sets the context-timeout parameter to 30 seconds:

context-timeout 30
crc-errors-fo

Sets the limits for when a NACK message is sent while in the FO (First Order) state. A NACK is sent whenever CRC errors are detected within a specified number of packets.

Product
HSGW
PDSN

Privilege
Administrator

Mode
Exec > Global Configuration > RoHC Profile Configuration >
configure > rohc-profile profile-name profile_name > decompression-options

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-rohcprofile-profile_name-decomp)#

Syntax

crc-errors-fo-k num_errors

crc-errors-fo-n num_packts

default crc-errors-fo-k

default crc-errors-fo-n

default

Returns the command to its default value.

Important: num_errors must be less than or equal to the value specified with the crc-errors-fo-n command.


crc-errors-fo-n num_packts

Specifies the number of packets to check for CRC errors as an integer from 1 through 10. Default: 1

Usage

Use this command to set the parameters that trigger sending a NACK message when in the FO state.

Example

To configure a NACK to be sent when 4 out of the last 10 packets have CRC errors when in the FO state, use the following commands:
crc-errors-fo-k 4

crc-errors-fo-n 10
**crc-errors-so**

Sets the limits for when a NACK message is sent while in the SO (Second Order) state. A NACK is sent whenever CRC errors are detected within a specified number of packets.

**Product**

HSGW
PDSN

**Privilege**

Administrator

**Mode**

Exec > Global Configuration > RoHC Profile Configuration >

`configure > rohc-profile profile-name profile_name > decompression-options`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-rohcprofile-profile_name-decomp)#
```

**Syntax**

```
crc-errors-so-k num_errors

crc-errors-so-n num_packets

default crc-errors-so-k

default crc-errors-so-n
```

**Example**

Use this command to set the parameters that trigger sending a NACK message when in the SO state.

To configure a NACK to be sent when 4 out of the last 10 packets have CRC errors when in the SO state, use the following commands:
crc-errors-so-k 4

crc-errors-so-n 10
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Use this command to return to the parent configuration mode.
nack-limit

Sets the number of unsuccessful decompressions allowed before a NACK is sent.

**Product**
- HSGW
- PDSN

**Privilege**
- Administrator

**Mode**
Exec > Global Configuration > RoHC Profile Configuration >
```bash
command_profile > rohc-profile profile-name profile_name > decompression-options
```
Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-rohcprofile-profile_name-decomp)#
```

**Syntax**
```
nack-limit limit

default nack-limit
```

- **default**
  Returns the command to its default value.

- **limit**
  Specifies the number of unsuccessful decompressions allowed as an integer from 0 through 20. Default: 0

**Usage**
Use this command to set the maximum number of unsuccessful decompressions before a NACK message is sent.

**Example**
The following command sets the number of unsuccessful decompressions allowed to 10:
```
nack-limit 10
```
**optimistic-mode-ack**

When this command is enabled and a type 2 IR-DYN packet is successfully decompressed, an optional ACK is sent in U-mode.

**Product**
HSGW

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > RoHC Profile Configuration >
`configure > rohc-profile profile-name profile_name > decompression-options`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-rohcprefile-profile_name-decomp)#
```

**Syntax**

```
[ default | no ] optimistic-mode-ack
```

- **default**
  - Returns the command to its default value of enabled.

- **no**
  - Disables the sending of the optional ACK.

**Usage**

Use this command to enable and disable the sending of an optional ACK in U-mode when a type 2 IR-DYN packet is successfully decompressed.

**Example**

To enable the sending of the optional ACK, enter the following command:

```
optimistic-mode-ack
```

To disable the sending of the optional ACK, enter the following command:

```
no optimistic-mode-ack
```
optimistic-mode-ack-limit

Sets the number of packets for which to send ACKs.

Product
HSGW
PDSN

Privilege
Administrator

Mode
Exec > Global Configuration > RoHC Profile Configuration >
configure > rohc-profile profile-name profile_name > decompression-options

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-rohcpprofile-profile_name-decomp)#

Syntax

optimistic-mode-ack-limit num_pkts

default optimistic-mode-ack-limit

default
Returns the command to its default value.

num_pkts
Specifies the number of packets for which to send ACKs as an integer from 0 through 20.
Default: 3

Usage
Use this command to set the number of packets to send the optional ACK for when a type 2 IR-DYN packet is successfully decompressed.

Example
Enter the following command to set the number of packets to send and ACK for to 6:

optimistic-mode-ack-limit 6

Use the following command to set the number of packets to send an ACK for back to the default of 3:

default optimistic-mode-ack-limit
piggyback-wait-time

Specifies the time in milliseconds to wait for a feedback packet to be picked up as piggybacked feedback by the associated compressor.

Product
HSGW
PDSN

Privilege
Administrator

Mode
Exec > Global Configuration > RoHC Profile Configuration >
configure > rohc-profile profile-name profile_name > decompression-options

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-rohcprofile-profile_name-decomp)#

Syntax

piggyback-wait-time m_secs

default piggyback-wait-time

default

Returns the command to its default value.

m_secs

Specifies the time (in milliseconds) to wait for a feedback packet to be picked up as an integer value from 0 through 1000.
Default: 80

Usage

Use this command to set the time in milliseconds to wait for a feedback packet to be picked up as piggybacked feedback by the associated compressor.

Example

The following command sets the wait time to 120 ms:

piggyback-wait-time 120
preferred-feedback-mode

Specifies the preferred feedback mode to use between the compressor and the decompressor

Product
- HSGW
- PDSN

Privilege
Administrator

Mode
Exec > Global Configuration > RoHC Profile Configuration >
configure > rohc-profile profile-name profile_name > decompression-options

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-rohcprofile-profile_name-decomp)#

Syntax

preferred-feedback-mode { bidirectional-optimistic | bidirectional-reliable | unidirectional }

default preferred-feedback-mode

Returns the command to its default setting of bidirectional-optimistic.

bidirectional-optimistic

This mode is similar to the Unidirectional mode, with the exception of a feedback channel used to send error recovery requests from the decompressor to compressor. This is the default mode.

bidirectional-reliable

Reliable mode makes extensive use of a feedback channel to avoid packet loss from context invalidation. A secure reference model is used instead of the optimistic approach used in the other modes. With the secure reference model, the confidence of the compressor depends on acknowledgements from the decompressor for every context updating packet. Periodically the compressor sends context updating packets repeatedly until an acknowledgement is received from the decompressor.

unidirectional

Packets are sent in only one direction, from the compressor to the decompressor.

Usage

Use this command to specify the preferred feedback method to use between the compressor and the decompressor for the current RoHC profile.

Example

Use this command to specify the preferred feedback method to use between the compressor and the decompressor for the current RoHC profile.
Use the following command to set the preferred feedback mode to bidirectional-reliable:

```bash
preferred-feedback-mode bidirectional-reliable
```
rtp-sn-p

Specifies the value of p in RTP SN (RTP Sequence Number) calculation. Least Significant Bits (LSB) encoding is used for header fields whose values are usually subject to small changes. With LSB encoding, the k least significant bits of the field value are transmitted instead of the original field value, where k is a positive integer. After receiving k bits, the decompressor derives the original value using a previously received value as reference (v_ref). The scheme is guaranteed to be correct if the compressor and the decompressor each use interpretation intervals as follows:

- In which the original value resides
- And in which the original value is the only value that has the exact same k least significant bits as those transmitted.

The interpretation interval can be described as a function:

\[ f(v_{\text{ref}}, k) = [v_{\text{ref}} - p, v_{\text{ref}} + (2^k - 1) - p] \]

Where p is an integer.

Syntax

rtp-sn-p value

default rtp-sn-p

default

Returns the command to its default value.

value

Specifies the number the value of p in the RTP SN calculation as an integer from 0 through 999.

Usage

Use this command to set the value to use for p when performing the RTP SN calculation.

Example

The following command sets the RTP Sequence Number integer “p” value to 100:

rtp-sn-p 100
rtp-sn-p-override

Allows an override of p in RTP SN calculation. This is disabled by default.

Product

HSGW
PDSN

Privilege

Administrator

Mode

Exec > Global Configuration > RoHC Profile Configuration >
configure > rohc-profile profile-name profile_name > decompression-options

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-rohcprofile-profile_name-decomp)#

Syntax

[ default | no ] rtp-sn-p-override

---

default

Returns the command to its default value of disabled.

---

no

Disables overriding p in RTP SN calculation.

Usage

Use this command to allow an override of p in RTP SN calculations.

Example

The following command enables the override of p in the RTP SN calculation:

rtp-sn-p-override
sliding-window-ts

Computes jitter as described in RFC 3095.[4.5.4]

Product
HSGW
PDSN

Privilege
Administrator

Mode
Exec > Global Configuration > RoHC Profile Configuration >
configure > rohc-profile profile-name profile_name > decompression-options
Entering the above command sequence results in the following prompt:

[context_name]host_name(config-rohcprofile-profile_name-decomp)#

Syntax

sliding-window-ts size

default sliding-window-ts

default
Returns the command to its default value of 4.

size
Sets the size of the sliding window. size must be an integer from 1 through 1000.
Default: 4

Usage
Use this command to set the size of the sliding window used to compute jitter for the current RoHC profile.

Example
The following command sets the sliding window size to 500:

sliding-window-ts 500
use-clock-option

Controls usage of the RoHC clock option. The clock option informs the compressor of the clock resolution of the decompressor. This allows the compressor to estimate the jitter introduced by the clock of the decompressor when doing timer-based compression of the RTP timestamp.

Product
HSGW
PDSN

Privilege
Administrator

Mode
Exec > Global Configuration > RoHC Profile Configuration >
configure > rohc-profile profile-name profile_name > decompression-options

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-rohcprofile-profile_name-decomp)#

Syntax

[ default | no ] use-clock-option

  default
  Returns the command to its default value of enabled.

  no
  Disables use of the RoHC clock option.

Usage
Use this command to enable and disable the use of the RoHC clock option.

Example

The following command enables RoHC clock option usage:

  use-clock-option

The following command disables RoHC clock option usage:

  no use-clock-option
**use-crc-option**

Controls usage of the RoHC cyclic redundancy check (CRC) option. The CRC option contains an 8-bit CRC computed over the entire feedback payload, without the packet type and code octet, but including any CID fields.

**Product**
- HSGW
- PDSN

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > RoHC Profile Configuration >
configure > rohc-profile profile-name profile_name > decompression-options

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-rohcprofile-profile_name-decomp)#
```

**Syntax**

```
[ default | no ] use-crc-option
```

- **default**
  Returns the command to its default value of enabled.

- **no**
  Disables use of the CRC option.

**Usage**

Use this command to enable and disable the use of the RoHC CRC option.

**Example**

The following command enables RoHC CRC option usage:

```
use-crc-option
```

The following command disables RoHC CRC option usage:

```
no use-crc-option
```
**use-feedback**

Controls use of the feedback channel. A feedback channel sends error recovery requests and (optionally) acknowledgments of significant context updates from the decompressor to the compressor.

**Product**
- HSGW
- PDSN

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration > RoHC Profile Configuration >
  - `configure > rohc-profile profile-name profile_name > decompression-options`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-rohcreprofile-profile_name-decomp)#
```

**Syntax**

```
[ default | no ] use-feedback
```

- `default`
  - Returns the command to its default value of disabled.

- `no`
  - Disables use of the feedback channel.

**Usage**

Use this command to enable and disable the use of the RoHC feedback channel.

**Example**

The following command enables RoHC feedback channel usage:

```
use-feedback
```

The following command disables RoHC feedback channel usage:

```
no use-feedback
```
**use-jitter-option**

Controls usage of RoHC jitter option. The jitter option allows the decompressor to report the maximum jitter it has observed.

**Product**
- HSGW
- PDSN

**Privilege**
- Administrator

**Mode**
Exec > Global Configuration > RoHC Profile Configuration >
- configure > rohc-profile profile-name profile_name > decompression-options

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-rohcprofile-profile_name-decomp)#
```

**Syntax**

```
[ default | no ] use-jitter-option
```

- **default**
  Returns the command to its default value of enabled.

- **no**
  Disables use of the jitter option.

**Usage**

Use this command to enable and disable the use of the RoHC jitter option.

**Example**

The following command enables RoHC jitter option usage:

```
use-jitter-option
```

The following command disables RoHC jitter option usage:

```
no use-jitter-option
```
use-reject-option

Controls usage of RoHC reject option. The reject option informs the compressor that the decompressor does not have sufficient resources to handle the flow.

Product
HSGW
PDSN

Privilege
Administrator

Mode
Exec > Global Configuration > RoHC Profile Configuration >

configure > rohc-profile profile-name profile_name > decompression-options

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-rohcprofile-profile_name-decomp)#

Syntax

[ default | no ] use-reject-option

default
Returns the command to its default value of disabled.

no
Disables use of the reject option.

Usage
Use this command to enable and disable the use of the RoHC reject option.

Example
The following command enables RoHC reject option usage:

use-reject-option

The following command disables RoHC reject option usage:

no use-reject-option
use-sn-not-valid-option

Controls usage of the RoHC SN not valid option. The sn-not-valid option indicates that the SN of the feedback is not valid. A compressor must not use the SN of the feedback to find the corresponding sent header when this option is present.

**Product**
HSGW
PDSN

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > RoHC Profile Configuration >

```bash
configure > rohc-profile profile-name profile_name > decompression-options
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-rohcprofile-profile_name-decomp)#
```

**Syntax**

```
[ default | no ] use-sn-not-valid-option
```

- **default**
  Returns the command to its default value of enabled.

- **no**
  Disables use of the sn-not-valid option.

**Usage**

Use this command to enable and disable the use of the RoHC sn not valid option.

**Example**

The following command enables RoHC sn not valid option usage:

```
use-sn-not-valid-option
```

The following command disables RoHC sn not valid option usage:

```
no use-sn-not-valid-option
```
use-sn-option

Controls usage of RoHC sn option. The sn option provides eight additional bits of SN (Sequence Number, usually the RTP Sequence Number.)

Product
HSGW
PDSN

Privilege
Administrator

Mode
Exec > Global Configuration > RoHC Profile Configuration >
configure > rohc-profile profile-name profile_name > decompression-options

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-rohçprofile-profile_name-decomp)#

Syntax

[ default | no ] use-sn-option

default
Returns the command to its default value of enabled.

no
Disables use of the SN option.

Usage
Use this command to enable and disable the use of the RoHC SN option.

Example
The following command enables RoHC SN option usage:

    use-sn-option

The following command disables RoHC SN option usage:

    no use-sn-option
Chapter 269
Route-map Configuration Mode Commands

The Route-Map Configuration sub-mode is used for the OSPFv2 and BGP-4 routing protocols. This mode includes commands that configure matching rules and set actions to perform on matched routes.

Mode

Exec > Global Configuration > Context Configuration > Route-map Configuration

configure > context context_name > route-map map_name { deny | permit } seq_number

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-route-map)#

⚠️ **Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

`exit`

**Usage**
Use this command to return to the parent configuration mode.
match as-path

Matches an Autonomous System (AS) path access list

Product
HA

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Route-map Configuration

```
configure > context context_name > route-map map_name { deny | permit } seq_number
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-route-map)#
```

Syntax

```
[ no ] match as-path AS_list
```

- `no`
  Disables matching the specified AS path access list.

- `AS_list`
  Specifies the name of an AS path access list for matching as an alphanumeric string of 1 through 79 characters.

Usage

This command is used for BGP-4 routing to specify an AS path access list to be matched. Refer to the `ip as-path access-list` command for more information.

Example

To match entries in an AS path access list named `ASlist1`, enter the following command;

```
match as-path ASlist1
```
match interface

Specifies the next-hop interface name of a route to be matched.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Route-map Configuration
configure > context context_name > route-map map_name ( deny | permit ) seq_number

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-route-map)#

Syntax

[ no ] match interface interface-name

no
Disables matching the specified interface name.

interface-name
Specifies the name of the virtual interface for matching as an alphanumeric string of 1 through 79 characters.

Usage
Use this command to specify the next hop interface name for routes to be matched.

Example
To match routes that have the next hop interface specified as Interface123, enter the following command:

    match interface Interface123

To disable matching routes that have the next hop interface specified as Interface123, enter the following command:

    no match interface Interface123
match ip address

Matches IPv4 routes with entries in a route-access-list or prefix-list.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Route-map Configuration

```
configure > context context_name > route-map map_name { deny | permit } seq_number
```

Entering the above command sequence results in the following prompt:

```
[context_name] host_name(config-route-map)#
```

**Syntax**

```
[ no ] match ip address { prefix-list | route-access-list } list_name
```

- **no**
  Disables matching from the specified prefix list or route access list.

- **prefix-list**
  Matches any routes with entries in a prefix-list.

- **route-access-list**
  Matches any routes with entries in a route-access-list.

- **list_name**
  Specifies the name of the IPv4 prefix list or IPv4 route access-list as an alphanumeric string of 1 through 79 characters.

**Usage**

Use this command to match routes specified in an IPv4 route-access-list or prefix-list.

**Example**

To match routes that are specified in an IPv4 prefix list named Prefix100, enter the following command:

```
match ip address prefix-list Prefix100
```

To disable matching routes that are specified in an IPv4 prefix list named Prefix100, enter the following command:

```
no match ip address prefix-list Prefix100
```
**match ip next-hop**

Matches next-hop IPv4 addresses with entries in a specified prefix-list or route-access-list.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Route-map Configuration

`configure > context context_name > route-map map_name { deny | permit } seq_number`

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-route-map)#`

**Syntax**

```
[ no ] match ip next-hop { prefix-list | route-access-list }list_name
```

- **prefix-list**
  Matches any routes that have a next-hop router IPv4 address that has an entry in the specified prefix list.

- **route-access-list**
  Matches any routes that have a next-hop router IPv4 address that has an entry in the specified route-access-list.

- **list_name**
  Specifies the name of the prefix-list or route-access-list as an alphanumeric string of 1 through 79 characters.

**Usage**

Use this command to match next-hop IPv4 addresses that have entries in the specified prefix-list or route-access-list.

**Example**

To match next-hop IPv4 addresses with entries in a prefix-list named *Prefix100*, enter the following command:

```
matic ip next-hop prefix-list Prefix100
```

To disable matching next-hop IPv4 addresses with entries in a prefix-list named *Prefix100*, enter the following command:

```
no match ip next-hop prefix-list Prefix100
```
**match ipv6 address**

Matches IPv6 routes with entries in a specified route-access-list or prefix-list.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Route-map Configuration

configure > context context_name > route-map map_name { deny | permit } seq_number

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-route-map)#

**Syntax**

```
[ no ] match ipv6 address { prefix-list | route-access-list } list_name
```

- **no**
  Disables matching from the specified prefix list or route access list.

- **prefix-list**
  Matches any routes with entries in a prefix-list.

- **route-access-list**
  Matches any routes with entries in a route-access-list.

- **list_name**
  Specifies the name of the IPv6 prefix list or IPv6 route access-list as an alphanumeric string of 1 through 79 characters.

**Usage**

Matches IPv6 routes with entries in a specified route-access-list or prefix-list.

**Example**

To match routes that are specified in an IPv6 prefix list named *Prefix600*, enter the following command:

```
match ipv6 address prefix-list Prefix600
```

To disable matching routes that are specified in an IPv6 prefix list named *Prefix600*, enter the following command:

```
no match ipv6 address prefix-list Prefix100
```
match ipv6 next-hop

Matches next-hop IPv6 addresses with entries in specified standard prefix-list or route-access-list.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Route-map Configuration
configure > context context_name > route-map map_name { deny | permit } seq_number

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-route-map)#

Syntax

[ no ] match ipv6 next-hop { prefix-list | route-access-list }list_name

---

prefix-list
Matches any routes that have a next-hop router IPv6 address that has an entry in the specified prefix list.

route-access-list
Matches any routes that have a next-hop router IPv6 address that has an entry in the specified route-access-list.

list_name
Specifies the name of the prefix-list or route-access-list as an alphanumeric string of 1 through 79 characters.

Usage
Use this command to match next-hop IPv6 addresses that have entries in the specified prefix-list or route-access-list.

Example
To match next-hop IPv6 addresses with entries in a prefix-list named Prefix600, enter the following command:

    match ipv6 next-hop prefix-list Prefix600

To disable matching next-hop IPv6 addresses with entries in a prefix-list named Prefix600, enter the following command:

    no match ipv6 next-hop prefix-list Prefix600
match metric

Matches routes that have the specified route metric.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Route-map Configuration

configure > context context_name > route-map map_name { deny | permit } seq_number

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-route-map)#

Syntax

[ no ] match metric metric_value

no
Disables matching of the specified route metric.

metric_value
Specifies the route metric to match as an integer from 0 through 4294967295.

Usage
Use this command to match routes that have the specified route metric.

Example
To match routes with the route metric of 1200, enter the following command:

match metric 1200

To disable matching routes with a route metric of 1200, enter the following command:

no match metric 1200
match origin

Matches the origin code learned from BGP. This command is for route maps that are used with BGP routing only.

**Product**
HA

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Route-map Configuration

configure > context context_name > route-map map_name { deny | permit } seq_number

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-route-map)#

**Syntax**

[ no ] match origin { egp | igp | incomplete }

- **no**
  Disables matching of the origin code.

- **egp**
  Matches origins learned via the External Gateway Protocol (EGP)

- **igp**
  Match origins learned via the local Interior Glittery Protocol (IGP)

- **incomplete**
  Match origins with unknown heritage.

**Usage**

Use this command to match origin codes for BGP routing.

**Example**

To match origin codes learned from EGP, enter the following command:

```
match origin egp
```
**match route-type external**

Match external Open Shortest Path First (OSPF) routes of the specified type.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Route-map Configuration

```
configure > context context_name > route-map map_name { deny | permit } seq_number
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-route-map)#
```

**Syntax**

```
[ no ] match route-type external { type-1 | type-2 }
```

- **type-1**
  Only matches type-1 external routes.

- **type-2**
  Only matches type-2 external routes.

**Usage**

Use this command to match external routes of a specific type.

**Example**

The following command matches all external routes that are type-2:

```
match route-type external type-2
```

The following command disables matching external routes that are type-2:

```
no match route-type external type-2
```
match tag

Matches routes with the specified route tag value.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Route-map Configuration
configure > context context_name > route-map map_name { deny | permit } seq_number

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-route-map)#

Syntax

[ no ] match tag tag_value

no
Disables matching routes with the specified route tag value.

tag_value
Specifies the route tag value to match as an integer from 0 through 4294967295.

Usage
Use this command to match routes that have the specified route tag value.

Example
Use the following command match routes that have a route tag value of 1234:

    match tag 1234

Use the following command to disable matching routes that have a route tag value of 1234:

    no match tag 1234
set as-path

Modifies an Autonomous System (AS) path for a route by adding the specified AS numbers to the front of the path.

**Product**
HA

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Route-map Configuration

```
configure > context context_name > route-map map_name { deny | permit } seq_number
```

Entering the above command sequence results in the following prompt:

```
[context_name] host_name(config-route-map) #
```

**Syntax**

```
[ no ] set as-path prepend ASN
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Disables prepending the AS path. Any previously set prepends are removed.</td>
</tr>
<tr>
<td>prepend</td>
<td>Prepends the AS path.</td>
</tr>
<tr>
<td>ASN</td>
<td>AS number(s) to be prepended to the AS path. You can specify up to 16 different AS numbers to be prepended in the order specified. Each AS number must be separated by a space. ASN must be an integer from 1 through 65535.</td>
</tr>
</tbody>
</table>

**Usage**

Use this command to add up to 16 specified AS numbers to the front of the AS path.

**Example**

The following command prepends the AS numbers 100, 200, and 1000 to matching AS paths:

```
set as-path prepend 100 200 1000
```
set ip next-hop

Sets the IPv4 address that is applied as the next hop for routes.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Route-map Configuration

configure > context context_name > route-map map_name { deny | permit } seq_number

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-route-map)#

Syntax

[ no ] set ip next-hop ipv4_address

- **no**
  - Disables the specified next hop IPv4 address.

- **ipv4_address**
  - Specifies the IPv4 address of the next hop to which packets are output, entered using IPv4 dotted-decimal notation.

Usage

Use this command to set the IPv4 address that is used as the next hop for routes.

Example

To set the next hop for routes to the IPv4 address 192.168.2.100, use the following command:

```
set ip next-hop 192.168.2.100
```

To disable setting the next hop for routes to the IP address 192.168.2.100, use the following command:

```
o set ip next-hop 192.168.2.100
```
set ipv6 next-hop

Sets the IPv6 address that is applied as the next hop for routes.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Route-map Configuration
```
configure > context context_name > route-map map_name { deny | permit } seq_number
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-route-map)#
```

**Syntax**
```
[ no ] set ipv6 next-hop ipv6_address
```

- **no**
  
  Disables the specified next hop address.

- **ipv6_address**
  
  Specifies the IPv6 address of the next hop to which packets are output, entered using IPv6 colon-separated-hexadecimal notation.

**Usage**

Use this command to set the IPv6 address that is used as the next hop for routes.

**Example**

To set the next hop for routes to the IPv6 address `2001:4A2B::1f3F`, use the following command:
```
set ip next-hop 2001:4A2B::1f3F
```

To disable setting the next hop for routes to the IP address `2001:4A2B::1f3F`, use the following command:
```
no set ip next-hop 2001:4A2B::1f3F
```
**set metric**

Sets the route metric for matching routes to a specified value.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Route-map Configuration

```bash
configure > context context_name > route-map map_name { deny | permit } seq_number
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-route-map)#
```

**Syntax**

```
[ no ] set metric metric_value
```

**Usage**

Specifies the metric value that is set for routes as an integer from 1 through 16777214.

**Example**

Use this command to set the route metric for matched routes.

To set the route metric to **12345**, use the following command:

```bash
set metric 12345
```

To disable setting the route metric to **12345**, enter the following command:

```bash
no set metric 12345
```
set metric-type

This command sets the route metric type to either Type-1 or Type-2 in the AS-external-LSA.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Route-map Configuration

configure > context context_name > route-map map_name { deny | permit } seq_number

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-route-map)#

Syntax

[ no ] set metric-type { type-1 | type-2 }

type-1
Sets the route metric to external type-1.

type-2
Sets the route metric to external type-2

Usage

Use this command to set the route metric to either external type-1 or external type-2.

Example

To set the route metric to type-1, enter the following command:

set metric type-1

To disable setting the metric to type, enter the following command:

no set metric type-1
set origin

Sets the Border Gateway Protocol (BGP) origin code to a specified value. This command is for route maps that are used with BGP routing only.

Product
HA

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Route-map Configuration

configure > context context_name > route-map map_name { deny | permit } seq_number

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-route-map)#

Syntax

[ no ] set origin { egp | igp | incomplete }

no
Disables setting the origin code.

ejp
Sets the origin code to specify that the path is from a remote External Gateway Protocol (EGP) system.

igp
Sets the origin code to specify that the path is from a local Interior Gateway Protocol (IGP) system.

incomplete
Sets the origin code to specify that the path is from an unknown system.

Usage
Use this command to set a specified origin code for BGP.

Example
To set the origin code to be from an External Gateway Protocol (EGP) system, enter the following command:

set origin egp
set tag

Sets the route tag value for matched routes.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Route-map Configuration

configure > context context_name > route-map map_name { deny | permit } seq_number

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-route-map)#

Syntax

[ no ] set tag tag_value

---

no

Disable setting the route tag to the specified value.

tag_value

Specifies the route tag value as an integer from 0 through 4294967295.

Usage

Use this command to set the route tag value that is applied to all matched routes.

Example

To set the route tag value to 12345, enter the following command:

    set tag 12345

To disable setting the route tag value to 12345, enter the following command:

    no set tag 12345
**set weight**

Sets the weight in the routing table for matching routes to the specified value.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Route-map Configuration

```text
configure > context context_name > route-map map_name { deny | permit } seq_number
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-route-map)#
```

**Syntax**

```
[ no ] set weight value
```

- **no**
  Disable setting the routing weight value.

- **value**
  Specifies the weight in the routing table as an integer from 1 through 4294967295.

**Usage**

Use this command to set the routing table weight on matched routes.

**Example**

The following command sets the routing table weight for matched routes to 1000:

```
set weight 1000
```
The RS-232 Port Configuration Mode is used to manage the RS-232 ports on the SPIO cards.

**Mode**

Exec > Global Configuration > RS-232 Port Configuration

`configure > port rs232 slot_number/port_number`

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-port-slot_number/port_number)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
default

Restores the port’s default speed and communication mode.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > RS-232 Port Configuration

configure > port rs232 slot_number/port_number

Entering the above command sequence results in the following prompt:

[local]host_name(config-port-slot_number/port_number)#

Syntax

default { preferred slot | terminal { all | databits | flowcontrol | parity | speed | stopbits } }

preferred slot

Sets the port for non-revertive operation for port redundancy auto-recovery; requiring an administrative user to manually issue a port switch to command to return service to the original port.

terminal { all | databits | flowcontrol | parity | speed | stopbits } 

Sets the terminal settings for the RS-232 port to their default settings.
all: Restores all settings to their default values.
databits: Restores the databits setting to its default value of 8.
flowcontrol: Restores the flowcontrol setting to its default value of none.
parity: Restores the parity setting to its default value of none.
speed: Restores the speed setting to its default value of 9600.
stopbits: Restores the stopbits setting to its default value of 1.

Usage

Restores port-level parameters to their default values.

Example

The following command restores all terminal settings to their default values:

    default terminal all
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

exit

Usage
Use this command to return to the parent configuration mode.
preferred slot

Assigns revertive or non-revertive control to port redundancy auto-recovery.
Default: non-revertive operation

Product
PDSN
FA
HA
GGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > RS-232 Port Configuration
configure > port rs232 slot_number/port_number

Entering the above command sequence results in the following prompt:

[local]host_name(config-port-slot_number/port_number)#

Syntax

preferred slot slot#
no preferred slot slot#

Usage
This command enables or disables revertive port redundancy, wherein after a port failover, when the original port is restored to service (such as link up) the system will return service to that port automatically. Disabled, which is the default setting, causes non-revertive operation; requiring an administrative user to manually issue a port switch to command to return service to the original port.

This command must be issued on a per port basis, allowing you to configure specific ports to be used on individual line cards or SPIO cards. For example, ports 1 through 4 could be configured as “preferred” on the line card in slot 17, while ports 5 through 8 are “preferred” on the line card in slot 33. In this scenario, both line cards would be in an Active operational state while still providing LC and port redundancy for the other.

Important: This command is not supported on all platforms.

Example
preferred slot 24
snmp trap link-status

Enables or disables the generation of an SNMP trap for link status changes.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > RS-232 Port Configuration
configure > port rs232 slot_number/port_number

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-port-slot_number/port_number)#
```

**Syntax**

```
snmp trap link-status

no snmp trap link-status
``` 

Disables the sending of traps for link status changes.

**Usage**

Enable link status change traps when a monitoring facility can use the information or if there are troubleshooting activities are in progress.

**Example**

```
  snmp trap link-status

  no snmp trap link-status
```
terminal

Configures the console port on the SPIO.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > RS-232 Port Configuration

configure > port rs232 slot_number/port_number

Entering the above command sequence results in the following prompt:

[local]host_name(config-port-slot_number/port_number)#

Syntax

terminal { carrierdetect { off | on } | databits { 7 | 8 } | flowcontrol { hardware | none } | parity { even | none | odd } | speed { 115200 | 19200 | 38400 | 57600 | 9600 } | stopbits { 1 | 2 } }

carrierdetect { off | on }  
Default:  
Specifies whether or not the console port is to use carrier detect when connecting to a terminal.

databits { 7 | 8 }  
Default: 8  
Specifies the number of data bits used to transmit and receive characters.

flowcontrol { hardware | none }  
Default: none  
Specifies how the flow of data is controlled between the SPIO and a terminal.

parity { even | none | odd }  
Default: none  
Specifies the type of error checking used on the port.  
 even: Enables error checking by setting the parity bit to 1 (if needed) making the number of 1s in the data bits even.  
 none: Disables error checking.  
 odd: Enables error checking by setting the parity bit to 1 (if needed) making the number of 1s in the data bits odd.

speed { 115200 | 19200 | 38400 | 57600 | 9600 }  
Default: 9600  
Specifies the flow of data in bits per second between the console port and terminal.
stopbits { 1 | 2 }
Default: 1
Specifies the number of stop bits between each transmitted character.

Usage
Sets the SPIO console port parameters for communication with the terminal device.

Example
The following command sets the SPIO’s console port. The terminal must support these values.

    terminal carrierdetect off databits 7 flowcontrol hardware parity even
    speed 115200 stopbits 1
Chapter 271
S1AP Cause Code Configuration Mode Commands

The cause code group object allows an operator to group together a set of cause codes. This group can then be used as a named object in other commands.

Mode
Exec > Global Configuration > LTE Policy Configuration > S1AP Cause Code Configuration
configure > lte-policy > cause-code-group group_name

Entering the above command sequence results in the following prompt:

[local] host_name (slap-cause-code)

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
class

Configures a set of cause codes within a cause code group.

Product

MME

Privilege

Administrator

Mode

Exec > Global Configuration > LTE Policy Configuration > S1AP Cause Code Configuration

configure > lte-policy > cause-code-group group_name

Entering the above command sequence results in the following prompt:

[local] host_name (s1ap-cause-code)

Syntax

[no] class { miscellaneous | nas | protocol | radio | transport } cause cause_no

- **no**
  - Removes the specified cause code class.

- **miscellaneous**
  - Specifies the class of miscellaneous cause codes.

- **nas**
  - Specifies the class of NAS cause codes.

- **protocol**
  - Specifies the class of protocol cause codes.

- **radio**
  - Specifies the class of radio cause codes.

- **transport**
  - Specifies the class of transport cause codes.

- **cause cause_no**
  - Specifies the cause codes to add to this class. Cause codes must be defined one at a time.
  - *cause_no* is a numeric cause code value, as defined in 3GPP TS 36.413.

Usage

Use this command to configure the specific cause codes within this S1AP Cause Code Group. A maximum of 16 cause codes can be added to a cause-code-group entry.
Refer to the `policy service-request` command and `policy tau` command in the MME Service Configuration Commands Chapter to configure the behavior of the MME when the initial context setup fails during a service request procedure or while processing a TAU request.

The specific action taken by the MME can be mapped to the cause codes defined in this command.

**Example**

The following commands add causes `failure-in-radio-interface-procedure` and `interaction-with-other-procedure` to the cause code group.

```
class radio cause 26
class radio cause 29
```
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

exit

Usage
Use this command to return to the parent configuration mode.
Chapter 272
S1-U Relay Configuration Mode Commands

The S1-U Relay configuration option enables the S1-U Relay service functionality to the HeNB-GW Access Service. In this mode user can configure associations to the Access and Network GTP-U services for S1-U Relay

Mode
Exec > Global Configuration > Context Configuration > HeNB-GW Access Service Configuration > S1-U Relay Configuration

configure > context context_name > henbgw-access-service access_svc_name > slu-relay

Entering the above command sequence results in the following prompt:

[context_name]host_name(slu-relay) #

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
**associate**

Associates previously configured Access GTP-U service as well as the Network GTP-U service to this HeNB-GW Access Service for S1-U relay service functionality. The Access and Network GTP-U services must be configured in the Context Configuration mode before using this configuration.

**Product**
HeNB-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > HeNB-GW Access Service Configuration > S1-U Relay Configuration

*configure > context context_name > henbgw-access-service access_svc_name > slu-relay*

Entering the above command sequence results in the following prompt:

*[context_name]host_name(slu-relay)#*

**Syntax**

```
associate { access-gtpu-service access_gtpu_svc | network-gtpu-service network_gtpu_svc } [ context ctxt_name ]
```

```
no associate { access-gtpu-service | network-gtpu-service }
```

- **no**
  Removes the associated Access or Network GTP-U service from this HeNB-GW Access service configuration.

  ```
  access_gtpu_svc
  ```

  Identifies the name of the pre-configured Access GTP-U service in Context Configuration Mode to associate with this HeNB-GW Access Service for S1-U relay.

  *access_gtpu_svc* is an alphanumeric string of 1 through 63 characters.

  ```
  network_gtpu_svc
  ```

  Identifies the name of the pre-configured Network GTP-U service to associate with this HeNB-GW Access Service for S1-U relay.

  *network_gtpu_svc* is an alphanumeric string of 1 through 63 characters.

**Usage**

Use this command to bind/associate a pre-configured Access or Network GTP-U service to this HeNB-GW Access service. When S1-U Relay is enabled, the association to ingress and egress GTP-U services is considered as critical configuration for the HeNB-GW Access service. When S1-U relay is enabled, both access and network gtpu services needs to be in STARTED state for the HENBGW access service to be started.

**Example**

```
```
Following command associates a Network GTP-U service named `net_gtpu` in egress context with a specific HeNB-GW Access service:

```
associate network-gtpu-service net_gtpu context egress
```
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
end
```

**Usage**
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Use this command to return to the parent configuration mode.
**ip**

Configures the Internet protocol (IP) parameters including downlink and uplink data IP QoS DSCP marking to this HeNB-GW Access Service for S1-U relay service functionality.

**Product**
HeNB-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > HeNB-GW Access Service Configuration > S1-U Relay Configuration

```
configure > context context_name > henbgw-access-service access_svc_name > slu-relay
```

Entering the above command sequence results in the following prompt:
```
[context_name]host_name(slu-relay)#
```

**Syntax**

```
ip { downlink | uplink } { qos-dscp { af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be | ef } }
```

```
no ip { downlink | uplink }
```

**no**

Removes the IP parameters for downlink/uplink data from this HeNB-GW Access service configuration.

```
qos-dscp { af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | af41 | af42 | af43 | be | ef }
```

Default: **af11**

Specifies the DSCP for the specified QoS traffic pattern. **qos-dscp** can be configured to any one of the following:

- **af11**: Assured Forwarding 11 per-hop-behavior (PHB)
- **af12**: Assured Forwarding 12 PHB
- **af13**: Assured Forwarding 13 PHB
- **af21**: Assured Forwarding 21 PHB
- **af22**: Assured Forwarding 22 PHB
- **af23**: Assured Forwarding 23 PHB
- **af31**: Assured Forwarding 31 PHB
- **af32**: Assured Forwarding 32 PHB
- **af33**: Assured Forwarding 33 PHB
- **af41**: Assured Forwarding 41 PHB
- **af42**: Assured Forwarding 42 PHB
- **af43**: Assured Forwarding 43 PHB
- **be**: Best effort forwarding PHB
- **ef**: Expedited forwarding PHB
Usage

Use this command to configure the S1-U relay uplink and downlink data traffic IP-QoS-DSCP value marking to this HeNB-GW Access service.

Example

Following command configures the DSCP-level for uplink data traffic through a specific HeNB-GW Access service to `af31`:

```
ip uplink qos-dscp af31
```
Chapter 273
SAEGW Service Configuration Mode Commands

The System Architecture Evolution Gateway (SAEGW) Service Configuration Mode is used to create and manage the relationship between specified services used for S-GW and P-GW network traffic.

Mode

Exec > Global Configuration > Context Configuration > SAEGW Service Configuration

configure > context context_name > saegw-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-saegw-service)#

⚠️ **Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
**associate**

Associates the SAEGW service with specific pre-configured services configured in the same context.

**Product**
SAEGW

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > SAEGW Service Configuration

`configure > context context_name > saegw-service service_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-saegw-service)#
```

**Syntax**

```
[ no ] associate { pgw-service name | sgw-service name }
```

- **no**
  Removes the selected association from this service.

- **pgw-service name**
  Specifies that the SAEGW service is to be associated with an existing P-GW service within this context.

  *name* must be an alphanumeric string of 1 through 63 characters and be an existing P-GW service.

- **sgw-service name**
  Specifies that the SAEGW service is to be associated with an existing S-GW service within this context.

  *name* must be an alphanumeric string of 1 through 63 characters and be an existing S-GW service.

**Important:** S-GW egress eGTP service must be in the same context as this SAEGW service. In addition, PMIP is not supported for the S-GW service egress.

**Usage**

Use this command to associate the SAEGW service with other pre-configured services configured in the same context.

**Important:** Each P-GW or S-GW service may only be associated with one SAEGW service; however, there may be multiple SAEGW services configured on a system in separate contexts.

**Example**

The following commands associate this SAEGW service with a P-GW service called *pgw1* and a S-GW service called *sgw2*:

```
associate pgw-service pgw1
```
associate sgw-service sgw2
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Use this command to return to the parent configuration mode.
Chapter 274
SaMOG Service Configuration Mode Commands

Creates SaMOG service and enters SaMOG service configuration mode.

Mode

Exec > Global Configuration > Context Configuration > SAMOG Service Configuration
configure > context context_name > samog-service samog_service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-samog-service)#

Important: Available commands or keywords/variables vary based on platform type, product version, and installed license(s).
associate

SaMOG associates another service to this SAMOG service.

Product
SaMOG

Mode
Exec > Global Configuration > Context Configuration > SAMOG Service Configuration

configure > context context_name > samog-service samog_service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-samog-service)#

Syntax

associate { cgw-service cgw_service_name | mrme-service mrme_service_name | subscriber-map subscriber_map_name }

no associate { cgw-service | dhcpv6-service | mrme-service | subscriber-map }

no

Disables the association of the service with the SaMOG service.

---

cgw-service cgw_service_name

The CGW service should be configured before associating the same with SaMOG service.
cgw_service_name must be an alphanumeric string between 1 and 63 characters.

---

mrme-service mrme_service_name

The MRME service should be configured before associating the same with SaMOG service.
mrme_service_name must be an alphanumeric string from 1 through 63 characters.

---

subscriber-map subscriber_map_name

The subscriber map service should be configured before associating the same with SaMOG service.
subscriber_map_name must be an alphanumeric string from 1 through 63 characters.

---

Usage

Use this command to associate the SaMOG service to CGW service, DHCPv4 service, MRME service, or Subscriber Mapping.

Example

The following command associates subscriber-map smap with SaMOG Service.

    associate subscriber-map smap

The following command associates cgw-service cgw with SaMOG Service.

    associate cgw-service cgw

The following command associates mrme-service mrme with SaMOG Service.
associate mrme-service mrme
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**
Use this command to return to the parent configuration mode.
max-sessions

Configures maximum number of subscribers SAMOG service can support, ranging from 0 to 4000000.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > SAMOG Service Configuration

configure > context context_name > samog-service samog_service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-samog-service)#

Syntax

max-sessions max_sessions

default max-sessions

max-sessions max_sessions

Configures maximum number of subscribers SAMOG service can support.

max_sessions is an integer value between 0 and 4000000.

default

Sets the default value, 4000000 for Max Sessions.

Usage

Use this command to configure the maximum number of subscribers SAMOG service can support.

Example

Use the following command to configure the maximum number of subscribers SAMOG service can support:

max-sessions 500
timeout

Configures the session's time-to-live (TTL) settings under SAMOG service.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > SAMOG Service Configuration
configure > context context_name > samog-service samog_service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-samog-service)#

Syntax

`timeout { absolute absolute | idle idle | setup-timeout setup_timeout }

defaulttimeout [ absolute absolute | idle idle | setup-timeout setup_timeout ]

notimeout [ absolute absolute | idle idle ]`

- **timeout { absolute absolute | idle idle | setup-timeout setup_timeout }**
  - **absolute absolute**: Designates the maximum duration of the session, in seconds, before system automatically terminates the session. `absolute` is number of seconds, an integer value between 0 and 2147483647.
  - **idle idle**: Designates the maximum duration a session can remain idle, in seconds, before system automatically terminates the session. Zero indicates function is disabled. Default is 0. `idle` is number of seconds, an integer value between 0 and 2147483647.
  - **setup-timeout setup_timeout**: It is the maximum time allowed for session setup in seconds. Default is 60 seconds. `setup_timeout` is number of seconds, an integer value between 0 and 1000000.

- **default**
  - Sets / Restores default value assigned for timeout. The default value of absolute and idle timeout is 0, which indicates the function is disabled. The default value of setup-timeout is 60.

- **no**
  - Enables / Disables the timeout option.

Usage

Use this command to configure the session's time-to-live (TTL) settings under SAMOG service.

Example

Use the following command to configure the setup-timeout to 500 seconds:

`timeout setup-timeout 500`
Use the following command to configure the absolute timeout to 120 seconds:

```
timeout absolute 120
```
Chapter 275
SCCP Network Configuration Mode Commands

The SCCP Network Configuration Mode is used to configure properties for Signaling Connection Control Part (SCCP) services for SS7.

Signaling Connection Control Part (SCCP) is a routing protocol in the SS7 protocol suite in layer 4, which provides end-to-end routing for TCAP messages to their proper database.

**Mode**

Exec > Global Configuration > SCCP Network Configuration

`configure > sccp-network id_number`

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-sccp-network-sccp_id)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
associate

Associates an SS7 routing domain with the SCCP network.

**Product**
SGSN
HNB-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > SCCP Network Configuration

```bash
configure > sccp-network id_number
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sccp-network-sccp_id)#
```

**Syntax**

```bash
associate ss7-routing-domain rd_id
```

```bash
no associate
```

no

Removes the association with the SS7 routing domain from the system configuration.

```bash
rd_id
```

This number identifies an already defined SS7 routing domain.

**Usage**

Use this command to associate SS7 routing domain configurations with SCCP network configurations.

**Example**

The following command associates the SCCP network with SS7 routing domain 2:

```bash
associate ss7-routing-domain 2
```
description

This command defines a string that describes the SCCP network. The description is used for operator reference.

Product
SGSN
HNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > SCCP Network Configuration
configure > sccp-network id_number

Entering the above command sequence results in the following prompt:

[local]host_name(config-sccp-network-sccp_id)#

Syntax

description string

no description

string

This is a string to describe the SCCP network.

string must be an alphanumeric string from 1 through 127 characters in length. If there are spaces in the string the string must be enclosed in double-quotes. For example; “This is a Description”.

no

Removes the description from the system configuration.

Usage

Use this command to configure a description of this SCCP service for operator reference.

Example

The following command sets the description to “This is the SCCP Service Number 1”:

    description "This is the SCCP Service Number 1."

**destination**

This command configures the SCCP network destination information. Use this command multiple times to set all of the destination information required.

**Product**

SGSN
HNB-GW

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > SCCP Network Configuration

```
configure > sccp-network id_number
```
Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sccp-network-sccp_id)#
```

**Syntax**

```
destination dpc pt_code { name route_name | next-hop pt_code [ priority priority ] | ssn subsys_num | version sccp_ver }

no destination dpc p_code [ name route_name | ssn subsys_num | version sccp_ver ]
```

**no**

Deletes the specified destination information from the SCCP network configuration.

**dpc pt_code**

Specifies the SCCP destination point code.

*pt_code*: Must be in SS7 point code dotted-decimal ###.###.### format or decimal ####### format.

**name route_name**

The name of the SCCP destination route.

*route_name*: enter an alphanumeric string from 1 through 64 characters in length.

**next-hop pt_code [ priority priority ]**

Associates the next destination defined in the SS7 routing domain and assigns the next-hop a priority for use.

*pt_code*: Must be in SS7 point code dotted-decimal ###.###.### format or decimal ####### format.

*priority*: Must be an integer from 0 to 15, with 0 setting the highest priority.

**ssn subsys_num**

The destination subsystem number.

*subsys_num*: enter an integer from 1 through 255.

**version sccp_ver**

*sccp_ver*: enter one of the following to select the SCCP variant:
- ANSI88
- ANSI92
- ANSI96
- BELL05
- CHINA
- GSM0806
- ITU88
- ITU92
- ITU96

Usage

Use this command to configure the destination information for the SCCP network.

Example

The following commands set the name of the destination route to default_route, the subsystem number to 1, and the variant version to ITU96, all with a destination point code of 1:

```plaintext
destination dpc 1 name default_route
destination dpc 1 ssn 1
destination dpc version ITU96
```
end

Exits the current configuration mode and returns to the Exec mode.

**Product**

SGSN
HNB-GW

**Privilege**

Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**

Return to the Exec mode.
exit

Exits the current configuration mode and returns to the global configuration mode.

Product
SGSN
HNB-GW

Privilege
Security Administrator, Administrator

Syntax

exit

Usage
Return to the global configuration mode.
global-title-translation

This command associates a GTT address-map with this SCCP network.

Product
SGSN
HNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > SCCP Network Configuration
configure > sccp-network id_number

Entering the above command sequence results in the following prompt:

[local]host_name(config-sccp-network-sccp_id)#

Syntax

global-title-translation address-map instance instance

no global-title-translation address-map instance instance

no

Deletes the GTT address-map instance associated with this SCCP network.

instance

This value uniquely identifies a specific previously defined instance of a GTT address-map.
instance: enter an integer from 1 to 4096.

Usage

Use this command to link a GTT address-map, configured with the GTT Address Map configuration mode, to a specific SCCP network configuration.

Example

global-title-translation address-map instance gtt-map1
hop-count

This command specifies the hop count for this SCCP network.

Product
SGSN
HNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > SCCP Network Configuration
configure > sccp-network id_number

Entering the above command sequence results in the following prompt:

[local]host_name(config-sccp-network-sccp_id)#

Syntax

hop-count hop_cnt

default hop-count

default

Resets the hop-count value to the system default of 5.

hop_cnt

The hop count to assign to this SCCP network.

hop_cnt: enter an integer from 1 to 15.

Usage

Use this command to define the hop count for this SCCP network.

Example

The following command sets the hop count to 3:

hop-count 3
self-point-code

This command specifies the SS7 point code for this SCCP service.

Product
SGSN
HNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > SCCP Network Configuration
configure > sccp-network id_number

Entering the above command sequence results in the following prompt:

[local]host_name(config-sccp-network-sccp_id)#

Syntax

self-point-code point_code

no self-point-code

no

Deletes the configured self point code.

point_code

Defines the point code to assign to this SCCP network service.

point_code: value entered must adhere to the point code variant selected when the SCCP network instance was defined:

- ITU Range 0.0.1 to 7.255.7
- ANSI Range 0.0.1 to 255.255.255
- TTC Range 0.0.1 to 15.31.255
- a string of 1 to 11 combined digits ad period.

Usage
Use this command to assign the self point code to use for this SCCP service.

Example
The following command sets an ITU-based point code for this SCCP service:

self-pointcode 4.121.5

The following command removes the configured self-point code:

no self-pointcode
timeout

This command configures the timeout parameters for this SCCP network.

Product
SGSN
HNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > SCCP Network Configuration
configure > sccp-network id_number

Entering the above command sequence results in the following prompt:

[local]host_name(config-sccp-network-sccp_id)#

Syntax

timeout { attack-timer | congestion-timer | conn-est-timer | crd-timer | decay-timer | iar-timer | ias-timer | interval-timer | reassembly-timer | release-timer | repeat-release-timer | reset-timer | sst-timer } +

default timeout

no timeout timer

---

attack-timer time

Defines the time before the attack timer expires.

`time`: enter an integer between 1 and 10.

---

congestion-timer time

Defines the time before the congestion timer expires.

`time`: enter an integer between 1 and 10.

---

conn-est-timer time

Defines the time before the connection timer expires.

`time`: enter an integer between 6 and 12.

---

crd-timer time

Defines the time before the coordinated-state-change timer expires.

`time`: enter an integer between 60 and 120.

---

decay-timer time

Defines the time before the decay timer expires.

`time`: enter an integer between 1 and 10.
### timeout

**iar-timer time**
Defines the time before the inactivity-receive timer expires.
`time`: enter an integer between 60 and 120.

**ias-timer time**
Defines the time before the inactivity-send timer expires.
`time`: enter an integer between 30 and 60.

**interval-timer time**
Defines the time before the interval timer expires.
`time`: enter an integer between 6 and 12

**reassembly-timer time**
Defines the time before the reassembly-timer expires.
`time`: enter an integer between 10 and 20.

**release-timer time**
Defines the time before the release-assembly timer expires.
`time`: enter an integer between 1 and 2.

**repeat-release-timer time**
Defines the time before repeat-release timer expires.
`time`: enter an integer between 1 and 2

**reset-timer time**
Defines the amount of time before the reset timer expires.
`time`: enter an integer between 1 and 2

**sst-timer time**
Defines the amount of time before the subsystem status test timer expires.
`time`: enter an integer between 5 and 1200.

**default**
Resets the timeout parameter to the system default.

**no**
Deletes the specified timer configuration.

#### Usage
Use this command to assign timeout timers and timeout values for this SCCP service.

#### Example
`
timeout reset-timer 75
`
Chapter 276
SCTP Parameter Template Configuration Mode Commands

This chapter provides information about commands used to configure parameters for Stream Control Transmission Protocol (SCTP) associations. The commands become part of a template that can be associated with services running on the system.

Mode

Exec > Global Configuration > SCTP Parameter Template Configuration

configure > sctp-param-template template_name

Entering the above command sequence results in the following prompt:

[local]host_name(sctp-param-template)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**

Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**
Use this command to return to the parent configuration mode.
sctp-alpha

Configures the SCTP retransmission timeout (RTO) alpha value.

Product
MME

Privilege
Administrator

Mode
Exec > Global Configuration > SCTP Parameter Template Configuration

configure > sctp-param-template template_name

Entering the above command sequence results in the following prompt:

[local]host_name(sctp-param-template)#

Syntax

sctp-alpha value

default sctp-alpha

default

Returns the command to its default setting of 5.

value

Default: 5
Specifies the SCTP retransmission timeout alpha value. value must be an integer from 0 through 65535.

Usage

Use this command to configure the SCTP RTO alpha value. The RTO alpha value is used in calculating the smoothed round-trip time (SRTT) and the round-trip time variation (RTTVAR) for new round trip time (RTT) measurements.

Example

The following command sets the SCTP RTO alpha value to 10:

    sctp-alpha 10
sctp-alt-accept-flag

Configures the SCTP alternate accept flag for additional life time for the association.

Product
MME

Privilege
Administrator

Mode
Exec > Global Configuration > SCTP Parameter Template Configuration

configure > sctp-param-template template_name

Entering the above command sequence results in the following prompt:

[local]host_name(sctp-param-template)#

Syntax

sctp-alt-accept-flag { disable | enable }

default sctp-alt-accept-flag

default

Returns the command to its default setting of enable.

disable | enable

Specifies if the alternate accept flag is enabled or disabled.

Usage

Use this command to configure the SCTP alternate accept flag for additional life time for the association.

Example

The following command disables the alternate accept flag for the SCTP association:

sctp-alt-accept-flag disable
**sctp-beta**

Configures the SCTP retransmission timeout (RTO) beta value.

**Product**
MME

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > SCTP Parameter Template Configuration

```
configure > sctp-param-template template_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(sctp-param-template)#
```

**Syntax**

```
sctp-beta value
```

```
default sctp-beta
```

<table>
<thead>
<tr>
<th>default</th>
<th>Returns the command to its default setting of 10.</th>
</tr>
</thead>
</table>

```
value
```

Specifies the SCTP retransmission timeout beta value as an integer from 0 through 65535. Default: 10

**Usage**

Use this command to configure the SCTP RTO beta value. The RTO beta value is used in calculating the smoothed round-trip time (SRTT) and the round-trip time variation (RTTVAR) for new round trip time (RTT) measurements.

**Example**

The following command sets the SCTP RTO beta value to 20:

```
sctp-beta 20
```
sctp-checksum-type

Configures the checksum type used to increase the integrity of the SCTP packets during transmission.

Product
- MME

Privilege
- Administrator

Mode
- Exec > Global Configuration > SCTP Parameter Template Configuration
- configure > sctp-param-template template_name

Entering the above command sequence results in the following prompt:

[local]host_name(sctp-param-template)#

Syntax

```
sctp-checksum-type { adler32 | crc32 }
```

```
default sctp-checksum-type
```

<table>
<thead>
<tr>
<th>Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>default sctp-checksum-type</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Returns the command to its default setting of CRC32.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>adler32</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the type of checksum used to increase data integrity of SCTP packets.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>adler32</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies that the Adler-32 checksum algorithm is used to increase data integrity for SCTP packets.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>crc32</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies that a 32-bit cyclic redundancy check is used to increase data integrity of SCTP packets.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Usage</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use this command to select the checksum for data integrity of SCTP packets.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>The following command enables the Adler-32 checksum algorithm used to increase data integrity of SCTP packets:</td>
</tr>
</tbody>
</table>

```
sctp-checksum-type adler32
```

<table>
<thead>
<tr>
<th>Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>The following command enables the Adler-32 checksum algorithm used to increase data integrity of SCTP packets:</td>
</tr>
</tbody>
</table>

```
sctp-checksum-type adler32
```
**sctp-cookie-life**

Configures the lifetime of the SCTP cookie.

**Product**
MME

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > SCTP Parameter Template Configuration

```bash
configure > sctp-param-template template_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(sctp-param-template)#
```

**Syntax**

```
sctp-cookie-life value
```

**default sctp-cookie-life**

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>default</strong></td>
<td>Returns the command to its default setting of 600 (60000 milliseconds).</td>
</tr>
</tbody>
</table>
| **value** | Default: 600 (60000 milliseconds)  
Specifies the lifetime of the SCTP cookie. value is an integer from 50 through 1200. The range translates to 5000 milliseconds to 120000 milliseconds, as the granularity is in 100-millisecond increments. |

**Usage**

Use this command to configure the lifetime of the SCTP cookie.

**Example**

The following command configures the lifetime of the SCTP cookie to 80000 milliseconds:

```
sctp-cookie-life 800
```
sctp-max-assoc-retx

Configures the maximum number of retransmissions for SCTP associations.

**Product**

MME

**Privilege**

Administrator

**Mode**

Exec > Global Configuration > SCTP Parameter Template Configuration

configure > sctp-param-template template_name

Entering the above command sequence results in the following prompt:

[local]host_name(sctp-param-template)#

**Syntax**

```
sctp-max-assoc-retx value

default sctp-max-assoc-retx
```

---

**default**

Returns the command to its default setting of 10.

---

**value**

Specifies the maximum number of retransmissions allowed by this template for SCTP associations as an integer from 0 through 255. Default: 10

---

**Usage**

Use this command to configure the maximum number of retransmissions allowed.

**Example**

The following command configures the maximum number of retransmissions to 7:

```
sctp-max-assoc-retx 7
```
sctp-max-in-strms

Configures the maximum number of incoming SCTP streams.

Product
MME

Privilege
Administrator

Mode
Exec > Global Configuration > SCTP Parameter Template Configuration

configure > sctp-param-template template_name

Entering the above command sequence results in the following prompt:

[local]host_name(sctp-param-template)#

Syntax

sctp-max-in-strms value

default sctp-max-in-strms

default

Returns the command to its default setting of 16.

default

value

Specifies the maximum number of incoming SCTP streams as an integer from 1 through 16. Default: 16. The MME restricts the allowable range as 2-16. If a value of 1 is entered, value 2 will be applied for any MME service associated with this SCTP parameter template.

Usage

Use this command to configure the maximum number of incoming SCTP streams.

Example

The following command configures the maximum number of incoming SCTP streams to 5:

sctp-max-in-strms 5
sctp-max-init-retx

Configures the maximum number of retransmissions for SCTP initiations.

**Product**
MME

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > SCTP Parameter Template Configuration
configure > sctp-param-template template_name

Entering the above command sequence results in the following prompt:

[local]host_name(sctp-param-template)#

**Syntax**

```text
sctp-max-init-retx value

default sctp-max-init-retx
```

- **default**
  Returns the command to its default setting of 5.

- **value**
  Specifies the maximum number of retransmissions for SCTP initiations as an integer from 0 through 255. Default: 5

**Usage**

Use this command to configure the maximum number of retransmissions for SCTP initiations.

**Example**

The following command configures the maximum number of retransmissions for SCTP initiations to 10:

```text
sctp-max-init-retx 10
```
sctp-max-mtu-size

Configures the maximum transmission unit (MTU) size (in bytes) for SCTP streams.

Product
MME

Privilege
Administrator

Mode
Exec > Global Configuration > SCTP Parameter Template Configuration

configure > sctp-param-template template_name

Entering the above command sequence results in the following prompt:

[local]host_name(sctp-param-template)#

Syntax

sctp-max-mtu-size bytes

default sctp-max-mtu-size

<table>
<thead>
<tr>
<th>bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Returns the command to its default setting of 1500 bytes.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the maximum MTU size (in bytes) for SCTP streams as an integer from 508 through 65535. Default: 1500</td>
</tr>
</tbody>
</table>

Usage
Use this command to configure the maximum MTU size, in bytes, for SCTP streams.

Example
The following command configures the maximum MTU size for SCTP streams to 3000:

    sctp-max-mtu-size 3000
sctp-max-out-strms

Configures the maximum number of outgoing SCTP streams.

Product
MME

Privilege
Administrator

Mode
Exec > Global Configuration > SCTP Parameter Template Configuration

configure > sctp-param-template template_name

Entering the above command sequence results in the following prompt:

[local]host_name(sctp-param-template)#

Syntax

sctp-max-out-strms value

default sctp-max-out-strms

default

Returns the command to its default setting of 2.

value

Specifies the maximum number of outgoing SCTP streams as an integer from 1 through 16.
MME Default 16.
SGSN Default: 2.

Usage

Use this command to configure the maximum number of outgoing SCTP streams.
The MME restricts the allowable range as 2-16. If a value of 1 is entered, value 2 will be applied for any
MME service associated with this SCTP parameter template.
For the SGSN, if the user tries to configure the value of sctpmax-out-strms less than "2", a message is
displayed and the default value is set.

Example

The following command configures the maximum number of outgoing SCTP streams to 5:

sctp-max-out-strms 5
sctp-max-path-retx

Configures the maximum number of retransmissions of SCTP paths.

**Product**
MME

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > SCTP Parameter Template Configuration

configure > sctp-param-template template_name

Entering the above command sequence results in the following prompt:

[local]host_name(sctp-param-template)#

**Syntax**

sctp-max-path-retx value

default sctp-max-path-retx

default

Returns the command to its default setting of 5.

value

Specifies the maximum number of retransmissions of SCTP paths as an integer from 0 through 255. Default: 5

**Usage**

Use this command to configure the maximum number of retransmissions of SCTP paths. An SCTP path is a connection between an endpoint address and a peer endpoint address.

**Example**

The following command configures the maximum number of retransmissions of SCTP paths to 10:

```
sctp-max-path-retx 10
```
sctp-min-mtu-size

Configures the minimum maximum transmission unit (MTU) size (in bytes) for SCTP streams.

Product
MME

Privilege
Administrator

Mode
Exec > Global Configuration > SCTP Parameter Template Configuration
configure > sctp-param-template template_name

Entering the above command sequence results in the following prompt:

[local]host_name(sctp-param-template)#

Syntax

sctp-min-mtu-size bytes

default sctp-min-mtu-size

Syntax

default

Returns the command to its default setting of 508 bytes.

bytes

Specifies the minimum MTU size (in bytes) for SCTP streams as an integer from 508 through 65535.
Default: 508

Usage

Use this command to configure the minimum MTU size, in bytes, for SCTP streams.

Example

The following command configures the minimum MTU size for SCTP streams to 1000:

sctp-min-mtu-size 1000
sctp-rto-initial

Configures the initial time for SCTP retransmission timeouts (RTOs).

Product
MME

Privilege
Administrator

Mode
Exec > Global Configuration > SCTP Parameter Template Configuration

**configure > sctp-param-template template_name**

Entering the above command sequence results in the following prompt:

[local]host_name(sctp-param-template)#

Syntax

```plaintext
sctp-rto-initial value

default sctp-rto-initial
```

**default**

Returns the command to its default setting of 30 (3000 milliseconds).

**value**

Specifies the initial time for SCTP RTO as an integer from 1 through 1200. The granularity is in 100ms increments (20 = 2000ms). Default: 30 (3000 milliseconds)

Usage

Use this command to configure the initial time for SCTP RTOs.

Example

The following command configures the initial SCTP RTO to 6000ms:

```plaintext
sctp-rto-initial 60
```
sctp-rto-max

Configures the maximum time for SCTP retransmission timeouts (RTOs).

**Product**
MME

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > SCTP Parameter Template Configuration
configure > sctp-param-template template_name

Entering the above command sequence results in the following prompt:

[local]host_name(sctp-param-template)#

**Syntax**

```
  sctp-rto-max  value
  default  sctp-rto-max
```

- **default**
  Returns the command to its default setting of 600 (60000 milliseconds).

- **value**
  Specifies the maximum time for SCTP RTOs as an integer from 5 through 1200. The granularity is in 100ms increments (120 = 12000ms). Default: 600 (60000 milliseconds)

**Usage**

Use this command to configure the maximum time for SCTP RTOs.

**Example**

The following command configures the maximum time for SCTP RTOs to 120000ms:

```
sctp-rto-max 120
```
sctp-rto-min

Configures the minimum SCTP retransmission timeout (RTO).

**Product**
MME

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > SCTP Parameter Template Configuration

```
configure > sctp-param-template template_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(sctp-param-template)#
```

**Syntax**

```
sctp-rto-min [ units-10ms ] value
```

```
default sctp-rto-min
```

<table>
<thead>
<tr>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Returns the command to its default setting of 10 (1000 milliseconds).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>units-10ms</th>
</tr>
</thead>
<tbody>
<tr>
<td>Including this keyword specifies that the integer <em>value</em> is to be calculated using 10ms increments (instead of 100ms increments) to allow for finer granularity. <em>value</em> is an integer from 0 through 500.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the minimum time for SCTP RTOs as an integer from 1 through 50. The granularity is in 100ms increments (20 = 2000ms). Default: 10 (1000 milliseconds)</td>
</tr>
</tbody>
</table>

**Usage**
Use this command to configure the minimum time for SCTP RTOs.

**Example**
The following command configures the minimum time for SCTP RTOs to 2000ms:
```
  sctp-rto-min 20
```
**sctp-sack-frequency**

Configures the frequency of transmission of SCTP selective acknowledgements (SACK).

**Product**
MME

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > SCTP Parameter Template Configuration

```bash
configure > sctp-param-template template_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(sctp-param-template)#
```

**Syntax**

```
sctp-sack-frequency value
```

```bash
default sctp-sack-frequency
```

```
default
   Returns the command to its default setting of 2.
```

```
value
   Specifies the frequency of SCTP selective acknowledgements as an integer from 1 through 20. Default: 2
```

**Usage**

Use this command to configure the frequency of SCTP selective acknowledgements.

**Example**

The following command configures the frequency of SCTP selective acknowledgements to 10:

```
sctp-sack-frequency 10
```
**sctp-sack-period**

Configures the delay before sending an SCTP selective acknowledgement (SACK).

**Product**
MME

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > SCTP Parameter Template Configuration
configure > sctp-param-template template_name

Entering the above command sequence results in the following prompt:

```
[local]host_name(sctp-param-template)#
```

**Syntax**

```
sctp-sack-period [ units-10ms ] value
default sctp-sack-period
```

**default sctp-sack-period**

```
default
```

Returns the command to its default setting of 2 (200 milliseconds).

```
units-10ms
```

Including this keyword specifies that the integer `value` is to be calculated using 10ms increments (instead of 100ms increments) to allow for finer granularity. `value` is an integer from 0 through 50.

```
value
```

Specifies the period for SCTP selective acknowledgements as an integer from 0 through 5. The granularity is in 100ms increments (3 = 300ms). Default: 2 (200 milliseconds).

**Important:** If this value is set to 0, the MME service will automatically configure a 10 ms sack period in order to allow proper initialization of the CCPU SCTP stack.

**Usage**

Use this command to configure the period for SCTP selective acknowledgements.

**Example**

The following command configures the period for SCTP selective acknowledgements to 400ms (using the 10ms granularity):

```
sctp-sack-period units-10ms 40
```
sctp-start-mtu-size

Configures the start maximum transmission unit (MTU) size (in bytes) for SCTP streams.

**Product**
MME

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > SCTP Parameter Template Configuration

```
configure > sctp-param-template template_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(sctp-param-template)#
```

**Syntax**

```
sctp-start-mtu-size bytes
```

```
default sctp-start-mtu-size
```

<table>
<thead>
<tr>
<th>default</th>
<th>Returns the command to its default setting of 1500 bytes.</th>
</tr>
</thead>
<tbody>
<tr>
<td>bytes</td>
<td>Specifies the start MTU size (in bytes) for SCTP streams as an integer from 508 through 65535. Default: 1500</td>
</tr>
</tbody>
</table>

**Usage**
Use this command to configure the start MTU size, in bytes, for SCTP streams.

**Example**
The following command configures the start MTU size for SCTP streams to 3000:

```
sctp-start-mtu-size 3000
```
timeout

Configures timeouts for SCTP data chunk bundle transmissions and/or SCTP heartbeat request responses.

Product
MME

Privilege
Administrator

Mode
Exec > Global Configuration > SCTP Parameter Template Configuration

configure > sctp-param-template template_name

Entering the above command sequence results in the following prompt:

[local]host_name(sctp-param-template)#

Syntax

timeout { sctp-bundle [ units-10ms ] timer | sctp-heart-beat value }

[ default | no ] timeout { sctp-bundle | sctp-heart-beat }

default
Returns the command to its default setting of disabled for sctp-bundle and 30 seconds for sctp-heart-beat.

no
Removes the selected configuration.

sctp-bundle [ units-10ms ] timer
Specifies that SCTP data chunks are to be queued until this timer expires at which time the data chunks are bundled and committed for transmission.

timer is an integer from 1 through 65535, in 100ms increments (10 = 1000ms or 1 second).

[ units-10ms ]: Including this optional keyword specifies that the integer timer is to be calculated using 10ms increments (instead of 100ms increments) to allow for finer granularity.

Default: Disabled.

sctp-heart-beat value

Default: 30 seconds
Specifies the SCTP heartbeat timeout (in seconds) as an integer from 1 through 300. An SCTP heartbeat is sent to a peer to determine reachability. If an acknowledgement is not received before this timer runs out, heartbeat requests are no longer sent and the peer is considered unreachable.

Usage
Use this command to configure timeouts for SCTP data chunk bundle transmissions and/or SCTP heartbeat request responses.

Example

The following command enables the SCTP data chunk bundle timeout value and configures it to 2 seconds:
timeout sctp-bundle 20
Chapter 277
Service Redundancy Protocol Configuration Mode Commands

The Service Redundancy Protocol Mode is used to configure properties for Interchassis Session Recovery (ICSR) services.

Mode

Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

configure > context context_name > service-redundancy-protocol

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-srp)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

Important: SRP commands must be identically configured on both the active and standby ICSR chassis.
**audit**

Sets the start time and periodicity for ICSR Service Redundancy Protocol (SRP) audits.

**Product**
All products supporting ICSR

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

`configure > context context_name > service-redundancy-protocol`

Entering the above command sequence results in the following prompt:

```
[context_name] host_name(config-srp) #
```

**Syntax**

```
[no] audit daily-start-time hour minute
[no] audit periodicity minutes

default audit periodicity
```  

**default**

Resets the specified parameter to its default setting of 60.

**no**

Disables the specified function.

**daily-start-time** *hour* *minute*

Specifies the daily start time. *hour* is a two-digit integer from 00 through 23. *minute* is a two-digit interval from 00 through 59. For example, a start time of 06 00 indicates that the audit will begin at 6:00 AM.

**periodicity** *minutes*

Specifies the interval in minutes for generating SRP audit statistics as an integer from 60 through 43200. For example, a periodicity of 90 indicates that SRP audit statistics will be generated every 90 minutes beginning at the specified start time. Default = 60.

**Usage**

Use this command and its keywords to specify the start time and periodicity for generating ICSR SRP audit statistics. This audit ensures that two ICSR peers are in synch and identifies any discrepancies prior to scheduled or unscheduled switchover events.

**Example**

The following command sequence specifies a start time of midnight and a periodicity of every two hours for generating SRP statistics:

```
audit daily-start-time 06 00
```
audit periodicity 90
bind

Binds the service to the IP address of the local chassis.

**Product**
All products supporting ICSR

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

```bash
configure context context_name service-redundancy-protocol
```

Entering the above command sequence results in the following prompt:

```bash
[context_name]host_name(config-srp)#
```

**Syntax**

```bash
bind address { ipv4_address | ipv6_address }
```

**no bind address**

```bash
no
```

Removes the IP bind address.

```bash
ipv4_address | ipv6_address
```

Specifies the system IP address using IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

**Important:** Both peers must be using the same address family (IPv4 or IPv6) or the Service Redundancy Protocol (SRP) connection will not be established.

**Usage**

Defines the IP address of the local chassis defined as part of the ICSR configuration.

**Example**

The following example binds the service to the IP address 10.1.1.1:

```bash
bind address 10.1.1.1
```
chassis-mode

Defines the chassis’s operational mode - primary or backup - for ICSR.

Product
All products supporting ICSR

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

configure > context context_name > service-redundancy-protocol

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-srp)#

Syntax

chassis-mode { backup | primary }

default chassis-mode

default
 Resets the chassis mode to the default setting of backup.

backup
 (Default) Configures the system as the backup chassis operating in standby state.

primary
 Configures the system as the primary chassis operating in active state.

Usage
Sets the chassis mode (primary or backup) for the system within the framework of ICSR.

Example

The following example configures the system as the primary chassis operating in active state

chassis-mode primary
checkpoint session

Configures checkpointing parameters between ICSR active and standby chassis.

Product
All products supporting ICSR

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

configure > context context_name > service-redundancy-protocol

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-srp)#

Syntax

checkpoint session duration seconds
default checkpoint session

default

Resets the following checkpoint session parameters to their default values:

Usage
Sets the amount of time the chassis waits before checkpointing an existing call session.
Configures the interval between the sending of macro-checkpoints (full checkpoints) between the active and standby chassis.
For additional information on ICSR checkpointing, see the System Administration Guide.

Example

The following example configures sets the checkpoint session duration to 6500 seconds:

checkpoint session duration 6500
configuration-interval

Defines the configuration validation interval.

Product
All products supporting ICSR

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

\texttt{configure \> context context\_name \> service\_redundancy\_protocol}

Entering the above command sequence results in the following prompt:

\texttt{[context\_name]host\_name(config\_srp)\#}

Syntax

configuration-interval \textit{interval}

default configuration-interval

---

default

Resets the configuration interval to the default setting of 3600 seconds.

interval

Specifies the amount of time (number of seconds) between one configuration validation and the next configuration validation. \textit{interval} must be an integer from 1 through 65535. Default = 3600.

Usage

This configures the interval between configuration validations of the primary and backup chassis.

Example

The following example sets the configuration interval to 34 seconds:

configuration-interval 34
dead-interval

Defines the timeout interval before a peer is determined to be down.

**Product**
All products supporting ICSR

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

```
configure > context context_name > service-redundancy-protocol
```

Entering the above command sequence results in the following prompt:

```
[context_name] host_name(config-srp)#
```

**Syntax**

```
dead-interval interval
```

```
default dead-interval
```

```
default
```
Resets the dead interval to the default setting of 30 seconds.

```
interval
```
Specifies the amount of time (in seconds) for the dead interval. `interval` must be an integer from 1 through 65535. Default = 30.

**Usage**
This command specifies the amount of time that one chassis waits to receive a communication from a peer before the listening chassis determines that the peer chassis is down.

**Example**
The following example sets the dead interval to 65 seconds:

```
deal-interval 65
```
**delay-interval**

Configures the delay time for starting the dead timer after configuration files are loaded.

### Product
All products supporting ICSR

### Privilege
Security Administrator, Administrator

### Mode
Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

```plaintext
configure > context context_name > service-redundancy-protocol
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-srp)#
```

### Syntax

- `delay-interval interval`
- `default delay-interval`

#### default delay-interval

- `default`
  
  Sets or restores the default value assigned for the specified parameter.

- `interval`
  
  Specifies the amount of time (in seconds) for the delay interval. `interval` must be an integer from 1 through 65535.

### Usage

This configures interval for starting the dead timer after configuration files are loaded.

### Example

The following example sets the delay interval to 65 seconds after the configuration files are loaded:

```
delay interval 65
```
delta-route-modifier

Specifies the delta used to compute the route modifier difference between the active and standby chassis. This delta is applied only in the standby state. For Release 15.0 or higher, it is used in both states.

**Product**

All products supporting ICSR

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

configure > context context_name > service-redundancy-protocol

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-srp)#
```

**Syntax**

```
delta-route-modifier value

default delta-route-modifier
```

**Usage**

The delta-route-modifier is used to compute the route modifier difference between active and standby chassis.

**Example**

The following example sets the delta for the route modifier to 2:

```
delta-route-modifier 2
```
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**

Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Use this command to return to the parent configuration mode.
**hello-interval**

Defines the lapse time between sending the hello message.

**Product**
All products supporting ICSR

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

`configure > context context_name > service-redundancy-protocol`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-srp)#
```

**Syntax**

```
hello-interval interval

default hello-interval
```

**Usage**

Resets the hello interval to the default setting of 10 seconds.

```
interv
```

Specifies the lapse time (in seconds) between sending the hello message. `interval` must be an integer from 1 through 65535. Default = 10.

**Example**

This command configures the hello interval - the amount of time that lapses between the sending of each hello message. Each chassis sends the other chassis a hello message at the expiration of every hello interval.

The following example sets the hello interval to 35 seconds:

```
hello-interval 35
```
**internal-switchover-retry-interval**

Defines the interval between internal switchover retries.

**Product**
All products supporting ICSR

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

```
configure > context context_name > service-redundancy-protocol
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-srp)#
```

**Syntax**

```
internal-switchover-retry-interval interval
```

```
default internal-switchover-retry-interval
```

```
default

Resets the internal switchover retry interval to the default setting of 60 seconds.
```

```
interval

Specifies the amount of time (in seconds) between internal switchover retries. *interval* must be an integer from 10 through 120. Default = 60.
```

**Usage**

This configures the interval between internal switchover retries. The system only initiates internal switchovers if Service Redundancy Protocol (SRP) monitoring is configured.

**Important:** See the `monitor authentication-probe`, `monitor bgp`, or `monitor diameter` commands for more information on associated SRP monitoring.

**Example**

The following example sets the internal switchover retry interval to 34 seconds:

```
internal-switchover-retry-interval 34
```
**monitor authentication-probe**

Enables SRP monitoring of the connection between the specified AAA server and the primary chassis.

**Product**
All products supporting ICSR

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

configure > context context_name > service-redundancy-protocol

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-srp)#
```

**Syntax**

```
[ no ] monitor authentication-probe context context_name { ipv4_address | ipv6_address } [ group group_id ] [ port port_number ]
```

- **no**
  Turns off the monitoring.

- **context context_name**
  Identifies the context being used.
  context_name must be an existing context expressed as an alphanumeric string of 1 through 79 characters.

- **ipv4_address | ipv6_address**
  Defines the IP address of the AAA server to be monitored in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

- **group group_id**
  Defines a Service Redundancy Protocol (SRP) peer group as an integer from 0 through 9. Default = 0.
  In an Interchassis Session Recovery (ICSR) configuration, failover would occur if all peers within a group fail.

- **port port_number**
  Identifies a specific AAA server port for the authentication probe. port_number must be an integer from 1 through 65535.

**Usage**
This command initiates monitoring of the connection between the primary chassis and the specified AAA server through the use of authentication probe packets. If the connection drops, the standby chassis becomes active.

**Example**

This section provides an example of how to use the `monitor authentication-probe` command.
The following example initiates the connection monitoring between the primary chassis and AAA server 10.2.3.4 at port 1025:

```
monitor authentication-probe context test1 10.2.3.4 port 1025
```
monitor bfd

Enables SRP monitoring of the connection between the specified Bidirectional Forwarding Detection (BFD) neighbor and the primary chassis.

Product
All products supporting ICSR

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

configure > context context_name > service-redundancy-protocol

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-srp)#

Syntax

[ no ] monitor bfd context context_name { ipv4_address | ipv6_address } { chassis-to-chassis | chassis-to-router }

no
Disables monitoring.

countext context_name
Identifies the context being used. context_name must be an existing context expressed as an alphanumeric string of 1 through 79 characters.

ipv4 _address | ipv6_address
Defines the IP address of the BFD neighbor to be monitored, entered using IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation

chassis-to-chassis | chassis-to-router

chassis-to-chassis: BFD runs between primary and backup chassis on non-SRP links.
chassis-to-router: BFD runs between chassis and router.

Usage

This command initiates monitoring of the connection between the primary chassis and the specified BFD neighbor in the specified context. If the connection drops, the standby chassis becomes active.

**Important:** BFD monitoring must run between chassis-to-chassis or chassis-to-router.

Example

The following example initiates the chassis-to-chassis connection monitoring between the primary chassis and BFD neighbor 12.2.1.54:
monitor bfd context test 12.2.1.54 chassis-to-chassis
monitor bgp

Enables SRP monitoring of the connection between the specified Border Gateway Protocol (BGP) peer and the primary chassis.

Product
All products supporting ICSR

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration
configure > context context_name > service-redundancy-protocol

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-srp)#

Syntax

[ no ] monitor bgp context context_name { ipv4_address | ipv6_address } [ group group_id [ vrf vrf_name ] ]

no
Disables monitoring.

class context context_name
Identifies the context being used. context_name must be an existing context expressed as an alphanumeric string of 1 through 79 characters.

ipv4_address | ipv6_address
Specifies the IP address of the BGP peer to be monitored in IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

group group_id
Defines a Service Redundancy Protocol (SRP) peer group as an integer from 0 through 9. Default = 0. In an Interchassis Session Recovery (ICSR) configuration, failover would occur if all peers within a group fail (instead of all BGP peers in a context). This option is useful in deployments in which a combination of IPv4 and IPv6 peers are spread across multiple paired VLANs and IPv4 or IPv6 connectivity is lost by all members of a peer group.

vrf vrf_name
Defines the VPN Routing/Forwarding instance as an alphanumeric string of 1 through 63 characters.

Usage
This command initiates monitoring of the connection between the primary chassis and the specified BGP peer in the specified context. If the connection drops, the standby chassis becomes active.

Example
The following example initiates the connection monitoring between the primary chassis and BGP peer 125.2.1.56:

```
monitor bgp context test 125.2.1.56
```
monitor diameter

Enables SRP monitoring of the connection between the specified Diameter server and the primary chassis.

**Product**
All products supporting ICSR

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

```bash
configure > context context_name > service-redundancy-protocol
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-srp)#
```

**Syntax**

```
[ no ] monitor diameter context context_name endpoint endpoint_name  [ fqdn fqdn | group group_id | peer { ipv4_address | ipv6_address } ] [ port port_number ]
```

- **no**
  Turns off the monitoring.

- **context context_name**
  Identifies the context being used. `context_name` must be an existing context expressed as an alphanumeric string of 1 through 79 characters.

- **endpoint endpoint_name**
  Identifies the endpoint being used. `endpoint_name` must be for the Diameter server expressed as an alphanumeric string of 1 through 63 characters.

- **fqdn fqdn**
  Identifies a Fully Qualified Domain Name (FQDN). `fqdn` must be for the Diameter server expressed an alphanumeric string of 1 through 127 characters.

- **group group_id**
  Defines a Service Redundancy Protocol (SRP) peer group as an integer from 0 through 9. Default = 0. In an Interchassis Session Recovery (ICSR) configuration, failover would occur if all peers within the specified group fail.

- **peer { ipv4_address | ipv6_address }**
  Defines the IP address of the Diameter server to be monitored, entered using IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.
**monitor diameter**

`port port_number`

Identifies a specific port to monitor. `port_number` must be the port for the Diameter server and an integer from 1 through 65535.

**Usage**

This command initiates monitoring of the connection between the primary chassis and the specified Diameter server in the specified context. If the connection drops, the standby chassis becomes active.

**Important:** Endpoint name, FQDN, IP address, and port must all match the Diameter protocol configured values for the peer state to be updated.

**Example**

The following example initiates the connection monitoring between the primary chassis and the Diameter server on context `test1` and endpoint `end2`:

```
monitor diameter context test1 10.6.7.8 endpoint end2
```
num-internal-switchover-retry

Defines the number of times an internal switchover would be retried.

Product
All products supporting ICSR

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

configure > context context_name > service-redundancy-protocol

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-srp)#

Syntax

num-internal-switchover-retry retries

default num-internal-switchover-retry

default

Resets the configuration interval to the default setting of 3 retries.

retries

The number of times an internal switchover would be retried in case of standby chassis. retries must be an integer from 1 through 10.
Default: 3

Usage

This configures the number of times an internal switchover would be retried in case of standby chassis failure to respond or become active.

Example

The following example sets the retry number to 5:

num-internal-switchover-retry 5
**peer-ip-address**

Specifies the IP address for the peer chassis.

**Product**
All products supporting ICSR

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

```bash
configure > context context_name > service-redundancy-protocol
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-srp)#
```

**Syntax**

```
peer-ip-address { ipv4_address | ipv6_address }
```

```bash
no peer-ip-address
```

- **no**
  Removes the peer IP address of the backup chassis.

- **ipv4_address | ipv6_address**
  Specifies the IP address of the backup chassis, entered using IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

**Important:** Both peers must be using the same address family (IPv4 or IPv6) or the Service Redundancy Protocol (SRP) connection will not be established.

**Usage**

This command is used to identify the peer chassis in the ICSR configuration. From the primary’s perspective, the peer is the backup and from the backup’s perspective, the peer is the primary.

**Example**

The following example specifies 10.2.3.4 as a backup peer system to the primary system:

```
peer-ip-address 10.2.3.4
```
priority

Sets the initial ICSR priority of each peer chassis.

**Important:** `priority` takes affect only during simultaneous initializing of all chassis in an ICSR configuration, and only if a misconfiguration has both chassis in the same mode (both Primary or both Backup).

**Product**
All products supporting ICSR

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

`configure > context context_name > service-redundancy-protocol`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-srp)#
```

**Syntax**

```
priority priority_value

default priority
```

**default priority**

Resets the priority to the default setting of 125.

**priority_value**

Specifies the priority for the chassis. `priority_value` must be an integer from 1 through 255, where 1 is the highest priority. Default = 125.

**Usage**

This command determines which chassis transitions to the Active state when all chassis have the same mode configuration. `priority` acts as a tie breaker for the state determination only when all chassis initialize simultaneously. The chassis with the higher priority (lower number) becomes Active, while the chassis with the lower priority (higher number) becomes Standby.

Once chassis become operational (after initialization), if there is an event requiring a chassis change of state, then each chassis returns to its previous state (Active or Standby) after both chassis recover.

**Example**

The following example sets the priority value to 5:

```
priority 5
```
route-modifier

Sets the route modifier for the peer chassis.

**Product**
All products supporting ICSR

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Service Redundancy Protocol Configuration

```
configure > context context_name > service-redundancy-protocol
```
Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-srp)#
```

**Syntax**

```
route-modifier threshold threshold_value
```

```
default route-modifier
```

```
default
```
Resets the route modifier to the default setting of 16.

```
threshold_value
```
Specifies the value that causes the route-modifier counter to be reset to the initial value. `threshold_value` must be an integer from 2 through 32. Default = 16.

**Usage**
This command is used to determine when the route modifier should be reset to its initial value to avoid rollover.

**Example**
The following example sets the route modifier threshold to 10:

```
route-modifier threshold 10
```
Chapter 278
Session Event Module Configuration Mode Commands

The Session Event Module Configuration Mode is used to configure how subscriber-specific event data is handled on the S-GW. As users attach, detach, and move through the network, they trigger signaling events that need to be recorded. To provide a per-subscriber level of reporting, the S-GW sends a stream of user event data to an event reporting server over SFTP.

Mode

Exec > Global Configuration > Context Configuration > Session Event Module Configuration

`configure > context context_name > session-event-module`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-event)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
**end**

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
end

**Usage**
Use this command to return to the Exec mode.
event

Sets the method and destination for transferring event files.

Product
SAEGW
S-GW

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > Session Event Module Configuration
configure > context context_name > session-event-module

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-event)#

Syntax

```bash
event { purge { storage-limit bytes | time-limit seconds } | push-interval value | push-trigger space-usage-percent trigger_percentage | remove-file-after-transfer | transfer-mode { pull [ module-only ] | push primary { encrypted-url encrypted_url | url url } [ max-files files ] [ module-only ] [ secondary { encrypted-secondary-url url | secondary-url url } ] [ via local-context ] } | use-harddisk }

default event [ purge | push-interval | push-trigger space-usage-percent | remove-file-after-transfer | transfer-mode | use-harddisk ]

no event [ purge | remove-file-after-transfer | use-harddisk ]
```

default

Configures the default setting for the specified keyword(s):

- `purge`: Not enabled.
- `push-interval`: 60 seconds
- `push-trigger`: 80 percent
- `remove-file-after-transfer`: Disabled
- `transfer mode`: Push
- `use-harddisk`: Disabled

no

Disables the configured event file storage and processing in this mode:

- `purge`: Disables the deleting of record files on the hard disk based on a storage limit or a time limit.
- `remove-file-after-transfer`: Retains a copy of the file even after it has been pushed or pulled to another server.
- `use-harddisk`: Disables data storage on the system’s hard disk.
purge { storage-limit bytes | time-limit seconds }

Configures parameters for deleting event records from the hard drive. This command is not enabled by default.

storage-limit bytes: Specifies that event records are to be deleted from the hard drive upon reaching a storage limit defined in bytes. bytes must be an integer value from 10485760 to 146800640.

time-limit seconds: Specifies that event records are to be deleted from the hard drive upon reaching a time limit defined in seconds. seconds must be an integer value from 600 to 2592000.

push-interval value

Default: 60
Specifies the transfer interval (in seconds) when event files will be pushed to an external file server. value must be an integer from 30 through 3600.

push-trigger space-usage-percent trigger_percentage

Default: 80
Specifies the disk space utilization percentage threshold at which an automatic push is triggered and files are transferred to the external server. trigger_percentage must be an integer from 10 through 80.

remove-file-after-transfer

Default: Disabled
Specifies that the system must delete event files after they have been transferred to the external file server.

transfer-mode { pull [ module-only ] | push primary { encrypted-url encrypted_url | url url } [ max-files files ] [ module-only ] [ secondary { encrypted-secondary-url url | secondary-url url } ] [ via local-context ] }

Specifies the transfer mode to be used when transferring event files to an external file server.

• pull: Specifies that the destination server will pull the event files.

• push: Specifies that the system will push event files to the destination server. This is the default mode.

• primary encrypted-url encrypted_url: Specifies the primary URL location to which the system pushes the files in encrypted format. encrypted_url must be an alphanumeric string of 1 through 8192 characters.

• primary url url: Specifies the primary URL location to which the system pushes the event files. url must be an alphanumeric string of 1 through 1024 characters in the format: //user:password@host:[port]/direct.

• max-files number: Specifies the maximum number of files that can be transferred per push. number must be an integer from 4 to 4000.

• module-only: Specifies that the transfer of event records is to be applied only to the module type for which the configuration was originally created. If this option is not enabled, the transfer will occur for all record types.

• secondary encrypted-secondary-url url: Specifies the secondary URL location to which the system pushes the files in encrypted format. url must be an alphanumeric string of 1 through 8192 characters.
• **secondary-url url**: Specifies the secondary URL location to which the system pushes the event files.
  
  `url` must be an alphanumeric string of 1 through 1024 characters in the format:
  `/user:password@host:[port]/direct`

• **via local-context**: Specifies that the local context, and, subsequently, the SPIO management ports, will be used to pull or push event files from/to the event server.

---

**use-harddisk**

Default: Disabled

Specifies that the hard disk drive on the SMC is to be used to store S-GW event records.

---

**Usage**

Use this command to configure how the S-GW event records are moved and stored. By default, records are stored in the PSC RAM where the CDRMOD instance is running.

The `event use-harddisk` command can be run only in a context where CDRMOD is running. Configuring in any other context will result in failure with the message “Failure: Please Check if CDRMOD is running in this context or not.”

If push transfer mode is configured, the server URL to which the event files will be transferred must be specified.

When changing the transfer-mode from pull to push, disable the pull setting before changing the transfer mode to push. The push to server URL must be accessible from the local context. Also, make sure that its base directory contains an `event` subdirectory.

After changing the transfer mode from push to pull, enable pull on the destination server. Any ongoing push activity will continue until all the file transfers are completed. If there is no ongoing push activity at the time of this configuration change, the push-related configuration is nullified immediately.

---

**Example**

The following command sets the space usage trigger for pushing files to the event server to 60%:

```
event push-trigger space-usage-percent 60
```

The following command specifies that the event files are to be transferred to a server with the URL of `user:password@event-server.com`:

```
event transfer-mode push primary url //user:password@event-server.com
```
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
exit

**Usage**
Use this command to return to the parent configuration mode.
**file**

Sets the format and handling characteristics of event files.

**Product**

SAEGW

**Privilege**

Administrator

**Mode**

Exec > Global Configuration > Context Configuration > Session Event Module Configuration

configure > context context_name > session-event-module

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-event)#
```

**Syntax**

```
file [ compression { gzip | none } ] [ current-prefix string ] [ delete-timeout seconds ]
[ directory directory_name ] [ exclude-checksum-record ] [ field-separator { hyphen | omit | underscore } ]
[ file-sequence-number rulebase-seq-num ] [ headers ] [ name file_name ] [ reset-indicator ]
[ rotation { num-records number | time seconds | volume bytes } ] [ sequence-number { length length | omit | padded | padded-six-length | unpadded } ]
[ storage-limit limit ] [ time-stamp { expanded-format | rotated-format | unix-format } ]
[ trailing-text string ] [ trap-on-file-delete ] [ xor-final-record ] +
```

**default**

Configures the default setting for the specified keyword(s).

**compression { gzip | none }**

Specifies compression of S-GW event files.

- **gzip**: Enables GNU zip compression of the event file at approximately 10:1 ratio.
- **none**: Disables Gzip compression.

**current-prefix string**

Specifies a string to add to the beginning of the event file that is currently being used to store records. `string` must be an alphanumeric string of 1 through 31 characters. Default: **curr**

**delete-timeout seconds**

Specifies a time period, in seconds, after which event files are deleted. By default, files are never deleted. `seconds` must be an integer from 3600 through 3153600. Default: Disabled
**directory directory_name**

Specifies a subdirectory in the default directory in which to store event files.

*directory_name* must be an alphanumeric string of 1 through 191 characters. Default: /records/event

**exclude-checksum-record**

Excludes the final record containing #CHECKSUM followed by the 32-bit Cyclic Redundancy Check (CRC) of all preceding records from the event file.

Default: Disabled, a checksum record is included in the event file header.

**field-separator [ hyphen | omit | underscore ]**

Specifies the type of separators between two fields of an event file name:

- **hyphen**: Specifies the field separator as a “-” (hyphen) symbol between two fields.
- **omit**: Removes or omits the field separator between two fields.
- **underscore**: Specifies the field separator as an “_” (underscore) symbol between two fields.

**file-sequence-number rulebase-seq-num**

Specifies that the file name sequence numbers be unique per rulebase and event format name combination.

**headers**

Includes a file header summarizing the record layout.

**name file_name**

Specifies a string to be used as the base file name for event files.

*file_name* must be an alphanumeric string of 1 through 31 characters. The file name format is as follows:

```
base_sequencenum_timestamp
```

Default: event

- **base**: Specifies type of record in file or contains the operator-specified string. Default: event
- **sequencenum**: This is a 5-digit sequence number to detect the missing file sequence. It is unique among all event files on the system.
- **timestamp**: Adds a file creation timestamp (UTC time) in MMDDYYYYHHHMSS format.

**reset-indicator**

Specifies the inclusion of the reset indicator counter (value from 0 through 255) in the event file name. The counter is incremented whenever any of the following conditions occur:

- A peer chassis has taken over in compliance with Interchassis Session Recovery (ICSR).
- The sequence number (see sequence-number keyword) has rolled over to zero.

**rotation { num-records number | time seconds | volume bytes }**

Specifies when to close an event file and create a new one.

- **num-records number**: Specifies the maximum number of records that should be added to an event file. When the number of records in the file reaches this value, the file is complete.
  
  *number* must be an integer 100 through 10240. Default: 1024

- **time seconds**: Specifies the period of time to wait (in seconds) before closing the current event file and creating a new one.
  
  *seconds* must be an integer from 30 through 86400. Default: 3600
**volume bytes**: Specifies the maximum size of the event file (in bytes) before closing it and creating a new one.

`bytes` must be an integer from 51200 through 62914560. Note that a higher setting may improve the compression ratio when the compression keyword is set to gzip. Default: 102400

---

**sequence-number** { length length | omit | padded | padded-six-length | unpadded }

Includes with a specified format or excludes the sequence number in the file name.

- **length length**: Includes the sequence number with the specified length.
  
  `length` must be the file sequence number length with preceding zeroes in the file name, and must be an integer from 1 through 9.

- **omit**: Excludes the sequence number from the file name.

- **padded**: Includes the padded sequence number with preceding zeros in the file name. This is the default setting.

- **padded-six-length**: Includes the padded sequence number with six preceding zeros in the file name.

- **unpadded**: Includes the unpadded sequence number in the file name.

Default: padded

---

**storage-limit limit**

Files will be deleted when the specified amount of space (in bytes) is reached.

`limit` must be an integer from 10485760 through 536870912. Default: 33554432

---

**time-stamp** { expanded-format | rotated-format | unix-format }

Specifies the format of the file creation timestamp to be included in the file name.

- **expanded-format**: Specifies the UTC (Universal Time Coordinated) MMDDYYYYHHMMSS format.

- **rotated-format**: Specifies the time stamp format to YYYYMMDDHHMMSS format.

- **unix-format**: Specifies the UNIX format of `x.y`, where `x` is the number of seconds since 1/1/1970 and `y` is the fractional portion of the current second that has elapsed.

---

**trailing-text string**

Specifies the inclusion of an arbitrary text string in the file name as an alphanumeric string of 1 through 30 characters.

---

**trap-on-file-delete**

Instructs the system to send an SNMP notification (trap) when an event file is deleted due to lack of space.

Default: Disabled

---

**xor-final-record**

Specifies inserting an exclusive OR (XOR) checksum (instead of a CRC checksum) into the event file header if the `exclude-checksum-record` is left at its default setting. Default: Disabled

---

More than one of the previous keywords can be entered within a single command.
Usage
Use this command to configure event file characteristics.

Example
The following command sets the prefix of the current active event file to `Current`:

```
file current-prefix Current
```

The following command sets the base file name to `Eventfile`:

```
file name Eventfile
```
Chapter 279
SGSN ASP Configuration Mode Commands

The ASP (application server process) configuration mode defines the M3UA end-point parameters for a specific SS7 routing domain instance. The ASP instance is generated and accessed via the SS7 routing domain configuration mode commands.

Mode

Exec > Global Configuration > SS7 Routing Domain Configuration > ASP Configuration

```
configure > ss7-routing-domain routing_domain_id variant variant_type > asp instance
asp_number
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ss7-rd-ss7rd_id-asp-inst-instance)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
**end**

Exits the current mode and returns to the Exec Mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**
Change the mode back to the Exec Mode.
end-point

This command defines or deletes the IP address and/or port number to be associated with the local SCTP end-point for this ASP. At least one address needs to be configured before the end-point can be activated.

When using the `bind` keyword, this command also activates the end-point once the address has been defined. Once bound, it cannot be reconfigured until it is unbound with the `no end-point bind` command.

**Product**
SGSN
HNB-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > SS7 Routing Domain Configuration > ASP Configuration

```
configure > ss7-routing-domain routing_domain_id variant variant_type > asp instance
asp_number
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ss7-ss7rd_id-asp-inst-instance)#
```

**Syntax**

```
end-point { address ip_address context context_id | bind | port port_number }

no end-point { address ip_address context context_id | bind }
```

- **address ip_address context context_id:**
  Specifies the IP address and the context associated with the address for this end-point.
  - `ip_address`: must be defined using the standard IPv4 dotted decimal notation or the colon notation of IPv6.
  - `context context_id`: a string of 1 to 79 alphanumeric characters to identify the specific context associated with the end-point address.

- **bind**
  Activates (binds) the end-point.

- **Important:** Only use `bind` after you have configured other parameters.

- **port port_number**
  Identifies the M3UA’s SCTP port associated with this end-point.
  - `port_number`: must be an integer from 1 to 65535. Default is 2905.

- **no**
  Removes the end-point configuration or deactivates the end-point.
Caution: Entering this command will terminate all current subscriber sessions for associated peers.

Usage
Use this command to manage the ASP end-point. Once the ASP end-point is bound the end-point configuration cannot be changed until it is unbound.

Example
Activate the end-point with the following command:

```
end-point bind
```

Deactivate or unbind the end-point with the following command:

```
no end-point bind
```

Set the end-point port to default for ASP 1 with the following command:

```
default asp instance 1 end-point port
```
exit

Exits the current mode and returns to the previous mode.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Returns to the previous mode.
Chapter 280
SGSN Global Configuration Mode Commands

The commands in this mode configure parameters that impact the entire SGSN and that are independent of the GPRS or the IuPS services.

Mode

Exec > Global Configuration > SGSN Global Configuration
configure > sgsn-global

Entering the above command sequence results in the following prompt:

[local]host_name(config-sgsn-global)#

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
aggregate-ipc-msg

Configures the number of inter-process communication (IPC) messages that can be aggregated in the various managers and defines the frequency of flushing the messages.

**Product**
SGSN
HNB-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > SGSN Global Configuration
configure > sgsn-global

Entering the above command sequence results in the following prompt:

[local]host_name(config-sgsn-global)#

**Syntax**

```
aggregate-ipc-msg \{ gbmgr | linkmgr | sessmgr \} \{ flush-frequency frequency | num-msgs number_msgs \}

default aggregate-ipc-msg \{ gbmgr | linkmgr | sessmgr \}
```

- **default**
  Resets the managers to default values for flushing.

- **gbmgr**
  Selects the Gb manager to configure the number of IPC messages to be aggregated and frequency of flushing messages to the Session Manager that have been aggregated at the Gb Manager.

- **linkmgr**
  Selects the linkmgr to configure the number of IPC messages to be aggregated and frequency of flushing.

- **sessmgr**
  Selects the sessmgr to configure the number of IPC messages to be aggregated and frequency of flushing.

- **flush-frequency frequency**
  Configure the frequency, in 100-millisecond intervals, that the aggregated IPC messages will be flushed. Flushing limits the number of messenger calls between managers to transfer the received packets.
  
  *frequency*: Enter an integer from 1 to 3. Default is 1.

- **num-msgs number_msgs**
  Configure the number of IPC messages to aggregate before flushing.
  
  *number_msgs*: Enter the integer 1 (to disable aggregation) or an integer from 2 to 164 to define the number of messages. Default is 10.
**Usage**

Use this command to enable/disable aggregation of IPC messages in the linkmgr and/or the sessmgr. This command includes options to configure the frequency of aggregated message flushing and the number of packets to be buffered before the flush. This command provides a solution for reducing latency while sending the IPC messages towards the core network (CN).

The flushing limit will be based on either desired flush-frequency or maximum number of messages to be aggregated. Repeat the command to engage multiple limits.

By default, the link manager buffers packets and then send them over the SCCP link if there are events to be sent via SCCP Connection Request (SCCP CR) towards the core node. The HNB-GW/SGSN aggregate packets for 100 msecs and send them with whatever aggregation has been done during those 100 msecs.

At the HNB-GW/SGSN, this command can be used to reduce the processing involved in sending every event individually towards the core node in the following manner:

- If aggregation is enabled, then there could be a time delay for sending SCCP CRs depending on configuration of the HNB-GW or SGSN.
- If aggregation is reduced to 1, then there will be no delay for aggregation and events are sent via SCCP CR without delay. This reduces the SCCP connection setup time.

To view aggregate IPC message statistics, use command `show config | grep aggregate-ipc-msg`.

**Example**

Configure the linkmgr to buffer 45 messages before flushing the linkmgr IPC messages:

```
aggregate-ipc-msg linkmgr flush-frequency 45
```

The following command configures the `linkmgr` to flush the IPC messages towards the CN without aggregation:

```
aggregate-ipc-msg linkmgr:
```

The following command configures the `sessmgr` to flush the IPC messages towards the CN without aggregation:

```
aggregate-ipc-msg sessmgr:
```
apn-resolve-dns-query snaptr

Enable/disable sending of SNAPTR DNS query to resolve an APN for a subscriber with an EPS (evolved packet system)-capable handset.

**Important:** This command is no longer available in all 12.0 and 12.2 releases. If you do not see this command in your release, look for the `apn-resolve-dns-query snaptr` command in the APN Profile configuration mode to accomplish the same task.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > SGSN Global Configuration
configure > sgsn-global

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-sgsn-global) #
```

**Syntax**

```
[ no ] apn-resolve-dns-query snaptr
```

**default apn-resolve-dns-query**

```
default

Resets the default, the ability to send SNAPTR DNS query is disabled.
```

```
no

Disables the ability to send SNAPTR DNS query.
```

**Usage**

By default, sending the SNAPTR DNS query is disabled. Use this command to send SNAPTR DNS query when resolving an APN for an EPS-capable subscriber.

At PDP context activation, the SGSN will use the UE capability as input to select either a GGSN or a P-GW for the EPS-capable subscriber. The SNAPTR DNS query will be used for P-GW resolution. Enabling this feature will give priority to P-GW selection for E-UTRAN-capable UEs.

**Example**

Use the following command to enable sending of SNAPTR DNS query for APN resolution:

```
apn-resolve-dns-query
```

Use the following command to disable the use of SNAPTR DNS query for APN resolution:

```
no apn-resolve-dns-query
```
bssgp-message ms-flow-control-from-unknown-ms

This command determines the SGSN response to MS-Flow-Control messages received from an unknown MS.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > SGSN Global Configuration
configure > sgn-global

Entering the above command sequence results in the following prompt:

[local]host_name(config-sgsn-global)#

Syntax

bssgp-message ms-flow-control-from-unknown-ms { discard-message | send-ack | send-status }

default bssgp-message ms-flow-control-from-unknown-ms
default

Including default with the command configures the SGSN to use default behavior so that the SGSN sends BSSGP-Status messages whenever the SGSN receives an MS-Flow-Control message from an unknown MS.

discard-message

This keyword instructs the SGSN to discard the received BSSGP message. With this option, the SGSN does not send any response to the MS after discarding the received BSSGP message.

send-ack

This keyword instructs the SGSN to send an acknowledgement message (MS-Flow-Control-ACK) after receiving an MS-Flow-Control message.

send-status

Default
This keyword instructs the SGSN to send a BSSGP-Status message to the MS whenever the SGSN receives an MS-Flow-Control message from an unknown MS.

Usage

This command allows the operator to specify the action the SGSN needs to take whenever the SGSN receives an MS-Flow-Control message from an unknown mobile station. This configuration determines the response for the SGSN globally.

The list of possible actions are:
- send a BSSGP-Status response message
- send an ACK message (MS-Flow-Control-ACK)
- discard the BSSGP message

To see the statistics for the number of MS-Flow-Control messages that have been discarded, use the `show bssgp statistics` command from the Exec mode.

**Example**

Change the default configuration and have the SGSN acknowledge receipt of the MS-Flow-Control message:

```
bssgp-message ms-flow-control-from-unknown-ms send-ack
```
bssgp-message ptp-bvc-reset

This command determines the SGSN response, per BVCI, to receipt of a peer-to-peer BVC Reset.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > SGSN Global Configuration
configure > sgsn-global

Entering the above command sequence results in the following prompt:

[local]host_name(config-sgsn-global)#

Syntax

bssgp-message ptp-bvc-reset { frc-subscriber-standby | retain-current-state }

default bssgp-message ptp-bvc-reset

default
Including default with the command configures the SGSN to use default behavior so that the SGSN continues with the current state once a peer-to-peer BVC Reset is received.

frc-subscriber-standby
This keyword instructs the SGSN to change the state of the subscribers to standby when the peer-to-peer BVC Reset is received.

retain-current-state
Default
This keyword instructs the SGSN to continue the current state of the subscribers when the BVC Reset message is received.

Usage
This command allows the operator to specify the action the SGSN needs to take whenever the SGSN receives a peer-to-peer BVC Reset message for a specific BVCI.
To confirm the configuration for the response to the BVC Reset, use the show sgsn-mode command from the Exec mode.

Example
Change the default configuration and have the SGSN change subscriber states to standby:

bssgp-message ptp-bvc-reset frc-subscriber-standby
bssgp-timer

Configures the T2 and TH timers for the BVCs (BSSGP virtual connections) of the NSE (network service entities).

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > SGSN Global Configuration

```
configure > sgsn-global
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sgsn-global)#
```

**Syntax**

```
bssgp-timer { t2 \( T2\_time \) | th \( TH\_time \) }
default bssgp-timer { t2 | th }
```

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>default</strong></td>
<td>Resets the specified timers to default settings.</td>
</tr>
<tr>
<td><strong>t2 ( T2_time )</strong></td>
<td>Configures the BVC reset guard timer (at the BSSGP layer) in units of 1 second. ( T2_time ): Enter an integer from 1 to 120. Default is 30 seconds.</td>
</tr>
<tr>
<td><strong>th ( TH_time )</strong></td>
<td>Configures, at the BSSGP layer, the MS flow control parameter validity timeouts in units of 1 second. ( TH_time ): Enter an integer from 6 to 5999. Default is 500 seconds.</td>
</tr>
</tbody>
</table>

**Usage**

Use this command to configure timer timeout values for MS flow control and BVC reset timers that control BVCs for the NSEs.

**Example**

Set the TH timeout for 20 seconds:

```
bssgp-timer th 20
```
bvc-unblock

This command enables (disabled by default) or disables the SGSN to unblock blocked BVCs based on the receipt of uplink packets from the BSC.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > SGSN Global Configuration
configure > sgsn-global

Entering the above command sequence results in the following prompt:

[local]host_name(config-sgsn-global)#

Syntax

bvc-unblock { data-or-flow-control | flow-control | ul-data }

[ default | no ] bvc-unblock

default
Include default with the command to disable the function.

no
Include no with the command to disable this function.

data-or-flow-control
Enables the BVC-Unblock function when the SGSN receives either a FLOW-CONTROL-BVC packet or a UL-UNITDATA packet.

flow-control
Enables the BVC-Unblock function when the SGSN receives a FLOW-CONTROL-BVC packet.

ul-data
Enables the BVC-Unblock function when the SGSN receives a UL-UNITDATA packet.

Usage
Configurations defined with this command are common to all NSE defined for the SGSN. This command is useful if there is a BVC status mismatch across different SGSN managers (such as the sessmgr and the linkmgr) when the BSC sends BVC-Block (SGSN should move to BLOCKED) followed by a BVC-Reset (SGSN should move to UNBLOCKED). Such mismatches can easily occur, particularly on Gb-IP network connection, when one link receives the BVC-Block and a different link receives the BVC-Reset with little delay between the two.
bvc-unblock

If BVC-Unblock function is enabled, the SGSN ensures that BVCs which are in the BLOCKED state move to the UNBLOCKED state upon receipt of the configured packet type(s).

**Example**

Instruct the SGSN to perform BVC-Unblock when a mismatch occurs and the SGSN receives a FLOW-CONTROL-BVC packet:

```
bvc-unblock flow-control
```
dscp-template

Creates and/or deletes DSCP templates that can be configured for use for all GPRS services on the SGSN and provides access to the DSCP Template configuration mode. This command is also supported on HNB-GW service to create a DSCP template.

Product
SGSN
HNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > SGSN Global Configuration
    configure > sgsn-global

Entering the above command sequence results in the following prompt:

[local]host_name(config-sgsn-global)#

Syntax

```
dscp-template template_name [ -noconfirm ]
no dscp-template template_name
```

no
Deletes the template instance from the SGSN Global configuration.

```
template_name
```

Enter 1 to 64 alphanumeric characters, including dots (.), dashes (-), and forward slashes (/) to identify a unique instance of a DSCP template.
There is no known limit to the number of templates that can be created.

Usage

This command enables the operator to create or delete an instance of a DSCP template and access the DSCP Template configuration mode. The DSCP templates are used to define the DSCP configuration for control packets and data packets for the GPRS services.

Related commands:

- This command provides access to the mode containing all the configuration commands used to define DSCP markings for the control packets and data packets for a particular GPRS service (see the DSCP Template Configuration Mode Commands section).

- To associated a specific DSCP template with a specific GPRS service configuration, for builds prior to release 14.0 use the `associate-dscp-template downlink` command and for builds in releases 14.0 and higher use the `associate dscp-template downlink` command. Both commands are documented in the GPRS Service Configuration Mode Commands section.

- To check the list of DSCP templates configured, use the `show sgsn-mode` command documented in the Exec Mode Commands section.
This command is also supported on HNB-GW service to create a DSCP template.

**Related commands for HNB-GW:**

- This command provides access to the mode containing all the configuration commands used to define DSCP markings for the control packets and data packets for a particular HNB-GW service (see the *DSCP Template Configuration Mode Commands* chapter).

- To associate a specific DSCP template with a system for a PSP instance in SS7 routing domain, use the `associate-dscp-template downlink` documented in the *SGSN PSP Configuration Mode Commands* chapter.

**Example**

Use a command similar to the following to create a DSCP template with ID `dscp_london` that can be used specifically for Gb/IP calls from subscribers in London:

```
dscp-template dscp_london
```

Following command creates a DSCP template with ID `dscp_hnb1` that can be used specifically for HNB-GW services on a chassis:

```
dscp-template dscp_hnb1
```
dual-address-pdp

This command makes it possible for the operator to enable (default) / disable SGSN support for MS requests for dual PDP type (IPv4v6) addressing.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > SGSN Global Configuration

```
configure > sgsn-global
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sgsn-global)#
```

**Syntax**

```
[ default | no ] dual-address-pdp
```

- `default`
  Enables dual PDP type address support.

- `no`
  Disables the default behavior so that the SGSN does not honor requests for dual PDP type addresses.

**Usage**

With release 12.2 and in accordance with 3GPP Release 9.0 specifications, by default the SGSN honors the MS/UE request for dual PDP type addressing (IPv4v6) for PDP context association with one IPv4 address and one IPv6 address/prefix. This support can be disabled by configuration.

**Important:** For the dual PDP addressing feature to function, `common-flags` must be enabled with the `gptc send` command in the SGTP service configuration mode prior to enabling the feature with the `dual-address-pdp` command.

With this default behavior, the operator has multiple options to refine the level of support for dual PDP type addressing through the use of several related commands.

- `dual-address-pdp` command in the RNC configuration mode disables SGSN support for dual PDP type addressing for a specific RNC that either does or does not support this type of addressing.

- `pdp-type-ipv4v6-override` in the APN profile configuration mode allows the SGSN to override the MS/UE request for dual PDP type addressing.

- Using the `dual-ipv4v6` keyword with the `wildcard-apn pdp-type` command in the APN remap table configuration mode enables the operator to configure a default APN with a wildcard subscription with PDP type IPv4v6.

**Example**

With release 12.2 and in accordance with 3GPP Release 9.0 specifications, by default the SGSN honors the MS/UE request for dual PDP type addressing (IPv4v6) for PDP context association with one IPv4 address and one IPv6 address/prefix. This support can be disabled by configuration.

**Important:** For the dual PDP addressing feature to function, `common-flags` must be enabled with the `gptc send` command in the SGTP service configuration mode prior to enabling the feature with the `dual-address-pdp` command.

With this default behavior, the operator has multiple options to refine the level of support for dual PDP type addressing through the use of several related commands.

- `dual-address-pdp` command in the RNC configuration mode disables SGSN support for dual PDP type addressing for a specific RNC that either does or does not support this type of addressing.

- `pdp-type-ipv4v6-override` in the APN profile configuration mode allows the SGSN to override the MS/UE request for dual PDP type addressing.

- Using the `dual-ipv4v6` keyword with the `wildcard-apn pdp-type` command in the APN remap table configuration mode enables the operator to configure a default APN with a wildcard subscription with PDP type IPv4v6.
Use the following command to disable support for dual PDP type addressing (IPv4v6):

    no dual-address-pdp

If dual PDP addressing has been disabled, to re-enable the feature, move to the SGTP service configuration mode, in the appropriate context, to perform the following as the first command needed to re-enable support for dual PDP type addressing in the configuration:

    gtpc send common-flags

Now in the SGSN global configuration mode, use the following as the second command required to re-enable support for dual PDP type addressing in the configuration:

    dual-address-pdp
end

Exits the current mode and returns to the Exec Mode.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax

end

Usage
Change the mode back to the Exec Mode.
exit

Exits the current mode and returns to the previous configuration mode.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Change the mode to the Global Configuration Mode.
gmm-message

This command configures the SGSN to discard (drop) the Attach-Request message received with a random TLLI already in use.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > SGSN Global Configuration
configure > sgsn-global

Entering the above command sequence results in the following prompt:

[local]host_name(config-sgsn-global)#

Syntax

[ default ] gmm-message attach-with-tlli-in-use discard-message

default
Resets the default function allowing multiple MS, using the same random TLLI, to attempt to Attach simultaneously and disables discarding the Attach-Request message for random TLLI already in use.

Usage

Working with the two related commands (noted below), this command is part of a procedure for handling multiple MS Attaches all with the Same Random TLLI. Use this command to configure the SGSN to allow only one subscriber at a time to attach using a fixed random TLLI.

Related Commands:

- The old-tlli invalidate tlli command configures a list of random TLLI to be invalidated from the GMM after the invalidate old-TLLI timer expires.
- The old-tlli hold-time command configures the old-TLLI expiry timer.

Example

Configure the SGSN to drop Attach Request containing TLLI already in use:

\[ gmm-message attach-with-tlli-in-use discard-message \]
gmm-sm-statistics

**Important:** This command has been deprecated.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > SGSN Global Configuration

- configure > sgsn-global

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-sgsn-global)#
```

**Syntax**

```
gmm-sm-statistics attach-rejects cause network-failure only-internal

no gmm-sm-statistics attach-rejects
```
gprs-mocn

Enables or disables General Packet Radio Service (GPRS) Multi-Operator Core Network (MOCN). With 2G MOCN, the radio network is shared among different operators, while each operator maintains its separate core network.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > SGSN Global Configuration
configure > sgsn-global

Entering the above command sequence results in the following prompt:

[local]host_name(config-sgsn-global)#

Syntax

[ no ] gprs-mocn

no
Disables GPRS MOCN when it has been previously enabled.

Usage
Use this command to enable 2G MOCN, which is disabled by default.
For complete information about the 2G (GPRS) MOCN feature and its configuration, refer to the MOCN for 2G SGSN feature section in the Serving GPRS Support Node Administration Guide

Example
The following command enables GPRS MOCN support for SGSN:

gprs-mocn
**interface-management**

This command creates an interface management configuration and provides access to the SGSN Interface Management configuration mode.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > SGSN Global Configuration
`configure > ssgn-global`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ssgn-global)#
```

**Syntax**

```
interface-management
```

**Usage**

Use this command to access the SGSN Interface Management configuration mode to map NSE-ID and NSE-name to the Gb interface and/or to lock and unlock interface by the NSE/BSC identifier.

**Example**

Access the SGSN Interface Management configuration mode:

```
interface-management
```
**imsi-range**

Configure an IMSI range or a PLMN ID to associate with an Operator Policy.

**Product**

SGSN

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > SGSN Global Configuration

configure > sgsn-global

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sgsn-global)#
```

**Syntax**

```
imsi-range mcc mcc_num mnc mnc_num { msin first start_number last stop_number [ operator-policy policy_name [ description description ] ] | plmnid plmn_id operator-policy policy_name [ description description ] } +

no imsi-range mcc mcc_num mnc mnc_num { msin first start_number last stop_number | plmnid plmn_id }
```

Using **no** in the command deletes the definition from the SGSN Global configuration.

---

**mcc mcc_num**

`mcc` defines the mobile country code (MCC) of an IMSI.

`mcc_num`: Enter a 3-digit number from 100 to 999 - 000 to 099 are reserved.

---

**mnc mnc_num**

`mnc` defines the mobile network code (MNC) of an IMSI.

`mnc_num`: Enter a 2 or 3-digit number from 00 to 999.

---

**msin**

MSIN (mobile subscriber international number) portion of the IMSI.

`first start_number`: Defines first MSIN prefix number in a range

`last stop_number`: Defines the last or final MSIN prefix number in a range.

---

**operator-policy policy_name description description**

Identify the operator policy that the IMSI range definition and/or the PLMN-ID is to be associated.

`policy_name`: Enter a string of 1 to 64 alphanumeric characters.

`description`: Enter a string of 1 to 100 alphanumeric characters to provide range clarification for converted Release 9.0 configurations.

If a PLMN-ID is to be included in the definition, enter the **plmnid** before entering the operator policy name.
plmnid  plmn_id

The 5-6 digit PLMN-ID consists of the MCC (mobile country code) plus the MNC (mobile network code) to identify the public land mobile network (PLMN) for a specific operator. This keyword associates a specific PLMN with this specific SGSN operator policy.

plmn_id: Enter 5 to 6 digits.

+ This symbol indicates that command can be repeated to create repeated definitions.

Usage

An IMSI = maximum of 15 digits. An IMSI consists of the MCC (3 digits) + the MNC (2 or 3 digits) + the MSIN (the remaining 10 or 9 digits depending on the length of the MNC).

MCC and MNC are the minimum amount of information required to identify a unique operator policy with IMSI filtering. The MCC and MNC combine uniquely to identify the country and the network operator, for example: Cingular Wireless in the United States = mcc 311 mnc 180

To improve the granularity of call handling, an operator policy with additional IMSI filtering parameters can be defined, to include filtering based on the MSIN, by defining a MSIN range - first (or start-of-range) MSIN and last (or end-of-range) MSIN. The range numbers do not include the maximum allowed for the MSIN but should include a sufficient number to enable the operator policy to filter effectively.

For the most efficient IMSI filter, the operator policy should include all of the above parameters and the PLMN ID which defines the current location of the MS -- this parameter is particularly useful for highlighting which calls are roaming.

And if none of the operator policies contain useful filtering information, then the default operator policy will be applied as the information in this command is never defined for the default operator policy.

The following table will illustrate how these filtering parameters determine which operator policy will govern a call:

<table>
<thead>
<tr>
<th>Operator Policy ID</th>
<th>MCC</th>
<th>MNC</th>
<th>MSINfirst</th>
<th>MSINlast</th>
<th>PLMN ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>OpPol-1</td>
<td>123</td>
<td>45</td>
<td>67890</td>
<td>67898</td>
<td></td>
</tr>
<tr>
<td>OpPol-2</td>
<td>123</td>
<td>45</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OpPol-3</td>
<td>123</td>
<td>45</td>
<td>67890</td>
<td>67898</td>
<td>23232</td>
</tr>
<tr>
<td>OpPol-4</td>
<td>123</td>
<td>45</td>
<td></td>
<td></td>
<td>23232</td>
</tr>
<tr>
<td>OpPol-5</td>
<td>123</td>
<td>45</td>
<td>6789012</td>
<td>6789019</td>
<td></td>
</tr>
<tr>
<td>OpPol-6</td>
<td>123</td>
<td>45</td>
<td>6789012</td>
<td>6789019</td>
<td>23232</td>
</tr>
<tr>
<td>default</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The filtering selects which operator policy will be used to determine how a call is handled - the operator policy that best matches the IMSI. So, a call with IMSI 123456789012345 PLMNID 23232 is best matched with OpPol-6.

In most cases, the operator policy with the most information defined will be used as a combination of PLMNID and IMSI provides the best match. But OpPol-6 won’t always be the best match. Using the table above:

OpPol-1 is the best match for IMSI 123456789011111
OpPol-2 is the best match for IMSI 123456789099999
OpPol-5 is the best match for IMSI 123456789012345 if the PLMNID is 12344
Example

The following associates operator policy `oppol1` with country code 310, mobile network code of 33, and IMSI range 1231234 - 1231244:

```
imsi-range mcc 310 mnc 33 msin first 1231234 last 1231244 operator-policy oppol1
```
location-services

Enable or ‘start’ Location Services (LCS) on the SGSN.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > SGSN Global Configuration

```
configure > sgsn-global
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-sgsn-global)#
```

**Syntax**

```
location-services

no location-services
```

---

**Usage**

By default, Location Services is not enabled on the SGSN. This command is mandatory to enable the SGSN to support LCS, which is a license-controlled feature. Multiple other commands are required to configure LCS functionality. For more information about the operation and configuration of LCS on the SGSN, refer to the *Location Services* section of the *SGSN Administration Guide*.

**Example**

Use the following command to disable Location Services once they have been enabled:

```
no location-services
```
**map-message**

This command instructs the SGSN to ignore the CAMEL subscription when there is no CAMEL service associated or in existence.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > SGSN Global Configuration

```
configure > sgsn-global
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sgsn-global)#
```

**Syntax**

```
map-message insert-subscriber-data csi-handling when-camel-not-associated ignore-subscription
```

```
default map-message insert-subscriber-data csi-handling
```

**Example**

Instruct the SGSN to validate the CAMEL subscription:

```
default map-message insert-subscriber-data csi-handling
```
max-pending-attaches

Configure the maximum length of the pending attach queue.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > SGSN Global Configuration
configure > sgsn-global
Entering the above command sequence results in the following prompt:

[local]host_name(config-sgsn-global)#

Syntax

max-pending-attaches limit

default max-pending-attaches

default
Resets the SGSN’s Attach queue to a maximum pending value of 10,000.

limit
Set the a maximum limit to the pending Attach/RAU messages queue in the LinkMgr. When the limit is reached a message is sent to the IMSIMgr.

limit: Enter an integer from 5000 - 50000. Default is 10000.

Usage

With this command, configure the maximum limit to the pending ATTACH/RAU messages queue in the LinkMgr. When the limit is reached, the LinkMgr sends the Query/Forward messages to the IMSIMgr. As the IMSIMgr gets busier and does not responded to Query/Forward requests, the response to the requests will get slower and slower and the queue size continues inflating if the incoming message rate is high. To avoid this situation, set the max-pending-attaches for the pending queue for Attach and RAU messages. All other messages from the HLR will be added to the queue as they cannot be dropped. High and low watermarks are set to the queue at 80% of max-pending-attaches ” and 60% of max-pending-attaches respectively.

Once a high watermark is reached, the new Attach and RAU requests are dropped and relevant statistics are incremented. Once a low watermark is hit, the new Attach/RAU requests are accepted and added to the pending queue. The entries are added to the pending queue only when the window-size between IMSIMgr and LinkMgr becomes zero. This is a very rare occurrence and will not affect the current behavior in normal circumstances.

Example

Set the queue length to a maximum of 15000 requests:

max-pending-attaches 15000
old-tlli invalidate tlli

This command configures a list of random TLLI to be invalidated (removed) from the GMM after the invalidate old-TLLI timer expires.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > SGSN Global Configuration
configure > sgsn-global

Entering the above command sequence results in the following prompt:

[local]host_name(config-sgsn-global)#

**Syntax**

```
[ no ] old-tlli invalidate tlli < hexadecim al >
```

- **no**
  Removes a single random TLLI from the configured list.

- **< hexadecimal >**
  Identifies a single random TLLI to be removed from the GMM after the old-TLLI timer expires.

**Usage**

Use this command to create a list of up to 50 random TLLI to be dropped from the GMM after the old-TLLI timer expires. This command also starts the invalidate old-TLLI timer.

**Important:** If the old-TLLI expiry timer is not configured with the `old-tlli hold-time` command, then the SGSN will only drop second Attach Requests using the same random TLLI already in use.

**Related Commands:**
- The `gmm-message` command configures the SGSN to discard (drop) the Attach-Request message received with a random TLLI already in use
- The `old-tlli hold-time` command configures the old-TLLI expiry timer.

**Example**

Add random TLLI `0x7f05a30a` to the Invalidate List:

```
old-tlli invalidate tlli 0x7f05a30a
```
old-tlli hold-time

This command configures the old-TLLI expiry timer to be started in GMM when anyone of the listed random TLLI are received.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > SGSN Global Configuration
configure > sgsn-global

Entering the above command sequence results in the following prompt:

[local] host_name(config-sgsn-global) #

Syntax

[ default ] old-tlli hold-time < seconds >

<table>
<thead>
<tr>
<th>default</th>
<th>Resets the timer to 5 seconds</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt; seconds &gt;</td>
<td>Sets the numbers of seconds before the timer expires; range 1 to 125.</td>
</tr>
</tbody>
</table>

Usage
Use this command to configure the old-TLLI expiry timer to be started in GMM when anyone of the listed random TLLI are received. If the timer expires prior to receiving Attach-Complete then the SGSN invalidates (removes) the TLLI from the GMM.

Important: For this configuration to work, the list of random TLLI to be removed (invalidated) from the GMM must be defined with the old-tlli invalidate tlli command.

Related Commands:
- The gmm-message configures the SGSN to discard (drop) the Attach-Request message received with a random TLLI already in use
- The old-tlli invalidate tlli command configures the random invalidate TLLI list.

Example
Set the timer for 2 seconds:

old-tlli hold-time 2
pdp-deactivation-rate

Set the rate the SGSN deactivates PDP connections per second per SessMgr when GTP-C path failure is detected. Beginning with release 15.0, this command is also supported on the S4-SGSN.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > SGSN Global Configuration
configure > sgsn-global
Entering the above command sequence results in the following prompt:

[local]host_name(config-sgsn-global)#

Syntax

pdp-deactivation-rate { connected-ready rate | idle-standby rate }

default pdp-deactivation-rate { connected-ready | idle-standby }

default

If this keyword is used with the command, then the default deactivation rates are used.

connected-ready rate

Subscribers that are in the PMM-Connected / GPRS-Ready state and actively using the SGSN service need to be deactivated at a faster rate to facilitate the deactivation/re-activation process.
rate - sets the number of subscribers to be deactivated per second per SessMgr and the valid range is 1 to 1000 and the default is 760 connected-ready subscribers deactivated per second.

idle-standby rate

Subscribers that are in the PMM-Idle / GPRS-Standby state are not actively using the SGSN service and can be deactivated at a slower rate. The deactivation process for idle-standby subscribers includes paging before the Deactivate Request is sent.
rate - sets the number of subscribers to be deactivated per second per SessMgr and the valid range is 1 to 1000 and the default is 240 idle-standby subscribers deactivated per second.

Usage

Use this command to define a rate at which the SGSN processes PDP deactivations when a GTP-C path failure is detected (and confirmed according to the SGSN's default behavior). The operator can use this command to set a deactivation rate that ensures radio network congestion is avoided.

Related commands:
* max-remote-restart-counter-change - allows the operator to set a maximum variance between stored and received values for restart counter changes coming from the GGSN. For details, refer to the SGSN Global configuration mode documentation.
**disable-remote-restart-counter-verification** - allows the operator to disable the default behavior. For details, refer to this command in the SGSN Global configuration mode documentation.

**Example**

Use the following command to deactivate PDP connections for **600** PMM-Connected / GPRS-Ready subscribers per second:

```
pdp-deactivation-rate connected-ready 600
```

Use the following command to deactivate PDP connections for **320** PMM-Idle / GPRS-Standby subscribers per second:

```
pdp-deactivation-rate idle-standby 320
```

Use the following command to reset the default **760** per second deactivation rate for PMM-Connected / GPRS-Ready subscribers:

```
default pdp-deactivation-rate connected-ready
```
**ranap excess-len ignore**

Configure the SGSN to ignore excess length of received RANAP messages.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > SGSN Global Configuration
   configure > sgsn-global

Entering the above command sequence results in the following prompt:

[local]host_name(config-sgsn-global)#

**Syntax**

```
[ default | no ] ranap excess-len ignore
```

- **default**
  Resets the default behavior - a decode error is generated when received RANAP messages are more than an extra octet in length.

- **no**
  Disables the configuration to ignore overly long RANAP messages.

**Usage**

By default, the SGSN issues a decode error when the RANAP messages include extra octets. Use this command to ignore RANAP messages that have extra octets.

**Example**

Use the following command to enable the SGSN to ignore overly long RANAP messages:

```
ranap excess-len ignore
```

Use the following command to disable ignoring of RANAP messages that are excessive in length:

```
no ranap excess-len ignore
```
ran-information-management

Enable/disable RAN information management (RIM) support for the SGSN.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > SGSN Global Configuration

```configure > sgsn-global```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sgsn-global)#
```

**Syntax**

```
[ default | no ] ran-information-management
```

- **default**
  
  Resets the default so RIM is disabled.

- **no**
  
  Disables the RIM support in the configuration file.

**Usage**

By default, handling of RAN information management (RIM) messages is disabled. This command enables the SGSN to handle RIM messages. When this command is enabled and RIM message handling is enabled on the destination node, then RIM PDUs will be forwarded to the BSC/RNC. If RIM message handling is not enabled on both nodes, then the RIM PDUs will be dropped silently.

Confirm RIM configuration with the `show sgsn-mode` command in the Exec mode.

**Example**

Use the following command to enable RIM support:

```
ran-information-management
```

Use the following command to disable RIM support that has been added to the configuration:

```
no ran-information-management
```
target-offloading

Selects the subscriber offloading algorithm to be applied to the SessMgr and the IMSIMgr.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > SGSN Global Configuration
configure > sgsn-global

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sgsn-global)##
```

**Syntax**

```
target-offloading algorithm [ optimized-for-speed | optimized-for-target-count ]
```

**default target-offloading algorithm**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Resets the configuration to default values.</td>
</tr>
<tr>
<td>optimized-for-speed</td>
<td>Enables faster algorithm to achieve the target count.</td>
</tr>
<tr>
<td>optimized-for-target-count</td>
<td>Enables a reliable algorithm to achieve the target count. Default.</td>
</tr>
</tbody>
</table>

**Usage**

With the SGSN’s distributed architecture, there are many SessMgrs and offloading will happen in parallel at all SessMgrs. This command enables the operator to control the total number of subscribers being offloaded.

**Important:** The value for this command can not be altered once dynamic offloading has begun - refer to the command description for the `sgsn-offload` command in the *Exec Mode* chapter.

**Example**

Set the SGSN to use the faster algorithm for offloading:

```
target-offloading algorithm optimized-for-speed
```
**tlli-cb-audit**

This command enable (default is disabled) or disables a periodic (hourly) audit of TLLI-CBs in the BSSGP layer.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > SGSN Global Configuration
configure > sgsn-global
Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sgsn-global)#
```

**Syntax**

```
tlli-cb-audit
[ default | no ] tlli-cb-audit
```

- **default**
  Include **default** with the command to disable the audit function.

- **no**
  Include **no** with the command to disable the audit function.

**Usage**

This command is used to clean-up hanging or unassociated TLLI in the BSSGP layer. This configuration defined with this command will be common to all NSE configured for this SGSN.

Independent of this command configuration, the SGSN triggers and audit when the number of TLLI-CBs reaches 35,000.

**Example**

Use the following command to enable the hourly audit for unassociated TLLI-CBs:

```
tlli-cb-audit
```
umts-aka-r99

This command enables the operator to authenticate mobile equipment (MEs) with R99+ USIMs and capable of UMTS AKA.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > SGSN Global Configuration
configure > sgsn-global

Entering the above command sequence results in the following prompt:

[local]host_name(config-sgsn-global)#

Syntax

umts-aka-r99

no umts-aka-r99

 Including no with the command disables the authentication.

Usage

This command enables operators to authenticate MEs that are attempting to connect to a 2.5G network with R99+ USIMs if the MEs are UMTS AKA capable. For R99 mobiles, the SGSN will continue to perform GSM AKA even if quintuplets are received from the HLR.

Example

Use the following command to disable UMTS AKA authentication for MEs with R99+ USIMs:

no umts-aka-r99
Chapter 281
SGSN Interface Management Configuration Mode

The interface management commands, accessed via the SGSN Global configuration mode, are applicable to the SGSN on a global level. They map the NSC/BSC to the SGSN’s Gb interface and enable the operator to quickly configure lock or unlock for the BSC interface on the basis of the NSE’s ID or name.

Mode

Exec > Global Configuration > SGSN Global Configuration > Interface Management Configuration

configure > sgsn-global > interface-management

Entering the above command sequence results in the following prompt:

[local]host_name(config-sgsn-interface-mgmt)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
end

Exits the current configuration mode and returns to the Exec mode.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Return to the Exec mode.
exit

Exits the current configuration mode and returns to the SGSN Global configuration mode.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Returns to the SGSN Global configuration mode.
interface

Maps the Gb interface to an NSE-ID and an NSE-name to facilitate the identification of the peer NSE/BSC.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > SGSN Global Configuration > Interface Management Configuration

Syntax
interface gb peer-nsei id { name <value> | id <value> }

no interface gb peer-nsei id { name <value> | id <value> }

Usage
This command configures mapping between an NSE-ID and an NSE name and the SGSN’s Gb interface. The mapping allows the operator to use the lock-interface command (also in this mode) to more easily configure locking or unlocking of the interface to the BSC by identifying the network service entity by ID or by name.

Related Commands:
lock-interface

Example
Map NSE with ID of 422 and the name Dover to the Gb interface:

interface gb peer-nsei id 422 name Dover

The following example disables the mapping for NSEI 2321:

no interface gb peer-nsei id 2321
lock-interface

This command enables the operator to configure the SGSN’s Gb interface, toward the peer NSE/BSC, as locked or unlocked on the basis of the NSE’s name or identifier.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > SGSN Global Configuration > Interface Management Configuration
configure > sgsn-global > interface-management

Entering the above command sequence results in the following prompt:

[local]host_name(config-sgsn-interface-mgmt)#

Syntax

[ no ] lock-interface gb peer-nsei { id nsei-id | name nsei_name }

<table>
<thead>
<tr>
<th>no</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disables a previously configured lock on the interface to the NSE/BSC.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>peer-nsei id nsei_id</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the numeric identifier of the network service entity mapped to the Gb interface.</td>
</tr>
<tr>
<td>nsei_id - Enter an integer from 0 to 65535.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>peer-nsei nsei_name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the name of the NSE associated with the BSC, which is stored in the SCT.</td>
</tr>
<tr>
<td>nsei_id - Enter an alphanumeric string of 1 to 64 characters.</td>
</tr>
</tbody>
</table>

Usage
This command allows the operator to lock/unlock the interface, towards the NSE/BSC, based on the NSE name or NSE identifier.
Lock is configured primarily to avoid the high CPU usage the SGSN can experience when BSCs attempt to reconnect after an SGSN reboot or reload. The lock stops the auto-learn procedure for the locked BSC connected via Gb over IP.
The auto-learn facility can be enabled in a staggered manner for each BSC after reboot/reload by unlocking the BSCs one-by-one.
The NSE unlock state is the default state and the NSE can accept or send any uplink and downlink data.

Related Commands:
interface

Example
Lockout NSE/BSC ID 319 from the SGSN:

lock-interface gb peer-nsei id 319
Chapter 282
SGSN Pool Area Configuration Mode Commands

The Pool Area configuration mode configures the parameters used to setup the VLRs to use with a pool area in a Gs service.

Mode

Exec > Global Configuration > Context Configuration > Gs Service Configuration > Pool Area Configuration

configure > context context_name > gs-service service_name > pool-area pool_area_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-gs-pool-area)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
end

Exits the current configuration mode and returns to the Exec mode.

Product
SGSN

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Return to the Exec mode.
exit

Exits the current configuration mode and returns to the previous configuration mode.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**
exit

**Usage**
Return to the previous configuration mode.
hash-value

This command configures the load distribution for the VLRs that service this pool area.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Gs Service Configuration > Pool Area Configuration

configure > context context_name > gs-service service_name > pool-area pool_area_name

Entering the above command sequence results in the following prompt:

}\[context_name]host_name(config-gs-pool-area)#

Syntax

`hash-value { hash_value | non-configured-values | range start_value to end_value } use-vlr vl_r_name`

`no hash-value { hash_value | non-configured-values | range start_value to end_value }`

**no**
Removes the configured Gs procedures from this Gs service.

**hash_value**
Specifies the specific hash value for VLR(s).

*hash_value* must be an integer value from 0 through 999.

**range start_value to end_value**
Specifies the range of hash values for a VLR.

*start_value* specifies the start value for range of hash and is an integer value from 0 through 999.

*start_value* must be lower than *end_value*.

*end_value* specifies the end value for range of hash and is an integer value from 0 through 999. *end_value* must be higher than *start_value*.

**non-configured-values**
This keyword assign all non-configured hash values to use the named VLR.

**use-vlr vl_r_name**
Specifies the name of the VLR to be associated with this pool area.

*vl_r_name* is the name of VLR and must be an alpha and/or numeric string of 1 to 63 characters.
Usage

Use this command to configure the load distribution for the VLRs that service this pool area as defined in TS 23.236.

The algorithm for selection of VLR from a pool area is based on the hash value computed on the IMSI digits. The SGSN derives a hash value (V) using procedure as defined in TS 23.236. Every hash value from the range 0 to 999 corresponds to a single MSC/VLR node. Typically many hash values may point to the same MSC/VLR node.

This command can be entered multiple times for different hash value.

Example

Following command configure the all non configured hash values to use VLR named `starvlr1` in this pool area:

```
hash-value non-configured-values use-vlr starvlr1
```
lac

This command defines a set of location area code (LAC) values for a pool area.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Gs Service Configuration > Pool Area Configuration
configure > context context_name > gs-service service_name > pool-area pool_area_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-gs-pool-area)#
```

**Syntax**

```
lac lac_id +

no lac lac_id
```

- `lac` Removes the configured LAC value from this pool area configuration.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>lac</td>
<td>Specifies the subscribers’ location area code (LAC) to be associated with this pool area and a specific VLR. This LAC is obtained from the radio area identity (RAI). <code>lac_id</code>: Must be an integer from 1 through 65535.</td>
</tr>
<tr>
<td>+</td>
<td>More than one <code>lac_id</code>, separated by a space, can be entered within a single command.</td>
</tr>
</tbody>
</table>

**Usage**

Use this command to specify a set of LACs to use for a pool area. This command can be entered multiple times, subject to a limit of 32 LAC definitions (total for non-pool-area and pool-area configuration) per Gs service.

**Important:** LAC values across multiple pool areas and non-pool-areas must be unique within the Gs service.

**Example**

The following command configures LACs 101, 301, and 222 for the pool area.

```
lac 101 301 222
```
Chapter 283
SGSN PSP Configuration Mode Commands

The Peer-Server Process (PSP) configuration mode provides the commands to create, configure, bind, and manage a specific PSP instance included in an SS7 routing domain configuration.

Mode
Exec > Global Configuration > SS7 Routing Domain Configuration > Peer-Server Configuration > PSP Configuration

configure > ss7-routing-domain routing_domain_id variant variant_type > peer-server id id > psp instance psp_instance

Entering the above command sequence results in the following prompt:

[local] host_name(config-ss7-rd-ss7rd_id-ps-peer-server_id-psp-psp_instance)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
**associate**

Defines an association between the PSP instance and an application server process (ASP) instance and/or a DSCP marking template.

**Product**

SGSN

HNB-GW

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > SS7 Routing Domain Configuration > Peer-Server Configuration > PSP Configuration

```configure > ss7-routing-domain routing_domain_id variant variant_type > peer-server id id > psp instance psp_instance```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ss7-rd-ss7rd_id-ps-peer-server_id-psp-psp_instance)#
```

**Syntax**

```
associate { asp instance asp_num | dscp-template downlink template_name }
```

```
no associate [ asp | dscp-template downlink ]
```

**Important:** Using the `no associate` command will most likely result in the termination of all current subscriber sessions active through the peer-server.

**asp instance asp_num**

Identifies a specific ASP configuration. Up to four ASP instances can be configured for a single SS7 routing domain.

`asp_num` is a digit from 1 to 4.

**dscp-marking downlink template_name**

Identifies a specific DSCP marking template to associate with this PSP configuration.

`template_name` is a string of 1 to 64 characters, including letters, digits, dots (.), dashes (-), and forward slashes (/), to identify a unique instance of a DSCP template. For more information about DSCP marking templates, refer to the `DSCP Template Configuration Commands Mode` chapter.

The DSCP marking template provides a mechanism enabling the SGSN to perform differentiated services code point (DSCP) marking of control packets and signaling messages at the SGSN’s M3UA level on the Gb interface. This DSCP marking feature enables the SGSN to perform classifying and managing of network traffic and to determine quality of service (QoS) for the interfaces to an IP network.

While enabling DSCP marking of SCTP (control packets) on HNB-GW only `associate dscp-template downlink template_name` command is applicable. This command is used to provides a mechanism
enabling the HNB-GW to perform differentiated services code point (DSCP) marking of control packets and signaling messages at the HNB-GW. This DSCP marking feature enables the HNB-GW to perform classifying and managing of network traffic and to determine quality of service (QoS) for the interfaces to an IP network.

Usage

Use this command to create an association between a specific peer-server process (PSP) and a specific application server process (ASP) instance or a specific differentiated services code point (DSCP marking template).

Before using the `associate` command, the values for the `psp-mode` and `end-point` commands must be configured.

Before using the `associate` command, the M3UA end-point of the ASP must be configured. Use the commands defined in the ASP Configuration Mode chapter of the Command Line Interface Reference.

While enabling DSCP marking of SCTP (control packets) on HNB-GW only associated dscp-template downlink template_name command is applicable. For more information about DSCP marking templates, refer to the DSCP Template Configuration Commands Mode chapter.

Example

Associate this PSP instance with ASP configuration instance 2:

```
associate asp instance 2
```

Use the following command to terminate all associations with this PSP instance:

```
no associate
```

Associate this PSP instance with a DSCP marking template identified as `dscptemp1`:

```
associate dscp-template downlink dscptemp1
```
end

Exits the configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
end

**Usage**
Change the mode back to the Exec mode.
end-point

This command defines or deletes the IP address to be associated with the local SCTP end-point for the application server process (ASP).

**Product**

SGSN
HNB-GW

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > SS7 Routing Domain Configuration > Peer-Server Configuration > PSP Configuration

configure > ss7-routing-domain routing_domain_id variant variant_type > peer-server id id > psp instance psp_instance

Entering the above command sequence results in the following prompt:

[local]host_name(config-ss7-rd-ss7rd_id-ps-peer-server_id-psp-psp_instance)#

**Syntax**

```
end-point { address ip_address | port port_number }
no end-point [ address ip_address ]
```

- **no**
  - Removes the ASP end-point association configuration from the PSP configuration.

**Important:** This command can not be used as long as the PSP and the ASP are associated. Use the no associate command when entering any form of this command, including no end-point. When the change is made, re-enter the ASP association with the association command.

```
port port_number
```

- Configures the M3UA’s SCTP port number for the end-point.
- **port_number:** Must be an integer from 1 to 65535.
- Default: 2905.

**Usage**

Use this command to manage the ASP end-point. At least one address needs to be configured for the ASP before the end-point can be associated with the PSP.

**Example**

Set the ASP end-point to IP address 192.168.1.1 with the following command:

```
end-point address 192.168.1.1
```
exchange-mode

Configures the exchange-mode for the PSP communication.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > SS7 Routing Domain Configuration > Peer-Server Configuration > PSP Configuration
configure > ss7-routing-domain routing_domain_id variant variant_type > peer-server id id
> psp instance psp_instance

Entering the above command sequence results in the following prompt:
[local]host_name(config-ss7-rd-ss7rd_id-ps-peer-server_id-psp-psp_instance)#

Syntax
exchange-mode [ double-ended | single-ended ]

Usage

**Important:** Before using this command to set a value or reset the default, you must disassociate the PSP instance with the `no associate` command. When you have modified your configuration with this command, then use the `associate` command to setup a new ASP association.

Use this command to toggle the exchange modes for the PSP to match the exchange mode supported by the ASP. The exchange mode specifies what type of ASP messages exchange is used in an IPSP communication. The `exchange-mode` must be configured for 'single-ended' if the `psp-mode` has been configured for 'client'.

Example
Change the exchange mode from the standard double-ended to single-ended:

```
exchage-mode single-ended
```
exit

Exits the current configuration mode and moves to the previous configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

exit

Usage
Return to the Peer-Service configuration mode.
psp-mode

Configures either client-mode or server-mode as the PSP’s operational mode.

Product
SGSN
HNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > SS7 Routing Domain Configuration > Peer-Server Configuration > PSP Configuration
configure > ss7-routing-domain routing_domain_id variant variant_type > peer-server id id > psp instance psp_instance

Entering the above command sequence results in the following prompt:

[local]host_name(config-ss7-rd-ss7rd_id-ps-peer-server_id-psp-psp_instance)#

Syntax

psp-mode { client | server }

client
The PSP operates as a client.

server
The PSP operates as a server.

Usage

Important: Before using this command to change the configuration, you must disassociate the PSP instance with the no associate command. When you have modified your configuration with this command, then use the associate command to setup a new ASP association.

Example

Instruct the peer-server process to operate in either client or server mode.

Configure the PSP to operate in server mode:

```bash
psp-mode server
```
routing-context

Configures the behavior of the routing context in M3UA messages.

**Important:** This keyword function is only available in releases 8.1 and higher.

**Product**
- SGSN
- HNB-GW

**Privilege**
- Security Administrator, Administrator

**Mode**

Exec > Global Configuration > SS7 Routing Domain Configuration > Peer-Server Configuration > PSP Configuration

```
configure > ss7-routing-domain routing_domain_id variant variant_type > peer-server id id > psp instance psp_instance
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ss7-rd-ss7rd_id-ps-peer-server_id-psp-psp_instance)#
```

**Syntax**

```
routing-context { discard-inbound | process-inbound | m3ua-data { insert-outbound | suppress-outbound } }
```

**default routing-context**

```
  default
  Include this keyword with the command, to reset the configuration to the system default for routing-context which is a combination of process-inbound and insert-outbound.
```

```
discard-inbound
Sets the routing context received in M3UA messages to be discarded.
```

```
process-inbound
Sets the routing context received in M3UA messages to be processed.
```

```
m3ua-data
This keyword controls the insertion of routing context in outbound M3UA data messages. The default behavior is to insert routing context in management messages and suppress routing context in data messages.
```

```
insert-outbound
Sets the routing context so that it is added in the M3UA messages.
```

```
suppress-outbound
Sets the routing context so that it is suppressed in the M3UA messages.
```
Usage

**Important:** Before using this command to change the configuration or reset the default, you must disassociate the PSP instance with the `no associate` command. When you have modified your configuration with this command, then use the `associate` command to setup a new ASP association.

In PSP (singled-ended) configuration mode, the settings for both the local routing context (the SGSN’s routing context) and the peer routing context (the RNC’s routing context) should be the same. If the routing contexts created at the SGSN and on the peer are different then this can cause the M3UA link to fail. Routing context is an optional parameter when an M3UA association has only one associated peer-server.

Example

If the peer does not support routing context, then disable the routing context feature:

```
routing-context discard-inbound suppress-outbound
```
sctp-alpha

This stream control transmission protocol (SCTP) retransmission time out (RTO) parameter defines the RTO-Alpha value.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > SS7 Routing Domain Configuration > Peer-Server Configuration > PSP Configuration

configure > ss7-routing-domain routing_domain_id variant variant_type > peer-server_id id > psp_instance psp_instance

Entering the above command sequence results in the following prompt:

[local]host_name(config-ss7-rd-ss7rd_id-ps-peer-server_id-psp-psp_instance)#

Syntax

sctp-alpha value

default sctp-alpha

value

Defines a percentage (%) that represents the RTO portion of the round-trip time (RTT) calculation. This percentage value must be an integer between 0 and 65535.

default

 Resets the sctp-alpha to the default value of 5%.

Usage

sctp-alpha is used in conjunction with other commands, such as the sctp-beta command, to determine the round-trip time (RTT) calculations. The Alpha parameter is used to manage load balancing within the SS7 environment for multi-homed peers.

Important: Before using this command to set a value or reset the default, you must disassociate the PSP instance with the no associate command. When you have modified your configuration with this command, then use the associate command to setup a new ASP association.

Example

Set the SCTP RTO-Alpha value to 256% of the RTT calculation:

sctp-alpha 256
sctp-beta

This stream control transmission protocol (SCTP) retransmission time out (RTO) parameter defines the RTO-Beta value.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > SS7 Routing Domain Configuration > Peer-Server Configuration > PSP Configuration

configure > ss7-routing-domain routing_domain_id variant variant_type > peer-server id id
> psp instance psp_instance

Entering the above command sequence results in the following prompt:

[local]host_name(config-ss7-rd-ss7rd_id-ps-peer-server_id-psp-psp_instance)#

Syntax

sctp-beta value

default sctp-beta

value

Defines a percentage (%) that represents the RTO portion of the round-trip time (RTT) calculation. This percentage value must be an integer between 0 and 65535.

default

Resets the sctp-beta to the default value of 10%.

Usage

Use this command in conjunction with other commands, such as the sctp-alpha command, to determine the round-trip time (RTT) calculations. The Beta parameter is used to manage load balancing within the SS7 environment for multi-homed peers.

Important: Before using this command to set a value, you must disassociate the PSP instance with the no associate command. When you have set the value with this command, then use the associate command to setup a new association.

Example

Set the SCTP RTO-Alpha value to 512% of the RTT calculation:

sctp-beta 512
**sctp-checksum-type**

This command selects the type of checksum algorithm to be used.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > SS7 Routing Domain Configuration > Peer-Server Configuration > PSP Configuration

```
configure > ss7-routing-domain routing_domain_id variant variant_type > peer-server id id
> psp instance psp_instance
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ss7-rd-ss7rd_id-ps-peer-server_id-psp-psp_instance)#
```

**Syntax**

```
sctp-checksum-type { adler32 | crc32 }
```

**default sctp-checksum-type**

- **adler32**
  Selects the Adler-32 type of algorithm as a faster checksum function.

- **crc32**
  Selects the CRC-32, a slower but more reliable 32-bit cyclic redundancy check.

- **default**
  Resets the `sctp-checksum-type` to the default of CRC-32.

**Usage**
Use this command to set which type of checksum algorithm the SGSN is to use to validate SCTP packets.

**Important:** Before using this command to set a value, you must disassociate the PSP instance with the `no associate` command. When you have set the value with this command, then use the `associate` command to setup a new association.

**Example**

Set the checksum type for CRC32:

```
sctp-checksum-type crc32
```
sctp-cookie-life

This command sets the SCTP valid cookie life.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > SS7 Routing Domain Configuration > Peer-Server Configuration > PSP Configuration

```
configure > ss7-routing-domain routing_domain_id variant variant_type > peer-server id id > psp instance psp_instance
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ss7-rd-ss7rd_id-ps-peer-server_id-psp-psp_instance)#
```

**Syntax**

```
sctp-cookie-life value
```

**default sctp-cookie-life**

```
value
```

Sets the valid cookie life value in increments of 100 milliseconds. The range is 50 to 1200.

```
default
```

Resets the sctp-cookie-life value to the default, 600 (= .6 seconds).

**Usage**

Use this command to set the SCTP cookie life.

**Important:** Before using this command to set a value, you must disassociate the PSP instance with the no associate command. When you have set the value with this command, then use the associate command to setup a new association.

**Example**

Set the SCTP cookie life to 1 second (1000 milliseconds):

```
sctp-cookie-life 1000
```
**sctp-init-rwnd**

This command sets the size of the SCTP receiver window.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > SS7 Routing Domain Configuration > Peer-Server Configuration > PSP Configuration

```
configure > ss7-routing-domain routing_domain_id variant variant_type > peer-server id id > psp instance psp_instance
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ss7-rd-ss7rd_id-ps-peer-server_id-psp-psp_instance)#
```

**Syntax**

```
sctp-init-rwnd window_size
```

**default sctp-init-rwnd**

```
window_size
```

Sets an integer to configure the window size. The range is 32768 to 1048576.

```
default
```

 Resets the **sctp-init-rwnd** window size to the default, 1048576.

**Usage**

Use this command to set the receiver window size in the configuration. Configuring this parameter enables the SCTP client to send configured ‘sctp-init_rwnd’ as a_rwnd parameter in the INIT message. For the SCTP server, the INIT ACK will be populated with sctp-init_rwnd as a_rwnd parameter per RFC 4960. The command enables the operator to configure a reduced priority for LinkManager Control messages, thereby giving Timer messages the highest priority. The Timer messages are retained at the highest priority and Data messages are kept at a lower priority.

**Important:** Before using this command to set a value, you must disassociate the PSP instance with the `no associate` command. When you have set the value with this command, then use the `associate` command to setup a new association.

**Example**

Use the following command to set the SCTP window size to **32768**:

```
sctp-init-rwnd 32768
```
**sctp-max-assoc-retx**

This command sets the maximum number of datagram retransmissions to be associated with this peer server configuration.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > SS7 Routing Domain Configuration > Peer-Server Configuration > PSP Configuration

```
configure > ss7-routing-domain routing_domain_id variant variant_type > peer-server id id > psp instance psp_instance
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ss7-rd-ss7rd_id-ps-peer-server_id-psp-psp_instance)#
```

**Syntax**

```
sctp-max-assoc-retx value

default sctp-max-assoc-retx
```

**value**

Defines the maximum number of datagram retransmissions for an association. The value must be an integer between 0 and 255.

**default**

Resets the default for `sctp-max-assoc-retx` to 10.

**Usage**

Use this command to configure the maximum number of datagram retransmissions for an association. The endpoint will be declared unreachable after `sctp-max-assoc-retx` number of consecutive retransmissions to an endpoint on any transport address.

**Important:** Before using this command to set a value, you must disassociate the PSP instance with the `no associate` command. When you have set the value with this command, then use the `associate` command to setup a new association.

**Example**

Set the maximum number to 3 datagram retransmissions:

```
sctp-max-assoc-retx 3
```
sctp-max-data-chunks

This command sets the operator-preferred limit to the number of data chunks that can be bundled in an SCTP message.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > SS7 Routing Domain Configuration > Peer-Server Configuration > PSP Configuration
configure > ss7-routing-domain routing_domain_id variant variant_type > peer-server id id
> psp instance psp_instance

Entering the above command sequence results in the following prompt:

[local]host_name(config-ss7-rd-ss7rd_id-ps-peer-server_id-psp-psp_instance)#

Syntax

sctp-max-data-chunks ( limit max_chunks | mtu-limit )

default sctp-max-data-chunks

default
Resets the default for sctp-max-data-chunks to the limit set for the MTU with the sctp-max-mtu-size command.

limit max_chunks
Sets the operator-preferred maximum number of data chunks that can be bundled into SCTP messages. Enter an integer from 1 to 65535.

mtu-limit
Instructs the SGSN to bundle only as many data chunks for the SCTP streams as defined by for the maximum transmission unit (MTU) size configured with the sctp-max-mtu-size command.

Usage
Use this command to override the default MTU-limit for data chunk bundling and configure a preferred maximum number of data chunks that can be bundled into an SCTP message.

Important: Before using this command to set a value, you must disassociate the PSP instance with the no associate command. When you have set the value with this command, then use the associate command to setup a new association.

Example
Set 1024 as a maximum number of data chunks to bundled:

sctp-max-data-chunks limit 1024
sctp-max-in-strms

Configures the maximum number of incoming SCTP streams

Product
SGSN

Privilege
Administrator

Mode
Exec > Global Configuration > SS7 Routing Domain Configuration > Peer-Server Configuration > PSP Configuration

configure > ss7-routing-domain routing_domain_id variant variant_type > peer-server id id > psp instance psp_instance

Entering the above command sequence results in the following prompt:

[local] host_name(config-ss7-ss7rd_id-ss7rd_id-ps-peer-server_id-psp-psp_instance)#

Syntax

sctp-max-in-strms value

default sctp-max-in-strms

default

Returns the configuration to the default of 16.

value

Default: 16.
Specifies the maximum number of incoming SCTP streams as an integer from 1 to 16. The SGSN restricts the allowable range to 2 to 16. If a value of 1 is entered, a value 2 will be applied for any SGSN service associated with this SCTP parameter template.

Usage

Use this command to configure the maximum number of incoming SCTP streams.

Example

The following command configures the maximum number of incoming SCTP streams to 5:
sctp-max-in-strms 5
**sctp-max-init-retx**

This command sets the maximum number of retries to send the INIT datagram.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > SS7 Routing Domain Configuration > Peer-Server Configuration > PSP Configuration

```
configure > ss7-routing-domain routing_domain_id variant variant_type > peer-server id id > psp instance psp_instance
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ss7-rd-ss7rd_id-ps-peer-server_id-psp-psp_instance)#
```

**Syntax**

```
sctp-max-init-retx value
```

**default sctp-max-init-retx**

```
value

Sets the maximum number of retries. This value must be an integer between 0 and 255.

default

Resets the default for sctp-max-init-retx to 5.
```

**Usage**

Use this command to set the maximum number of retries the SCTP layer should make to send the INIT datagram to the peer to open an association.

**Important:** Before using this command to set a value, you must disassociate the PSP instance with the no associate command. When you have set the value with this command, then use the associate command to setup a new association.

**Example**

```
sctp-max-init-retx 3
```
sctp-max-mtu size

This command sets the number of bytes that comprise the maximum MTU size.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > SS7 Routing Domain Configuration > Peer-Server Configuration > PSP Configuration

configure > ss7-routing-domain routing_domain_id variant variant_type > peer-server id id > psp instance psp_instance

Entering the above command sequence results in the following prompt:

[local]host_name(config-ss7-ss7rd_id-ps-peer-server_id-psp-psp_instance)#

Syntax

sctp-max-mtu-size value

default sctp-max-mtu-size

value

Sets the maximum number of bytes for the SCTP MTU size. This value must be an integer between 508 and 65535.

default

Resets the default for sctp-max-mtu-size to 1500 bytes.

Usage

Use this command to configure the size of the MTU.

Important: Before using this command to set a value, you must disassociate the PSP instance with the no associate command. When you have set the value with this command, then use the associate command to setup a new association.

Example

Set the maximum size of the MTU to 3000 bytes:

sctp-max-mtu-size 3000
sctp-max-out-strms

This command sets the maximum number of outgoing streams through the PSP going towards the peer server.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > SS7 Routing Domain Configuration > Peer-Server Configuration > PSP Configuration
configure > ss7-routing-domain routing_domain_id variant variant_type > peer-server id id
> psp instance psp_instance

Entering the above command sequence results in the following prompt:

[local]host_name(config-ss7-rd-ss7rd_id-ps-peer-server_id-ps-peer-server_id-ps-psp-ps_psp_instance)#

Syntax

sctp-max-out-strms max#_out_streams

default sctp-max-out-strms

default

Resets the SGSN’s sctp-max-out-strms value to the default of 2.

max#_out_streams

The value must be an integer between 1 and 16. The value should match the peer node’s (STP/SG/RNC/HLR) number of in-bound streams.

Important: For releases prior to 14.0, the value range was 1 to 65535. However, the system always capped at 16 so in Release 14.0 the range has been decreased to reflect that fact.

Usage

Use this command to balance the stream throughput from the PSP to the peer server. The value for this command is used to validate the incoming packets in the SCTP layer.
If the user tries to configure the value of sctpmax-out-strms less than "2", a message is displayed and the default value is set.

Important: Before using this command to set a value, you must disassociate the PSP instance with the no associate command. When you have set the value with this command, then use the associate command to setup a new association.

Example

Set a maximum SCTP out streams to 12:

sctp-max-out-strms 12
Set a maximum SCTP out streams to the default of 2 streams:

```
default sctp-max-out-strms
```
**sctp-max-path-retx**

This command sets the maximum number of datagram retransmissions for this path.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > SS7 Routing Domain Configuration > Peer-Server Configuration > PSP Configuration

```
configure > ss7-routing-domain routing_domain_id variant variant_type > peer-server id id > psp instance psp_instance
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ss7-rd-ss7rd_id-ps-peer-server_id-psp-psp_instance)#
```

**Syntax**

```
sctp-max-path-retx value

default sctp-max-path-retx
```

**Value**

Sets the maximum number of datagram retransmission to a destination transport address. This value must be an integer from 0 to 255.

**Default**

Resets the `sctp-max-path-retx` default to 5.

**Usage**

Use this command to set the maximum number of datagram retransmissions to a destination transport address. The destination transport address will be declared unreachable after the SGSN exhausts the `sctp-max-path-retx` number of consecutive retransmissions to a destination transport address. Depending upon network conditions, lower values typically means faster detection of SCTP-Path failure.

**Important:** Before using this command to set a value, you must disassociate the PSP instance with the `no associate` command. When you have set the value with this command, then use the `associate` command to setup a new association.

**Example**

```
sctp-max-path-retx 10
```
sctp-parameter

This command enables the SGSN administrator to alter the contents of the Optional Address Parameter IE.

**Product**
SGSN

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > SS7 Routing Domain Configuration > Peer-Server Configuration > PSP Configuration

configure > ss7-routing-domain routing_domain_id variant variant_type > peer-server id id
> psp instance psp_instance

Entering the above command sequence results in the following prompt:

[local]host_name(config-ss7-ss7rd_id-ps-peer-server_id-ps-psp-psp_instance)#

**Syntax**

```
[ default | no ] sctp-parameter ipv4-address suppress single-ended
```

Either command prefix resets the default behavior to repeat the source IP address in the IE.

**Usage**

In situations when the endpoint is uni-homed (that is, single transport layer address), this command enables the SGSN administrator to override the default behavior and to configure the SGSN to suppress (not repeat) the source IP address which is typically included as part of the Optional Address Parameter IE in the INIT/INIT-Ack chunk.

**Example**

Enable suppression of sending repeated IP address in the OAP IE with this command:

```
sctp-parameter ipv4-address suppress single-ended
```

Repeat sending the source IP address in the OAP IE with the following command:

```
no sctp-parameter ipv4-address suppress single-ended
```
**sctp-rto-initial**

This command sets the initial retransmission timeout for the SCTP.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > SS7 Routing Domain Configuration > Peer-Server Configuration > PSP Configuration

`configure > ss7-routing-domain routing_domain_id variant variant_type > peer-server id id > psp instance psp_instance`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ss7-rd-ss7rd_id-ps-peer-server_id-psp-psp_instance)#
```

**Syntax**

```
sctp-rto-initial value
```

```
default sctp-rto-initial
```

- **default**
  
  Resets the system to the `sctp-rto-initial` default of 30 (3 seconds).

- **value**
  
  The value must be an integer between 1 and 50.

**Usage**

**Important:** Before using this command to set a value, you must disassociate the PSP instance with the `no associate` command. When you have set the value with this command, then use the `associate` command to setup a new association.

- Use this command to define the initial retransmission timer.
- The value set for `sctp-rto-initial` should be greater than or equal to the minimum value set with `sctp-rto-min (sctp-rto-initial => sctp-rto-min)`.  
- The value set for `sctp-rto-initial` should be less than or equal to the maximum value set with `sctp-rto-max (sctp-rto-initial <= sctp-rto-max)`.

**Example**

```
sctp-rto-initial 240
```
sctp-rto-max

This command sets the maximum retransmission timeout value for the SCTP.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > SS7 Routing Domain Configuration > Peer-Server Configuration > PSP Configuration

configure > ss7-routing-domain routing_domain_id variant variant_type > peer-server id id > psp instance psp_instance

Entering the above command sequence results in the following prompt:

[local]host_name(config-ss7-rd-ss7rd_id-ps-peer-server_id-psp-psp_instance)#

**Syntax**

```
sctp-rto-max value
```

**default sctp-rto-max**

```
default
```

Sets the system to the default of 600 (60 seconds).

```
value
```

Sets the maximum retransmission timeout value in increments of 100 milliseconds (0.1 seconds) and the value must be an integer between 5 and 1200.

**Usage**

**Important:** Before using this command to set a value, you must disassociate the PSP instance with the `no associate` command. When you have set the value with this command, then use the `associate` command to setup a new association.

Use this command to configure the maximum time for retransmissions. The value set for `sctp-rto-max` should be greater than or equal to the value set for `sctp-rto-initial`.

**Example**

The following sets the timeout for 45 seconds:

```
sctp-rto-max 450
```
sctp-rto-min

This command sets the minimum retransmission timeout (RTO) value for the SCTP.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > SS7 Routing Domain Configuration > Peer-Server Configuration > PSP Configuration
configure > ss7-routing-domain routing_domain_id variant variant_type > peer-server id id
> psp instance psp_instance

Entering the above command sequence results in the following prompt:
[local]host_name(config-ss7-ss7rd_id-ss7rd_ps-peer-server_id-ps Peer-server_id-psp-psp_instance)#

Syntax

sctp-rto-min [ units-10ms ] value
default sctp-rto-min

default

Resets the sctp-rto-min to the default of 10 (1 second).

units-10ms

Including this keyword, before entering a value, enables configuration with finer granularity - in 10 millisecond units.

value

If the units-10ms keyword is included, then set the timeout in increments of 10 milliseconds. The value must be an integer between 1 and 500.
If the units-10ms keyword is not included then set the timeout in increments of 100 milliseconds. The value must be an integer between 1 and 50.

Usage

⚠️ Important: Before using this command to set a value, you must disassociate the PSP instance with the no associate command. When you have set the value with this command, then use the associate command to setup a new association.

Use this command to set the minimum time for retransmission before timeout.
The value set for sctp-rto-min should be less than or equal to the value set for sctp-rto-initial
(sctp-rto-min <= sctp-rto-initial)

Example

The following sets the timeout for 2 seconds:
sctp-rto-min 20
**sctp-sack-frequency**

This command sets the frequency of transmission of SCTP selective acknowledgements (SACK).

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > SS7 Routing Domain Configuration > Peer-Server Configuration > PSP Configuration

```
configure > ss7-routing-domain routing_domain_id variant variant_type > peer-server id id > psp instance psp_instance
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ss7-rd-ss7rd_id-ps-peer-server_id-psp-psp_instance)#
```

**Syntax**

```
sctp-sack-frequency [ units-10ms ] value
```

**default**

```
sack-frequency
```

Sets the maximum number of datagrams to be received prior to sending a SACK to the peer. The value must be an integer between 1 and 5.

```
default
```

Resets the `sctp-sack-frequency` default value of 2.

**Usage**

**Important:** Before using this command to set a value, you must disassociate the PSP instance with the `no associate` command. When you have set the value with this command, then use the `associate` command to setup a new association.

Use this command to set the maximum number of datagrams to be received before a SACK must be sent to the peer. The `sctp-sack-frequency` is used in conjunction with the `sctp-sack-period` to control the generation of SACK, depending on which one occurs first.

**Example**

```
sctp-sack-frequency 3
```
sctp-sack-period

This command sets the delay before sending an SCTP selective acknowledgement (SACK).

Product

SGSN

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > SS7 Routing Domain Configuration > Peer-Server Configuration > PSP Configuration

configure > ss7-routing-domain routing_domain_id variant variant_type > peer-server id id > psp instance psp_instance

Entering the above command sequence results in the following prompt:

[local]host_name(config-ss7-ss7rd_id-ps-peer-server_id-ps-psP_instance)#

Syntax

sctp-sack-period [ units-10ms ] value

default sack-period

units-10ms

Including this keyword, before entering a value, enables configuration with finer granularity - in 10 millisecond units.

value

If the units-10ms keyword is included, then set the timeout in increments of 10 milliseconds. The value must be an integer between 0 and 50.
If the units-10ms keyword is not included then set the timeout in increments of 100 milliseconds. The value must be an integer between 0 and 5.

default

Resets the system to the sctp-sack-period default value, 2 (=200 milliseconds).

Usage

Use this command to set the time the SCTP waits to send a SACK.

Important: Before using this command to set a value, you must disassociate the PSP instance with the no associate command. When you have set the value with this command, then use the associate command to setup a new association.

Example

sctp-sack-period 3
sctp-suppress-alarm

This command enables/disables the suppression of alarms for SCTP path failure between two peer endpoints.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > SS7 Routing Domain Configuration > Peer-Server Configuration > PSP Configuration
configure > ss7-routing-domain routing_domain_id variant variant_type > peer-server id id > psp instance psp_instance

Entering the above command sequence results in the following prompt:

[local] host_name(config-ss7-rd-ss7rd_id-ps-peer-server_id-psp-psp_instance)#

Syntax

[ no ] sctp-suppress-alarm path-failure self-end-point-address orig_IPV4_address peer-end-point-address peer_IPV4_address

no
Disables the pre-configured alarm suppression for SCTP path failure.

path-failure
This keyword specifies that the alarm suppression is for SCTP path failure between two peer nodes.

self-end-point-address orig_IPV4_address
This keyword specifies the IP address of the originating endpoint.
orig_IPV4_address is the IP address of originating endpoint in IPv4 dotted decimal notation.

peer-end-point-address peer_IPV4_address
This keyword specifies the IP address of the peer endpoint.
peer_IPV4_address is the IP address of peer endpoint in IPv4 dotted decimal notation.

Usage
Use this command to configure the path failure alarm suppression. This command ignores the alarms generated on SCTP path failure.

Important: Before using this command to set a value, you must disassociate the PSP instance with the no associate command. When you have set the value with this command, then use the associate command to setup a new association.

Example
The following command suppresses the path failure alarms occurred in SCTP path between originating peer address 1.2.3.4 and peer endpoint 6.7.8.9:

```
sctp-suppress-alarm path-failure self-end-point-address 1.2.3.4 peer-end-point-address 6.7.8.9
```
timeout

This command sets the times for various timeout timers.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > SS7 Routing Domain Configuration > Peer-Server Configuration > PSP Configuration

configure > ss7-routing-domain routing_domain_id variant variant_type > peer-server id id > psp instance psp_instance

Entering the above command sequence results in the following prompt:

[local]host_name(config-ss7-ss7rd_id-ssrd_id-ps-peer-server_id-psp-psp_instance)#

Syntax

timeout { m3ua-periodic-dest-audit dest_timeout | sctp-bundle [ units-10ms ] timer | sctp-heart-beat hrt_bt_timeout }

[ default | no ] timeout { m3ua-periodic-dest-audit | sctp-bundle | sctp-heart-beat }

default

Resets the specified command to the default value.

no

Removes the selected configuration.

m3ua-periodic-dest-audit dest_timeout

Sets the period (in increments of seconds) between the DAUD messages while auditing a destination state.

dest_timeout: Must be an integer from 1 to 65535. Default is 2.

sctp-bundle [ units-10ms ] timer

Specifies that SCTP data chunks are to be queued until this timer expires at which time the data chunks are bundled and committed for transmission. SCTP bundling provides better bandwidth utilization and less traffic, however, there is a packet transmission delay.

timer is an integer from 1 through 65535, in 100ms increments (10 = 1000ms or 1 second).

[ units-10ms ]: Including this optional keyword specifies that the integer timer is to be calculated using 10ms increments (instead of 100ms increments) to allow for finer granularity.

Important: Peer end should also be configured to support SCTP bundling.

Default: SCTP bundling is disabled.
sctp-heart-beat hrt_bt_timeout
Sets the number of seconds in the SCTP heart-beat timer
hrt_bt_timeout: This value is an integer between 1 and 300. Default is 30.

Usage
Use this command to configure timers. Repeat the command with each of the keywords to set values for each.

Important: Before using this command to set a value, you must disassociate the PSP instance with the no associate command. When you have set the value with this command, then use the associate command to setup a new association.

Example

    timeout m3ua-periodic-dest-audit 120
Chapter 284
SGSN Service Configuration Mode Commands

The SGSN Service configuration mode is used within the global configuration mode to specify the 3G operations of the SGSN and the available SGSN services for a specific context.

SGSN Service works with MAP Service, SGTP Service, GTPP Group, and IuPS Service. All five of these services must be configured to enable a 3G SGSN to communicate with other elements within a UMTS network.

**Mode**

Exec > Global Configuration > Context Configuration > SGSN Service Configuration

`configure > context context_name > sgsn-service service_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgsn-service)#
```

⚠️ **Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
accounting

This command defines the accounting context name and enables/disables specific types of CDR generation for the accounting in the SGSN service.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > SGSN Service Configuration

```
configure > context context_name > sgsn-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgsn-service)#
```

**Syntax**

```
accounting ( cdr-types { mcdr | scdr | sms { mo-cdr | mt-cdr } | lcs { mt-cdr | mo-cdr } | smmscdr }+ | context cntx_name )
```

```
default accounting cdr-types
```

```
no accounting ( cdr-types | context )
```

<table>
<thead>
<tr>
<th>command</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Returns the system to default settings for the selected type of CDR.</td>
</tr>
<tr>
<td>no</td>
<td>Removes the pre-configured type of CDR generation for accounting from the SGSN service.</td>
</tr>
</tbody>
</table>

**cdr-types { mcdr | scdr | sms { mo-cdr | mt-cdr } | lcs { mt-cdr | mo-cdr } | smmscdr }**

Default: enabled

Defines the types of CDRs to be generated within the specified SGSN service for accounting:

- **mcdr**: Enables generation of M-CDRs.
- **scdr**: Enables generation of S-CDRs.
- **sms**: Enables generation of SMS-type CDRs based on one of the following:
  - **mo-cdr**: SMS CDRs originates from the mobile.
  - **mt-cdr**: SMS CDRs terminates at the mobile.
- **smmscdr**: This CDR type is currently under development and should not be included in configuration for this release.
- **lcs**: Enables the generation of LCS CDRs, based on:
  - **mt-cdr**: Mobile terminated location request CDR
  - **mo-cdr**: Mobile originated location request CDR
+ Specifies that the specified keywords with in the group can be entered multiple times with a single command.

`context cntx_name`

Specifies an accounting context to be associated with the SGSN service.

`cntx_name`: Define a string of 1 to 79 alphanumeric characters.

**Usage**

Use this command to define the type of CDRs to generate for SGSN service. By default all type of CDRs are generated. Note that change of this configuration will be applied to new call and/or to new PDP contexts only.

By default, the generation of all CDR types is enabled.

**Example**

The following command configures the system to generate CDRs of M-CDR type for accounting in the current SGSN service:

```
accounting cdr-types mcdr
```
admin-disconnect-behavior

This command defines some of the actions the SGSN will take during an Admin-Disconnect procedure.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > SGSN Service Configuration

```
configure > context context_name > sgsn-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgsn-service)#
```

Syntax

```
admin-disconnect-behavior { clear-subscription | detach-type { reattach-not-required | reattach-required } }
[ default | no ] admin-disconnect-behavior { clear-subscription | detach-type }
```

**clear-subscription**

Including this keyword in the configuration instructs the SGSN to clear subscriber contexts and the subscription data database whenever the `clear subscribers all` command is issued (from the Exec mode) for attached subscribers. As well, the SGSN will issue an appropriate Map-Purge-MS-Req to the HLR if needed.

Default: disabled

**detach-type**

Including this keyword defines which type of detach instruction to include in the Detach-Request message during an Admin-Disconnect procedure. One of the following options must be included when this command is entered:

- reattach-not-required
- reattach-required

Default: reattach-required

**default | no**

Including either `default` or `no` keyword in the command, instructs the SGSN to use the default value for the specified parameter.

**Usage**

Include the `clear-subscription` keyword with this command configuration to ensure that more than attached MM-context and active PDP-contexts are cleared when the `clear subscribers all` command is issued for attached subscribers.
To clear subscription data for detached subscribers, refer to the `sgsn clear-detached-subscriptions` command described in the *Exec* mode chapter. Including the `detach-type` keyword with this command instructs the SGSN to include either a ‘reattach-required’ or a ‘reattach-no-required’ instruction in the Detach-Request message.

**Example**

Configure the SGSN to clear data such as PTMSI allocated, auth-vectors received, and NGAF flag values stored in the subscriber database for attached subscribers:

```
admin-disconnect-behavior clear-subscription
```
associate

Associates or disassociates supportive services and policies, such as an Evolved GPRS Tunnelling Protocol (eGTP) service, an HSS peer service, or a MAP service.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > SGSN Service Configuration
configure > context context_name > sgsn-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-sgsn-service)#

Syntax

associate { { camel-service camel_svc_name [ context context_name ] | egtp-service egtp_svc_name [ context context_name ] | gs-service gs_svc_name [ context context_name ] | hss-peer-service hss_svc_name [ context context_name ] | map-service map_svc_name [ context context_name ] | network-global-mme-id-mgmt-db | sgtp-service sgtp_svc_name [ context context_name ] | tai-mgmt-db database_name } | no associate { camel-service | egtp-service | gs-service | hss-peer-service | map-service | network-global-mme-id-mgmt-db | sgtp-service | tai-mgmt-db database_name }

no

Disassociates a previously associated service with this SGSN service.

camel-service camel_svc_name

Associates a CAMEL service with SGSN service.
camel_svc_name specifies the name for a pre-configured CAMEL service to associate with the SGSN service.

egtp-service egtp_svc_name

Associates an eGTP service with SGSN service.
egtp_svc_name specifies the name for a pre-configured eGTP service to associate with the SGSN service.

For more information on the eGTP service, refer to the egtp-service command in the Context Configuration Mode Commands chapter.

Important: Only one eGTP service can be associated with a SGSN service. The eGTP service should be configured prior to issuing this command.

gs-service gs_svc_name

Associates a GS service with this SGSN service.
gs_svc_name specifies the name for a pre-configured GS service to associate with the SGSN service.
**Important:** Only one Gs service can be associated with a SGSN service. The Gs service should be configured prior to issuing this command.

```
associate
```

```
hss-peer-service  hss_svc_name

Associates an HSS peer service with this SGSN service.  
*hss_svc_name* specifies the name for a pre-configured HSS peer service to associate with the SGSN service as an alphanumeric string of 1 through 63 characters. For more information about the HSS peer service, refer to the hss-peer-service command in the Context Configuration Mode Commands chapter and the HSS Peer Service Configuration Mode Commands chapter.
```

**Important:** Only one HSS peer service can be associated to a service in this release. The HSS peer service should be configured prior to issuing this command.

```
map-service  map_svc_name

Associates a MAP service with this SGSN service.  
*map_svc_name* specifies the name for a pre-configured MAP service to associate with the SGSN service. The MAP service is created with the map-service command in the Context Configuration Mode Commands chapter. The MAP service provides Mobile Application Part (MAP) protocol support for the interface between the SGSN and the HLR. For more information on the MAP service, refer to the MAP Service Configuration Mode Commands chapter.
```

**Important:** Only one MAP service can be associated with a SGSN service. The MAP service should be configured prior to issuing this command.

```
network-global-mme-id-mgmt-db

On the S4-SGSN, associates a pre-configured network global MME ID management database with the SGSN service. This enables operators to associate a single custom list of MME Group IDs for use in UMTS to E-UTRAN handovers on the S4-SGSN. The global MME ID management database must be configured on the S4-SGSN using the the network-global-mme-id-mgmt-db command in LTE Policy Configuration Mode before it can be associated with an SGSN service. This command is available on the SGSN only if the SGSN S4 Interface license is enabled.
```

```
sgtp-service  sgtp_svc_name

Associates an SGTP service with this SGSN service.  
*sgtp_svc_name* specifies the name for a pre-configured SGTP service to associate with the SGSN service as an alphanumeric string of 1 through 64 characters. For more information on the SGTP service, refer to the sgtp-service command in the Context Configuration Mode Commands chapter and/or the SGTP Service Configuration Mode Commands chapter.
```

**Important:** The SGTP service should be configured prior to issuing this command. Only one SGTP service can be associated with an SGSN service. When co-locating an SGSN and an MME, the SGSN Service cannot be associated with the same SGTP Service that is used by the MME.
context ctx_name

Identifies a specific context name where the named service is configured. If this keyword is omitted, the named service must exist in the same context as the SGSN service.

ctx_name is name of the configured context of the named service expressed as an alphanumeric string of 1 through 63 characters that is case sensitive.

tai-mgmt-db database_name

Associates this SGSN service with a pre-configured TAI Management Database.

database_name specifies the name of a pre-configured TAI Management Database to associate with the SGSN service as alphanumeric string of 1 through 64 characters. For more information, refer to the tai-mgmt-db command in the LTE Policy Configuration Mode Commands chapter and the LTE TAI Management Database Configuration Mode Commands chapter.

This command is available on the SGSN only if the SGSN S4 Interface license is enabled.

Usage

Use this command to associate a pre-configured service or policy with an SGSN service.

The eGTP service provides eGTP-C protocol interface support between EPS nodes. For more information on the eGTP service and the supported interface type, refer to the eGTP Service Configuration Mode Commands chapter.

**Important:** Only one eGTP service can be associated with a service. The eGTP service should be configured prior to issuing this command.

The HSS peer service provides S6d and S13-prime interface support via the Diameter protocol between the SGSN and an HSS (S6d) or EIR (S13-prime). For more information on HSS peer service and other parameters, refer to the HSS Peer Service Configuration Mode Commands chapter.

**Important:** Only one HSS peer service can be associated to a service in this release. The HSS peer service should be configured prior to issuing this command.

**Caution:** This is a critical configuration. The SGSN service cannot be started without this configuration. Any change to this configuration would lead to restarting the SGSN service. Removing or disabling this configuration will stop the SGSN service.

Example

The following command associates a pre-configured eGTP service called egtp1 in the dst_ctx context to an SGSN service:

```plaintext
associate egtp-service egtp1 context dst_ctx
```

The following command associates a pre-configured HSS peer service called hssl in the same context as SGSN service to an SGSN service:

```plaintext
associate hss-peer-service hssl
```
cc profile

Configures the charging characteristic (CC) profile with the triggers for generating various types of CDR as defined with the accounting command.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > SGSN Service Configuration

```
configure > context context_name > sgsn-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgsn-service)#
```

**Syntax**

```
cc profile profile_bits [ buckets number | interval time | tariff time1 mins hours [ time2 mins hours ] [ time3 mins hours ] [ time4 mins hours ] | volume { downlink down_vol uplink up_vol | total total_vol } ] +
[ no | default ] cc profile profile_bits [ buckets | interval | tariff | volume ]
```

- **no**
  Removes a previously configured CC profile.

- **default**
  Returns the specified CC profile to the original default system settings.

**profile_bits**

Defines the value of the profile bits for the SGSN service.

**index** can be configured to any integer value from 0 to 15. Some of the values have been predefined according to 3GPP standard:

- 1 for hot billing
- 2 for flat billing
- 4 for prepaid billing
- 8 for normal billing

- **buckets number**
  Specifies the number of statistics container changes in the CDR due to QoS changes or tariff times that can occur before an accounting record (CDR) is closed
  Default: 4
  **number**: Must be integer from 1 to 4.
interval time
Specifies the normal time duration (in seconds) that must elapse before closing an accounting record (CDR) provided that any or all of the following conditions occur:

  time: Enter any integer from 60 to 40000000.

tariff time1 mins hours [ time2 mins hours time3 mins hours time4 mins hours ]
Specifies the time-of-day (based on a 24-hour clock) to close the current statistics container in the CDR, but not necessarily the CDR itself. One tariff time must be defined and up to four tariff times can be specified.

Important: The system assumes that the billing system uses the day/date to determine if the statistics container represents an actual tariff period.

  • mins: The minutes of the hour. Enter an integer from 0 to 59.
  • hours: The hour of the day. Enter an integer from 0 to 23.

volume { downlink down_vol uplink up_vol | total total_vol }
Specifies the downlink, uplink, and total volumes octet counts that must be met for the closure of the CDR.

  down_vol: Enter any integer from 100000 to 1345294336.
  up_vol: Enter any integer from 100000 to 400000000.
  total_vol: Enter any integer from 100000 to 400000000.

Usage
Charging characteristics consist of a profile index and behavior settings. This command configures the profile index for the SGSN’s charging characteristics. The SGSN supports up to 16 profile indexes.

Example
The following command configures a profile index of 10 with tariff times of 7:00 AM and 7:30 PM:

    cc profile 10  tariff time1 0 7 time2 30 19 time3 0 7 time4 30 19
check-imei

This command configures the action the SGSN will take if the route towards the EIR is down.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > SGSN Service Configuration

configure > context context_name > sgsn-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-sgsn-service)#

Syntax

check-imei { gf-failure-action | gf-timeout-action } { continue | reject }

default check-imei { gf-failure-action | gf-timeout-action }

default
Resets the default function to reject the Attach.

gf-failure-action
Coupled with either continue or reject, this keyword instructs the SGSN to take action if a valid EIR configuration exists under the MAP service and if the EIR is temporarily unreachable due to associated DPC/SSN inaccessible/out-of-service.

gf-timeout-action
Coupled with either continue or reject, this keyword instructs the SGSN to take action if a valid EIR configuration exists under the MAP service and the route to the EIR is available, but no response is received from the EIR.

continue
Instructs the SGSN to continue the Attach process.

reject
Instructs the SGSN to reject the Attach process.

Usage
Typically, the Attach process will be continued when there is an IMEI check timeout based on the configuration under the SGSN service configuration and/or the GPRS service configuration. But this works only if the route towards the EIR is UP and the IMEI request timer expires. This command configures the SGSN to allow the Attach process to continue in the case the route towards the EIR is down, that is the DPC / SSN is out-of-service.
Example

Use the following command to reset the default and reject Attach:

    default check-imei gf-failure-action
check-imei-timeout-action

In Releases 12.0 and higher, this command has been replaced with enhanced functionality in the `check-imei` command, also available in this configuration mode.
core-network

This command specifies the numeric ID for a core network to identify which CN is to be used by the SGSN service.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > SGSN Service Configuration

configure > context context_name > sgsn-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-sgsn-service)#

Syntax

core-network id cn_id

no core-network id

no

Removes the currently configured core network ID from the current SGSN configuration.

id cn_id

This number identifies the core network to connect the SGSN service.

* cn_id: Must be an integer from 0 through 4095.

Usage

Use this command to set a global ID to identify this SGSN in the core network.

Example

The following command sets the core network ID for the current SGSN service to 127:

    core-network id 127
disable/enable super-charger

This command has been deprecated and replaced by the super-charger command. For the commands to configure the SuperCharger feature, refer to the Call-Control Profile Configuration Mode chapter.
**dns israu-mcc-mnc-encoding**

Configures either decimal or hexadecimal format for the MCC and MNC values in the DNS query which is sent during the ISRAU.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > SGSN Service Configuration
`configure > context context_name > sgsn-service service_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgsn-service)#
```

**Syntax**

```
dns israu-mcc-mnc-encoding { decimal | hexadecimal }
default dns israu-mcc-mnc-encoding
```

**default**
Resets the SGSN to send the MCC and MNC values in decimal format for DNS queries.

**decimal**
Default.
Instructs the SGSN to send the MCC and MNC in decimal format in the DNS query.

**hexadecimal**
Instructs the SGSN to send the MCC and MNC in hexadecimal format in the DNS query.

**Usage**
Use this command to determine the type of encoding for the MCC and MNC to be included in the DNS query sent during the inter-SGSN RAU (ISRAU). The choice must match the format of the DNS server. For example:

In decimal, the MNC/MCC in a DNS query would appear like:

```
rac0017.lac42e3.mnc310.mcc722.gprs
```

In hexadecimal, the MNC/MCC in a DNS query would appear like:

```
rac0017.lac42e3.mnc0136.mcc02d2.gprs
```

**Example**
Use hexadecimal values for the MCC/MNC in the DNS query.
dns israu-mcc-mnc-encoding

dns israu-mcc-mnc-encoding hexadecimal
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**
end

**Usage**
Return to the Exec mode.
**exit**

Exits the current configuration mode and returns to the context configuration mode.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Syntax**
```
exit
```

**Usage**
Return to the context configuration mode.
gmm

This command defines the GPRS mobility management parameters for the SGSN service.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > SGSN Service Configuration

configure > context context_name > sgsn-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-sgsn-service)#

Syntax

gmm { T3302-timeout t3302_dur | T3312-timeout t3312_dur | T3313-timeout initial t3313_init [ decrease t3313_decrement | increase t3313_increment ] | T3322-timeout t3322_dur | T3323-timeout T3323_dur | T3350-timeout t3350_dur | T3360-timeout t3360_dur | T3370-timeout t3370_dur | implicit-detach-timeout secs | max-auth-retransmission auth_retrans | max-identity-retransmission id_retrans | max-page-retransmission page_retrans | max-ptmsi-reloc-retransmission ptmsi_reloc_retrans | mobile-reachable-timeout ms_reach_dur | paging-failure-action downlink-data-lockout-timer seconds [ repeat number_repeats ] | perform-identity-on-auth-failure | purge-timeout minutes | t3346 min minimum max maximum | trau-timeout trau_dur }


no gmm { implicit-detach-timeout | max-auth-retransmission | max-identity-retransmission | perform-identity-on-auth-failure | t3346 }

default

Sets the default value for the specified parameter.

T3302-timeout t3302_dur

Default: 10

Specifies the retransmission timer value to guard the GPRS attach or RAU procedure on MS side.

t3302_dur is the waiting duration in minutes before retransmitting the specific message and must be an integer from 1 through 186.

T3312-timeout t3312_dur

Default: 54

Specifies the retransmission timer value to guard the RAU procedure initiation on network side.
t3312_dur is the waiting duration in minutes before retransmitting the specific message and must be an integer from 1 through 186.

T3313-timeout initial t3313_init [ decrease t3313_decrement | increase t3313_increment ]
Default: 5
Specifies the retransmission timer value to guard the for paging request procedure initiation on network side.
initial t3313_init - Specifies the initial waiting duration in seconds before retransmitting the specific message. t3313_init must be an integer from 1 through 60.
decrease t3313_decrement - Specifies the decrement of the initial timer value in seconds.
t3313_decrement must be an integer from 1 through 5.
increase t3313_increment - Specifies the increment of the initial timer value in seconds.
t3313_increment must be an integer from 1 through 5.

T3322-timeout t3322_dur
Default: 6
Specifies the retransmission timer value to guard the GPRS detach request procedure on network side. t3322_dur is the waiting duration in seconds before retransmitting the specific message and must be an integer from 1 through 20.

T3323-timeout T3323_dur
Default: 54
Specifies that the S4-SGSN Idle Mode Signaling Reduction T3323-timeout deactivation timer will be sent to the UE in Attach Accept and Routing Area Update Accept Messages. T3323_dur specifies the amount of time, in minutes, that will expire before the UE deactivates the ISR feature if the UE is no longer in the UMTS coverage area and has not completed a Routing Area Update with the S4-SGSN within the specified time duration. Once the timer expires, the S4-SGSN waits an additional four minutes before beginning an Implicit Detach for the UE and sends a Detach Notification message (cause = local detach) to the MME across the S3 interface. The MME will then deactivate ISR for the UE since it now also is aware that the UE is no longer in the UMTS coverage area. Valid entry is an integer from 1 to 186.
This command is available only if the Idle Mode Signaling Reduction license is enabled on the S4-SGSN and the Idle Mode Signaling Reduction feature has been activated via the idle-mode-signaling-reduction command in Call Control Profile Configuration Mode.

T3350-timeout t3350_dur
Default: 6
Specifies the retransmission timer value to guard the GPRS attach accept/RAU accept/realloc request procedure sent with P-TMSI and/or TMSI on network side. t3350_dur is the waiting duration in seconds before retransmitting the specific message and must be an integer from 1 through 20.

T3360-timeout t3360_dur
Default: 6
Specifies the retransmission timer value to guard the authentication and cipher request procedure on network side. t3360_dur is the waiting duration in seconds before retransmitting the specific message and must be an integer from 1 through 20.
T3370-timeout  \texttt{t3370\_dur}

Default: 6  
Specifies the retransmission timer value to guard the identity request procedure on network side.  
\texttt{t3370\_dur} is the waiting duration in seconds before retransmitting the specific message and must be an integer from 1 through 20.

\textbf{implicit-detach-timeout  \texttt{secs}}

Default: 3600  
Specifies the implicit detach timer (IDT) timeout value for any 3G calls (not specific to ISR activated calls) as part of the implicit detach procedure on the network side. The IDT starts after expiry of the mobile reachable timer (MNR). Soon after IDT expiry, the subscriber is implicitly detached from the SGSN.  
\texttt{secs} value must be an integer from 1 to 86400.

\textbf{Important:} From R15.0 release onwards the lowest configurable limit of the IDT timeout is modified to “240” seconds.

\textbf{max-auth-retransmission  \texttt{auth\_retrans}}

Default: 4  
Specifies the maximum retransmission of authentication requests allowed.  
\texttt{auth\_retrans} is the number of retries before declaring the authentication failure and must be an integer from 1 through 10.

\textbf{max-identity-retransmission  \texttt{id\_retrans}}

Default: 4  
Specifies the maximum retransmission of identity requests allowed.  
\texttt{id\_retrans} is the number of retries before declaring the identity failure and must be an integer from 1 through 10.

\textbf{max-page-retransmission  \texttt{page\_retrans}}

Default: 5  
Specifies the maximum retransmission of page requests allowed.  
\texttt{page\_retrans} is the number of retries before declaring the paging request failure and must be an integer from 1 through 5.

\textbf{max-ptmsi-reloc-retransmission  \texttt{ptmsi\_reloc\_retrans}}

Default: 5  
Specifies the maximum retransmission for P-TMSI relocation procedure allowed.  
\texttt{ptmsi\_reloc\_retrans} is the number of retries before declaring the P-TMSI relocation procedure failure and must be an integer from 1 through 10.

\textbf{mobile-reachable-timeout  \texttt{ms\_reach\_dur}}

Default: 58  
Specifies the timeout duration for the mobile reachable timer (MNR) for the mobile reachable procedure on network side.  
\texttt{impli\_detach\_dur} sets the waiting duration in minutes before retransmitting the specific message and must be an integer from 4 through 1440.
**paging-failure-action downlink-data-lockout-timer seconds [ repeat number_repeats ]**

Default: 1000 seconds.
Enables and configures the downlink data lockout timer, for the SGSN services, to reduce the frequency of mobile-initiated keep alive messages.

*seconds* set the number of seconds before timer expire, range of 0 to 10000.
*repeat number_repeats* optionally sets the number of times (1 to 10) that the timer restarts after paging failure. **Note:** If repeat is not configured then paging proceeds endlessly until the MR timer expires.

* [ default | no ] gmm paging-failure-action* disables the downlink data lockout timer.

**perform-identity-on-auth-failure**

Default: Enabled
Configures the SGSN service to perform an identity check to ascertain the IMSI after an authentication failure on a PTMSI-based message.

**purge-timeout minutes**

Default: 10080 (7 days)
The purge timer defines the MM-context lifetime, part of the MM-context procedure on the network side. The configured value sets the duration (number of minutes) the SGSN holds the detached subscriber’s MM-context profile. If the subscriber does not reattach to the SGSN during this time, then the SGSN purges this detached subscriber’s MM-context information from its database and sends a MAP purge request towards the HLR to indicate that the subscriber’s profile is gracefully purged from SGSN’s database.

*minutes* must be an integer from 1 through 20160.

**trau-timeout trau_dur**

This timer is available in releases 9.0 and higher.
Default: 30
Specifies the number of seconds the “old” 3G SGSN waits to purge the MS’s data. This timer is started by the “old” SGSN after completion of the inter-SGSN RAU.
*trau_dur*: Must be an integer from 5 to 60.

**Usage**
Repeat this command as needed to configure multiple parameters for GPRS mobility management in a UMTS network. This command provides the configuration of timers for mobility procedures and retries for different messages. GMM layer is defined in the 3GPP TS 24.008 (Release 7).

**Example**
Following command configures the timer to wait for 5 mins before retransmitting the message for GPRS attach or RAU procedure on MS side with maximum number of retries as 6 for authentication:

```
gmm T3302-timeout 5 max-auth-retransmission 6
```
gs-service

This command associates a previously defined Gs service configuration, for the Gs interface to an MSC/VLR, with this SGSN service.

**Important:** This command is used in Releases 12.0 and 12.2. For Release 14.0 refer to the `associate` command.

<table>
<thead>
<tr>
<th>Product</th>
<th>SGSN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privilege</td>
<td>Security Administrator, Administrator</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mode</th>
<th>Exec &gt; Global Configuration &gt; Context Configuration &gt; SGSN Service Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>configure &gt; context context_name &gt; sgsn-service service_name</code></td>
</tr>
</tbody>
</table>

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgsn-service)#
```

**Syntax**

```
gs-service gs_srvc_name context ctx_name

no gs-service gs_srvc_name
```

- **no**
  Removes/disassociates the named Gs service from this SGSN service.

- **gs_srvc_name**
  Specifies the name of a specific Gs service for which to display information.
  `svc_name` is the name of a configured Gs service and can be from 1 to 63 alpha and/or numeric characters and is case sensitive.

- **context ctx_name**
  Specifies the specific context name where Gs service is configured. If this keyword is omitted, the named Gs service must be exist in the same context as the SGSN service.
  `ctx_name` is name of the configured context of Gs service. This can be from 1 to 63 alpha and/or numeric characters and is case sensitive.

**Usage**

Use this command to associate a specific Gs service interface with this SGSN service instance.

**Important:** A single Gs service can be used with multiple SGSN and/or GPRS service.

**Example**

```
```

Cisco ASR 5x00 Command Line Interface Reference
Following command associates a Gs service instance named `stargs1`, which is configured in context named `star_ctx`, with an SGSN service:

```
gs-service stargs1 context star_ctx
```
lac

This command defines the location area code (LAC) in hexadecimal format.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > SGSN Service Configuration
configure > context context_name > sgsn-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-sgsn-service)#

Syntax

lac hex

no lac

no

Erases the lac configuration statement.

hex

Enter a hexadecimal number between 0x0 and 0xFFFF
**max-pdp-contexts**

Configures the maximum number of PDP contexts for a MS (mobile station) that will be supported on this SGSN service.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > SGSN Service Configuration

```bash
configure > context context_name > sgsn-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgsn-service)#
```

**Syntax**

```
max-pdp-contexts per-ms number
```

**default max-pdp-contexts per-ms**

- **default**
  
  Resets the maximum number of PDP contexts per mobile station to the default of 11 for the Gs service configuration.

- **per-ms number**
  
    Default: 11
    
    Defines the combined total number of primary and secondary PDP contexts for the SGSN service.
    
    `number` can be an integer from 2 to 11.

**Usage**

The following example defines 5 as the maximum number of primary and secondary PDP contexts that this SGSN will support for any connected MS.

**Example**

```
max-pdp-contexts per-ms 5
```
mobile-application-part

This command identifies an already defined MAP service (Mobile Application Part service) to associate with the SGSN service. Although the MAP service does not need to be defined in the same context as the SGSN service, there is a one-to-one relationship between a MAP service and an SGSN service.

**Important:** This command is used in Releases 12.0 and 12.2. For Release 14.0 refer to the `associate` command.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > SGSN Service Configuration

```
configure > context context_name > sgsn-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgsn-service)#
```

**Syntax**

```
mobile-application-part service map_svc [ context ctx_name ]
```

no mobile-application-part service

- **no**
  Remove the MAP service association from the SGSN service configuration.

- **service map_svc**
  Specifies the name of the MAP service to be associated with this SGSN service.
  `map_svc` must be the name of a MAP service previously configured on the system.

- **context ctx_name**
  Specifies the name of the context where the MAP service is configured. If the MAP service is not configured in the current context, then the context where it is configured must be specified to enable the SGSN to reach the MAP service.
  If this keyword is not specified, the current context is used.
  `ctxt_name`: Must be the name of the context where the specified MAP service is configured.

**Usage**

Use this command to identify the MAP service configuration to be used by the SGSN service configuration. Also use this command to specify the context in which the MAP service configuration was created.
If the MAP service is not identified or if the correct context is not identified, then the SGSN service will not START.

**Example**
The following command specifies a MAP service named map1 that is configured in the same context as the current SGSN service:

```
mobile-application-part service map1
```
network-sharing cs-ps-coordination

Enables/disables the SGSN service to perform a CS-PS coordination check.

**Important:** This command is no longer available in all 12.0 and 12.2 releases. If you do not see this command in your release, look for the `network-sharing cs-ps-coordination` command in the IuPS Service configuration mode to accomplish the same task. Configuring in the IuPS Service configuration mode allows for the possibility of multiple IuPS services with network-sharing and differing CS-PS coordination requirements.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > SGSN Service Configuration

```bash
configure > context context_name > sgsn-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgsn-service)#
```

**Syntax**

```
network-sharing cs-ps-coordination

default network-sharing cs-ps-coordination

no network-sharing cs-ps-coordination
```

- **default**
  Including this keyword resets the SGSN service to allow the check to be performed.

- **no**
  Disables this feature for the SGSN service.

**Usage**

Use this command to facilitate the network sharing functionality. With this command, the SGSN can be instructed to perform a check to determine if CS-PS coordination is needed.

3GPP TS 25.231 section 4.2.5 describes the functionality of the SGSN to handle CS-PS (circuit-switching/packet-switching) coordination for attached networks not having a Gs-interface. In compliance with the standard, the SGSN rejects an Attach in a MOCN configuration with cause 'CS-PS coordination required', after learning the IMSI, to facilitate the RNC choosing the same operator for both CS and PS domains.

**Example**

Use the following syntax to disable the CS-PS coordination check:

```
no network-sharing cs-ps-coordination
```
nri length

This command defines the Network Resource Identifier (NRI) of the SGSN that is stored in the P-TMSI (bits 23 to 18).

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > SGSN Service Configuration

configure > context context_name > sgsn-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-sgsn-service)#

Syntax

nri length  nri_length [ nri-value nri_value | null-nri-value null_nri_value non-broadcast mcc mcc mnc mnc lac lac_id rac rac_id nri-value value ]

default nri

no nri

default

Release 14.0 and higher.
Resets the nri configuration to nri length 6 and nri-value 0.

no

Deprecated in Release 14.0
Releases prior to 14.0, this command removes the configured NRI value and location information in the P-TMSI that would be retrieved by this SGSN.

nri length  nri_length

Specifies the number of bits to be used in the P-TMSI, bits 23 to 18, to define the network resource identifier (NRI). The NRI length configuration also sets the maximum size of the pool. If not configured, the NRI length will be of zero length.
nri_length: Must be an integer from 1 to 6 to identify the number of bits.

null-nri-value  null_nri_value

This keyword is only available in releases 8.1 and higher.
Configures the null NRI value which must be unique across the pool areas. This keyword is used for the offloading procedure for SGSN pooling (enabled with the sgsn offloading command, see the Exec Mode chapter).
null_nri_value is an integer 0 (zero) to 63 which identifies the SGSN to be used for the offloading procedure for SGSN pooling. There is no default value for this parameter.
**nri length**

This keyword set is only available in releases 8.1 and higher. Defines the non-broadcast LAC/RAC to be used in combination with the null-NRI for the offloading procedure. Including the MCC and MNC to specify the PLMN because the Iu-Flex feature supports multiple IuPS Services.

- **mcc** identifies the mobile country code, the first part of the PLMN ID. Must be an integer between 100 and 999.
- **mnc** identifies the mobile network code portion of the PLMN ID. Must be a 2- or 3-digit integer between 01 and 999.
- **lac_id** defines a location area code associated with an RNC. Must be an integer between 1 and 65535.
- **rac_id** defines the remote area code to be associated with an RNC. Must be an integer between 1 and 255.

**nri-value nri_value**

Specifies the MS-assigned value of the NRI to retrieve from the P-TMSI. This value must not exceed the maximum possible value specified by the NRI length. The NRI value must be unique across the pool or across all overlapping pools.

- **nri_value** must be an integer from 1 to 63 to identify a specific SGSN in a pool. Use of 0 (zero) value is not recommended.

Multiple NRI values can be identified by providing multiple nri-values separated by a blank space for example: `nri length 6 nri-value 29 43 61`

**Usage**

Use this command to identify the SGSN identified with the NRI in the MS generated P-TMSI. This command adds or removes the Iu Flex configuration for this SGSN service. When using Iu Flex, all keywords must be defined. The command can be repeated to specify different values for any of the keyword parameters. If more than one NRI is configured, the SGSN service will round-robin between the available NRIs when new subscribers (re)connect.

Use this command to retrieve the NRI (identity of an SGSN) stored in in bits 23 to 18 of the packet-temporary mobile subscriber identity (P-TMSI). If more than one NRI value is configured, the SGSN service will round-robin between the available NRIs when new subscribers (re)connect.

When using MOCN mode for network sharing without SGSN pooling, the NRI length and the NRI value should both be used.

**Important:** In Releases prior to 14.0, selection of one of the keywords (**nri-value** or **null-nri-value**) was mandatory. With Release 14.0 use of the keywords is optional.

**Example**

The following command specifies the the NRI length as 5 bits, identifies SGSN 23 with MCC 123 and MNC 22 and LAC 222 and RAC 12 for offloading procedure with NRIs 6 and 41:

```
nri length 5 null-nri-value 34 non-broadcast mcc 123 mnc 22 lac 222 rac 12 nri-value 6 41
```
override-lac-li

Refer to the *ASR 5000 Lawful Intercept Guide* for a description of this command.
override-rac-li

Refer to the *ASR 5000 Lawful Intercept Configuration Guide* for a description of this command.
rac

Refer to the *ASR 5000 Lawful Intercept Configuration Guide* for a description of this command.
qos-modification

This command provides the operator the flexibility to control RAB setup and negotiations based on the RNC.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > SGSN Service Configuration
configure > context context_name > sgsn-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-sgsn-service) #

Syntax

qos-modification { inform-rnc-before-ue | allow-s4-rab-negotiation }

no qos-modification [ inform-rnc-before-ue | allow-s4-rab-negotiation ]

no

The SGSN uses the default behavior

• to inform the UE before the RNC or

• to reject PDP Context Activation (in compliance with TS 23.00 section 9.2.2.1A), if the RNC negotiates QoS in the RAB assignment response when the S4 interface is used for the PDP context.

inform-rnc-before-ue

When this keyword is used the SGSN informs the RNC of new QoS before informing the UE. On execution of the command with this keyword, the SGSN initiates a RAB assignment to inform the RNC followed by UPCQ towards the GGSN / Modify towards the UE based on whether or not the RNC downgrades the QoS.

allow-s4-rab-negotiation

With this keyword used as part of the configuration, if the S4 interface is used for PDP activation then the SGSN locally accepts what the RNC sends as QoS in the RAB Assignment Response and sends that QoS in the Activate Response.

This CLI is applicable only for PDP activation. For any other scenario, if the RNC negotiates the QoS then the SGSN ignores this configuration and locally accepts the change and continues with the call.

Usage

This command enables the operator the flexibility to accommodate legacy RNCs that don’t meet the parameters set by TS 23.060.

With allow-s4-rab-negotiation, this keyword is needed for activation cases only as the default behaviour, per 3GPP spec, is to reject activation, which is service impacting. Hence to avoid such service impacts a configuration is added to control the behavior.

Example
Use this command to override the SGSN default behavior during the PDP modification procedure.

```
qos-modification inform-rnc-before-ue
```

Use this command to override the SGSN default behavior and accept PDP activation with legacy RNCs using the S4 interface for context activation:

```
qos-modification allow-s4-rab-negotiation
```
**ran-protocol**

This command specifies the IuPS service for the SGSN service to use for communication with the RAN.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > SGSN Service Configuration

configure > context context_name > sgsn-service service_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgsn-service)#
```

**Syntax**

```
ran-protocol iups-service iups_srvc [ context ctx_name ]

no ran-protocol iups-service

no

Removes the IuPS service information from the SGSN service configuration.

---

**iups-service iups_srvc**

Specifies the name of an IuPS service already configured on the system.

**iups_srvc**: Enter an alphanumeric string of 1 to 63 characters.

---

**ctx_name**

**ctx_name**: Enter the name of the IuPS context, an alphanumeric string of 1 to 63 characters.

---

**Usage**

Use this command to configure the IuPS service context that the current SGSN service will use to communicate with the RAN. Up to 8 definitions can be defined for a single SGSN service to allow for multiple PLMNs support.

**Example**

The following command configures the SGSN service to use an IuPS service named **iups1** that has been configured, in the same context as the SGSN service:

```
ran-protocol iups-service iups1
```
**reporting-action event-record**

This command enables the SGSN to log GMM/SM events in EDR files for 3G services.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > SGSN Service Configuration

```bash
configure > context context_name > sgsn-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgsn-service)#
```

**Syntax**

```
reporting-action event-record

[ default | no ] reporting-action event-record
```

- **default**
  Disables the logging function.

- **no**
  Removes the logging function from the configuration file.

**Usage**

This command is one of the steps needed to enable the SGSN to create a log for events such as Attach, RAU, and Activations. The log is an EDR (event data record) in CSV format. For details about how this feature works, refer to the *GMM-SM Event Logging* chapter in the *SGSN Administration Guide*.

**Related Commands:**
- To enable GMM/SM event logging for 2G services, the `reporting-action event-record` command must be configured in the GPRS service configuration.
- To enable a log to be generated in an EDR file, the `edr-module active-charging-service` command must be enabled in the Context configuration mode.
- To configure parameters for the logging file characteristics and for file transfer, use the commands in the EDR Module Configuration Mode.

**Example**

Enable GMM/SM event logging for 3G services:

```
reporting-action event-record
```
**sgsn-number**

This command defines the E.164 number that identifies this particular SGSN service context.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > SGSN Service Configuration

```
configure > context context_name > sgsn-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgsn-service)#
```

**Syntax**

```
sgsn-number  E.164_number

no sgsn-number
```

**no**

Removes the SGSN number configuration from the SGSN service configuration.

**E.164_number**

Enter a maximum of 15 digits to define the ‘phone’ number associated with this SGSN service in the specified context.

**Usage**
The SGSN supports multiple SGSN numbers – different numbers in the 2G GPRS service configuration and the 3G SGSN service configuration. If an HLR-initiated dialog is received, the SGSN will perform a lookup based on the IMSI and find the correct SGSN number with which the MS is associated. Subsequent messaging will use this address.

**Example**
To delete the sgsn-number associated with this SGSN service context, enter:

```
no sgsn-number
```
sgtp-service

This command creates an instance of an SGTP service and associates the SGTP service instance with this SGSN service.

⚠️ Important: This command is used in Releases 12.0 and 12.2. For Release 14.0 refer to the associate command.

Product
SGSN
PDG/TTG

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > SGSN Service Configuration

configure > context context_name > sgsn-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-sgsn-service)#

Syntax

sgtp-service sgtp_srvc_name

no sgtp-service

sgtp_srvc_name

Enter the name of an SGTP service that will be used by this SGSN service

sgtp_srvc_name: Enter a string of 1 to 63 alphanumeric characters.

Usage

Use this command to access the SGTP Service configuration mode to configure SGTP parameters.

Example

sgtp-service sgtp1
This command configures session management parameters for this SGSN service. This command can be repeated multiple times to configure each parameter individually.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > SGSN Service Configuration

```
configure > context context_name > sgsn-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgsn-service)#
```

**Syntax**

```
sm { T3385-timeout time | T3386-timeout time | T3395-timeout time | guard-timer guard_seconds | ignore-asi | max-actv-retransmission number | max-deactv-retransmission number | max-modf-retransmission number | t3396 min minimum max maximum cause cause_code}
```

```
default sm { T3385-timeout | T3386-timeout | T3395-timeout | guard-timer | max-actv-retransmission | max-deactv-retransmission | max-modf-retransmission }
```

**default**

Resets the selected timer to the system default value.

**T3385-timeout**

Retransmission timer for network-initiated Activate Request.
Default is 8 sec

**T3386-timeout**

Retransmission timer for network-initiated Modify Request.
Default is 8 sec

**T3395-timeout**

Retransmission timer for network-initiated Deactivate Request.
Default is 8 sec

**guard-timer guard_seconds**

Sets the number of seconds before the session manager resources are cleared.

guard_seconds is an integer from 30 to 150.
Default: 80 seconds
**ignore-asi**
Enables the operator to modify the SGSN service default configuration and instructs the SGSN to ignore the ASI bit in the SGSN Context Response during RAU-based handovers over Gn interfaces and to ignore establishing a RAB for any PDPs.

**max-actv-retransmission**
Configures maximum retries for activate PDP ctxt request.
Default is 4

**max-deactv-retransmission**
Configures maximum retries for deactivate PDP ctxt request.
Default is 4

**max-modf-retransmission**
Configures maximum retries for modify PDP ctxt request.
Default is 4

**Usage**
Repeat the command to configure multiple session management parameters for the SGSN service.

**Example**
Use a command similar to the following to set the expiry for 5 seconds for the session manager’s T3385-timeout:

```
sm T3385-timeout 5
```
Chapter 285
SGTP Service Configuration Mode Commands

The SGSN GPRS Tunneling Protocol (SGTP) Service configuration mode provides the configuration of GTP-C and GTP-U related parameters.

**Mode**

Exec > Global Configuration > Context Configuration > SGTP Service Configuration

```
configure > context context_name > sgtp-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgtp-service)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
direct-tunnel-disabled-ggsn

This command makes it possible for the operator to disable direct tunneling on the basis of a GGSN.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > SGTP Service Configuration
configure > context context_name > sgtp-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-sgtp-service)#

**Syntax**

```
direct-tunnel-disabled-ggsn ipv4/ipv6_address

no direct-tunnel-disabled-ggsn [ ipv4/ipv6_address ]
```

- **no**
  Deletes the direct-tunnel-disabled-ggsn configuration which results in re-enabling direct tunneling to the GGSN.
  - Including an IPv4 or IPv6 address for a specific GGSN, re-enables direct tunneling for that specific GGSN.
  - Excluding any IPv4 or IPv6 address from this command removes all direct-tunnel-disabled-ggsn definitions from the SGTP service configuration.

**Usage**

By default, GGSNs and RNCs are assumed to be capable of direct tunneling. This command disables direct tunneling for a specified GGSN. The command can be repeated to disable direct tunneling for multiple GGSNs, thereby creating a ’disabled GGSN’ list. Checking for a direct-tunnel-disabled GGSN is actually the last step in the PDP Activation procedure.

Restricting direct tunneling by a GGSN for an entire APN would be configured with the appropriate command in the APN profile configuration mode.

Restricting direct tunneling at the RNC level would be configured with the appropriate command in the IuPS service configuration mode.

This command can only be used if:
- The Direct Tunnel license has been purchased and applied.
- The Direct Tunnel feature is appropriately enabled via configurations of the IMEI profile and/or the Call-Control and APN profiles.
- The RNC does not restrict direct tunnel.
- The subscriber is not requesting CAMEL services.

**Example**

Use the following command to disable direct tunnel for the GGSN with the IP address of 141.21.4.20:
direct-tunnel-disabled-ggsn 141.21.4.20
disable-remote-restart-counter-verification

This command disables the SGSN’s default behavior for verification of the remote peer’s (GGSN) restart counter change values.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > SGTP Service Configuration

configure > context context_name > sgtp-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-sgtp-service)#

**Syntax**

```
[ default | no ] disable-remote-restart-counter-verification
```

- **default**
  Enables the default behavior for verification of the GGSN’s restart counter change values.

- **no**
  Disables the command configuration and enables the default behavior of verification.

**Usage**

This command disables the default behavior used to minimize PDP deactivations resulting from path failure detection due to erroneous restart counter change messages.

With the execution of this command, the SGSN stops verifying restart counters received in Create PDP Context Response or Update PDP Context Response or Update PDP Context Request (CPCR, CPCR, and UPCQ) messages. When the SGSN detects GTP-C path failure between the SGSN and the GGSN, the SGSN assumes PDP sessions at the GGSN are lost and the SGSN deactivates those PDP sessions towards the UE with an indication that the UE should activate the PDP session again. Potentially, this scenario could cause unnecessary traffic increases within the operator’s network.

The SGSN default behavior provides the ability to manage GTP-C path failures detected as a result of spurious restart counter change value messages received from the GGSN. With the default behavior, path failure detection is based on receipt of restart counter change values in CPCR, CPCR, and UPCQ messages. The session manager informs the SGTPC manager about a changed restart counter value. The SGTPC manager verifies the PDP context status by performing an echo request and echo response with the GGSN. Only then is the path failure confirmed if the echo response contains a new restart counter value. Then the SGTPC manager informs all session managers about the path failure and the session managers begin deactivation of the PDP contexts.

**Related commands:**

- **max-remote-restart-counter-change**, also part of the SGTP service configuration mode, allows the operator to set a maximum variance between stored and received values for restart counter changes coming from the GGSN.
**Example**

Disable the default behavior and stop verification with echo request/response process:

```
   disable-remote-restart-counter-verification
```

Use either of the following commands to enable the default verification behavior:

```
   no disable-remote-restart-counter-verification
   default disable-remote-restart-counter-verification
```
end

Exits the configuration mode and returns to the Exec mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

end

**Usage**

Changes the mode to the Exec mode.
exit

Exits the SGTP Service configuration mode and returns to the Context configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**
Return to the previous mode.
**ggsn-fail-retry-timer**

This command sets the amount of time that a GGSN will be unavailable.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > SGTP Service Configuration

```bash
configure > context context_name > sgtp-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgtp-service)#
```

**Syntax**

```bash

ggsn-fail-retry-timer value

no ggsn-fail-retry-timer

no

Removes the timer setting and disables the Local DNS feature.

value

Defines the amount of time, in seconds, that the GGSN is to be considered unavailable. Enter an integer from 60 to 600. Default is 300.
```

**Usage**

Setting this timer to a valid value enables the Local DNS feature - described in the *SGSN Administration Guide*. Setting this timer marks a GGSN in the primary GGSN pool as unavailable for PDP context creation and causes the SGSN to forward a PDP Context Activation Request to a remote pool GGSN, identified via a local (on the SGSN) DNS check. Marking a GGSN unavailable can be done if there is a reason to believe the GGSN is unavailable; for example, lack of response to GTP messages. Marking a GGSN as unavailable is usually done for a limited period to allow the GGSN time to recover.

**Example**

Enable the Local DNS feature and mark the GGSNs in the primary pool as unavailable for 4 minutes (240 seconds):

```bash

ggsn-fail-retry-timer 240
```
gn-delay-monitoring

This command configures monitoring of Gn/Gp interface to check for the delay of packets between the SGSN and the GGSN.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > SGTP Service Configuration

configure > context context_name > sgtp-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-sgtp-service)#

**Syntax**

```
gn-delay-monitoring [ num-delay number_delayed | num-no-delay-for-clear number_normal | tolerance-seconds number_seconds ]
default gn-delay-monitoring [ num-delay | num-no-delay-for-clear | tolerance-seconds ]
no gn-delay-monitoring
```

---

**default**

Resets the specified parameter to the default value.

---

**no**

Disables Gn/Gp monitoring for delayed GTP-C packets.

---

**num-delay number_delayed**

Defines the number of response messages, coming from the GGSN, that can be delayed (delay time defined by tolerance-seconds parameter) before the delay is flagged to generate an SNMP trap.

`number_delayed`: Enter an integer from 1 to 500, default is 30.

---

**num-no-delay-for-clear number_normal**

Defines the number of consecutive response messages, coming from the GGSN, that must be received without delay (in normal response time) to clear the flag towards the GGSN.

`number_normal`: Enter an integer from 1 to 500, default is 15.

---

**tolerance-seconds number_seconds**

Defines the 'normal' number of seconds the SGSN should wait for a response from the GGSN. After this time, the response would be considered 'delayed'.

`number_seconds`: Enter an integer from 1 to 20, default is 4 seconds.
**Important:** The value for this parameter should be less than the value set for the `retransmission-timeout` parameter of the `gtpc` command, also in this configuration mode.

**Usage**

With this command, the SGSN can monitor the control plane packet delay for GTP-C signaling messages on the SGSN’s Gn/Gp interface towards the GGSN. If the delay crosses this configurable threshold, an alarm will be generated to prompt the operator.

A delay trap is generated when the GGSN response to an ECHO message request is delayed more than a configured amount of time and for a configured number of consecutive responses. When this occurs, the GGSN will be flagged as experiencing delay.

A clear delay trap is generated when successive ECHO Response (number of successive responses to detect a delay clearance is configurable), are received from a GGSN previously flagged as experiencing delay.

This functionality can assist with network maintenance, troubleshooting, and early fault discovery.

**Example**

Enable Gn/Gp monitoring for GTP-C packets that arrive from the GGSN with a delay greater than 5 seconds:

```
    gn-delay-monitoring tolerance-secs 5
```
**gtpc**

Configure the GPRS Tunneling Protocol Control (GTP-C) settings for the SGTP service.

**Product**
- eWAG
- MME
- PDG/TTG
- SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > SGTP Service Configuration

```bash
configure > context context_name > sgtp-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgtp-service)#
```

**Syntax**

```bash
gtpc { bind address ipv4_address | dns-sgsn context context_name | echo-interval interval_seconds | echo-retransmission { exponential-backoff [ [ min-timeout timeout_seconds ] [ smooth-factor smooth_factor ] + ] | timeout timeout_seconds } | guard-interval interval_seconds | ignore response-port-validation | ip qos-dscp dscp_marking | max-retransmissions max_retransmissions | retransmission-timeout timeout_seconds | send { common_flags | rab-context | target-identification-preamble } | sync-echo-with-peer } 
```

```bash
no gtpc { bind address | dns-sgsn context | echo-interval | send { common_flags | rab-context | target-identification-preamble } | sync-echo-with-peer }
```

```bash
default gtpc { echo-interval | echo-retransmission | guard-interval | ignore response-port-validation | ip qos-dscp | max-retransmissions | retransmission-timeout | send { common_flags | rab-context | target-identification-preamble } | sync-echo-with-peer }
```

---

**no**

Disables the configured GTP-C setting.

---

**default**

Resets the specified parameter to its default value.

---

**bind address ipv4_address**

Binds SGTP service to the IP address of the interface.

The bind address for the `gtpc` and `gtpu` commands should be the same.

`ipv4_address` must be a standard IPv4 address.
**gtpc**

---

**SGTP Service Configuration Mode Commands**

---

**dns-sgsn context context_name**

Identify the context where the DNS client is configured to send the DNS query to get the peer SGSN address. If nothing is configured, the system assumes the DNS client is configured in the same context where the SGTP service is configured.

*context_name:* Enter a string of 1 to 79 alphanumeric characters to identify the context.

There is a `dns-sgsn` command option in the call-control profile, which, if configured, would override the configuration in this SGTP service configuration.

---

**echo-interval interval_seconds**

Configures the duration between echoes.

seconds Enter an integer from 0 through 3600.

Default: 60

---

**echo-retransmission { exponential-backoff [ [ min-timeout timeout_seconds ] [ smooth-factor smooth_factor ] + ] | timeout timeout_seconds }**

Configures the retransmission parameters for GTP-C echo messages. The operator can choose to use either an “exponential-backoff” timers or a “fixed-retransmission” timer:

- **The exponential-backoff** timer uses an exponential backoff algorithm to better manage the GTP-C path during periods of network congestion and to perform exponential-backoff echo timing. The exponential-backoff timer uses a calculated round-trip time (RTT), as well as a configurable factor or a multiplier to be applied to the RTT statistic. Different paths can each have a different RTT, so the exponential-backoff timer can be configured for multiple paths. One or both of the following parameters can be configured to refine the exponential-backoff timer configuration:
  - **min-timeout timeout_seconds:** Specifies the minimum time period (in seconds) for the exponential-backoff echo timer. If the RTT multiplied by the smooth factor is less than this minimum timeout value, then the node uses the value set with this keyword. Range is 1-20. Default is 5.
  - **smooth-factor smooth_factor:** Specifies the multiplier that the exponential-backoff echo timer uses when calculating the time to wait to send retries, when the gateway has not received a response from the peer within value defined for the path echo interval. Range is 1-5. Default is 2.
  - **timeout timeout_seconds:** Configures the number of seconds for the fixed retransmission timeout value for GTP-C echo messages. Range from 1 to 20. Default is 5.

---

**guard-interval interval_seconds**

Configures the interval (in seconds) for which the SGTP maintains responses sent to gateway. This optimizes the handling of retransmitted messages. This value should be configured to be greater than the gateway’s configuration for max-retries multiple by retry-interval.

*interval_seconds:* Enter an integer from 10 to 3600.

Default: 100

---

**ignore response-port-validation**

This keyword instructs the gateway to ignore the response port validation.

For the gateway to process incoming GTP responses to an incorrect port, this keyword must be entered, and the same *bind address* must be configured for GTPC and GTPU in the SGTP service.

Default: Disabled. To reset the default for this parameter, you must enter the following command: `no gtpc ignore response-port-validation`.
ip qos-dscp dscp_marking

Configures theDiffServ code point marking to be used per hop behavior (PHB) when sending GTP-C messages originating from the session manager and SGTPC manager.

Note that CS (class selector) mode options below are provided to support backward compatibility with the IP precedence field used by some network devices. CS maps one-to-one to IP precedence, i.e., CS1 is IP precedence value 1. If a packet is received from a non-DSCP aware router, that used IP precedence markings, then the DSCP router can still understand the encoding as a Class Selector code point.

dscp_marking: Enter one of the following values:

- **af11**: Marks traffic as Assured Forwarding 11 PHB (high throughput data)
- **af12**: Marks traffic as Assured Forwarding 12 PHB (high throughput data)
- **af13**: Marks traffic as Assured Forwarding 13 PHB (high throughput data)
- **af21**: Marks traffic as Assured Forwarding 21 PHB (low latency data)
- **af22**: Marks traffic as Assured Forwarding 22 PHB (low latency data)
- **af23**: Marks traffic as Assured Forwarding 23 PHB (low latency data)
- **af31**: Marks traffic as Assured Forwarding 31 PHB (multimedia streaming)
- **af32**: Marks traffic as Assured Forwarding 32 PHB (multimedia streaming)
- **af33**: Marks traffic as Assured Forwarding 33 PHB (multimedia streaming)
- **af41**: Marks traffic as Assured Forwarding 41 PHB (multimedia conferencing)
- **af42**: Marks traffic as Assured Forwarding 42 PHB (multimedia conferencing)
- **af43**: Marks traffic as Assured Forwarding 43 PHB (multimedia conferencing)
- **be**: Designates use of Best Effort forwarding PHB. This is the default value.
- **cs0**: Designates use of class selector mode 0 PHB.
- **cs1**: Designates use of class selector mode 1 PHB.
- **cs2**: Designates use of class selector mode 2 PHB.
- **cs3**: Designates use of class selector mode 3 PHB.
- **cs4**: Designates use of class selector mode 4 PHB.
- **cs5**: Designates use of class selector mode 5 PHB.
- **cs6**: Designates use of class selector mode 6 PHB.
- **cs7**: Designates use of class selector mode 7 PHB.
- **ef**: Designates use of Expedited Forwarding PHB

Default: be (best effort)

max-retransmissions max_retransmissions

Configures the maximum number of retries for packets.

max_retransmissions: Enter an integer from 0 to 15.

Default: 4

retransmission-timeout timeout_seconds

Configures the control packet retransmission timeout in GTP, in seconds.

timeout_seconds: Enter an integer value from 1 through 20.

Default: 5
SGTP Service Configuration Mode Commands

```
gtpc send { common-flags | rab-context | target-identification-preamble }
```

- **common-flags**: This option configures the SGTP service to include or exclude the common flags IE during an Inter-SGSN RAU. When selected, the default is to send the common flags IE.

**Important**: Sending of common flags must be enabled to configure dual PDP type (IPv4v6) addressing with the `dual-address-pdp` command in the SGSN global configuration mode.

- **rab-context**: This option configures the SGTP service to include/exclude the radio access bearer (RAB) context IE in SGSN ‘context response’ message during Inter-SGSN Routing Area Update procedure. Default is to send the RAB context IE.

- **target-identification-preamble**: This option configures the SGTP service to include the Target Identification IE preamble byte in the target-id of Relocation Requests that it sends. By default, the preamble is not included. In accordance with 3GPP TS 29.060, v9.2.0, if the preamble is included then multiple optional parameters, such as Extended RNC ID, are encoded. Extended RNC ID expands the ID range from 4095 to 65535.

  In situations of MME interaction with the SGSN during SRNS procedures via GTPv1, the SGSN can use this Extended RNC ID field to indicate the Target RNC ID associated with the MME and vice versa.

  Default: sending RAB context IE.

**sync-echo-with-peer**

This keyword is applicable to the SGSN only.

This keyword enables the SGSN to synchronize path management procedures with the peer after a GTP service restart recovery.

After GTP service recovery, the SGSN restarts the timers for GTP echo transmission, hence a drift in echo request transmission time (from the pre-recovery time) can occur causing the SGSN to be out of sync with the peer. By using this keyword, when the SGSN receives the first Echo Request (GTPC or GTPU) from the peer after the GTP service restart, in addition to replying with an ECHO Response, the SGSN transmits an ECHO Request to the peer and the SGSN restarts the timers associated with the path management procedures. This causes the path management procedure at SGSN to synchronize with the peer node.

Default: Enabled

**Usage**

Use this command to configure GTP-C settings for the current SGTP service. Repeat the command as needed to configure all required GTP-C parameters.

**Example**

Following command excludes the radio access bearer (RAB) context IE in the SGSN Context Response message during the inter-SGSN RAU procedure:

```
no gtpc send rab-context
```

Configure the SGSN to send `common flags` with all GTP-C messages:

```
gtpc send common-flags
```

Set the SGSN to use GTPC echo-retransmission with exponential-backoff and both filters set for default:

```
gtpc echo-retransmission exponential-backoff
```
**gtpu**

This command configures the GPRS Tunneling Protocol user data plane parameters (GTP-U) for this SGTP service.

**Product**
eWAG  
PDG/TTG  
SGSN  

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > SGTP Service Configuration
configure > context context_name > sgtp-service service_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgtp-service)#
```

**Syntax**

```plaintext
gtpu { bind address ipv4_address | echo-interval interval_seconds | echo-retransmission { exponential-backoff { [ min-timeout timeout_seconds ] [ smooth-factor smooth_factor ] + } | timeout timeout_seconds } | max-retransmissions max_retransmissions | retransmission-timeout timeout_seconds | sync-echo-with-peer

no gtpu { bind address ipv4_address | echo-interval | sync-echo-with-peer}

default gtpu { echo-interval | echo-retransmission | max-retransmissions | retransmission-timeout | sync-echo-with-peer }
```

**no**
Removes the configuration for the specified parameter from the current SGTP service configuration.

**default**
 Resets the specified GTP-U parameter to its factory default.

**bind address ipv4_address**
Defines the GTP-U Gn' interface IP address that binds to this SGTP service. The gtpu and the gtpc commands should be configured with the same bind address.
ipv4_address: Enter a standard dotted-quad IPv4 address.

**echo-interval interval_seconds**
Configures the echo interval.
interval_seconds: Enter an integer from 60 through 3600.
Default: 60
echo-retransmission { exponential-backoff [ [ min-timeout timeout_seconds ] [ smooth-factor smooth_factor ] + ] | timeout timeout_seconds

Configures the retransmission parameters for GTP-U echo messages. The operator can choose to use either an “exponential-backoff” timers or a “fixed-retransmission” timer:

- **exponential-backoff** timer uses an exponential backoff algorithm to better manage the GTP-U path during periods of network congestion and to perform exponential-backoff echo timing. The exponential-backoff timer uses a calculated round-trip time (RTT), as well as a configurable factor or a multiplier to be applied to the RTT statistic. Different paths can each have a different RTT, so the exponential-backoff timer can be configured for multiple paths. One or both of the following parameters can be configured to refine the exponential-backoff timer configuration:
  - **min-timeout timeout_seconds**: Specifies the minimum time period (in seconds) for the exponential-backoff echo timer. If the RTT multiplied by the smooth factor is less than this minimum timeout value, then the node uses the value set with this keyword. Range is 1-20. Default is 5.
  - **smooth-factor smooth_factor**: Specifies the multiplier that the exponential-backoff echo timer uses when calculating the time to wait to send retries, when the gateway has not received a response from the peer within value defined for the path echo interval. Range is 1-5. Default is 2.

- **timeout timeout_seconds** Configures the number of seconds for the fixed retransmission timeout value for GTP-U echo messages. Range from 1 to 20. Default is 5.

max-retransmissions max_retransmissions

Configures the maximum number of retries for retransmitting packets.

**max_retransmissions**: Must be an integer from 0 through 15.

Default: 4

retransmission-timeout timeout_seconds

Configures the retransmission timeout of packets, in seconds.

**timeout_seconds**: Must be an integer from 1 through 20.

Default: 5

sync-echo-with-peer

This keyword is applicable to the SGSN only.

This keyword enables the SGSN to synchronize path management procedures with the peer after a GTP service restart recovery.

After GTP service recovery, the SGSN restarts the timers for GTP echo transmission, hence a drift in echo request transmission time (from the pre-recovery time) can occur causing the SGSN to be out of sync with the peer. By using this keyword, when the SGSN receives the first Echo Request (GTPC or GTPU) from the peer after the GTP service restart, in addition to replying with an ECHO Response, the SGSN transmits an ECHO Request to the peer and the SGSN restarts the timers associated with the path management procedures. This causes the path management procedure at SGSN to synchronize with the peer node.

Default: Enabled

Usage

Use this command to configure the GTP-U settings for the SGTP service.

Example

Set the GTPU echo-interval for 5 seconds:
gtpu echo-interval 5

Set the gateway to use GTP-U echo-retransmission with exponential-backoff and the smooth-factor set for 4:

gtpc echo-retransmission exponential-backoff smooth-factor 4
ignore-remote-restart-counter-change

With the inclusion of the `disable-remote-restart-counter-verification` command, this command has been deprecated.
max-remote-restart-counter-change

Use this command to set a restart counter change window to avoid service deactivations and activations that could cause large bursts of network traffic if the restart counter change messages from the GGSN are erroneous.

**Product**
eWAG
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > SGTP Service Configuration

```
configure > context context_name > sgtp-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-ugtp-service)#
```

**Syntax**

```
max-remote-restart-counter-change variance

default max-remote-restart-counter-change
```

**Syntax**

<table>
<thead>
<tr>
<th>default</th>
<th>If this keyword is used or if a variance window is not configured, then the default value will be 255 and the default behavior will be to detect a restart on any change.</th>
</tr>
</thead>
</table>

**Syntax**

<table>
<thead>
<tr>
<th>variance</th>
<th>Set a number (an 8-bit value) that will define the variance range for restart counter change values compared between the gateway's stored value and the value received in messages from the GGSN. Valid entry is an integer from 1 to 255; default is 255. Value of 32 is recommended as it provides a sufficient window to allow the gateway to handle delayed messages with old restart counters.</th>
</tr>
</thead>
</table>

**Usage**

When the gateway detects GTP-C path failure between the gateway and the GGSN, the gateway assumes PDP sessions at the GGSN are lost and the gateway deactivates corresponding PDP sessions towards the UE with an indication that the UE should activate the PDP session again. Detection is based on receipt of restart counter change values in Create PDP Context Response or Update PDP Context Response or Update PDP Context Request (CPCR/UPCR/UPCQ) messages. Potentially, this scenario can cause major traffic increases within the operator's network. It is possible that the messages received from the GGSN are spurious. The gateway default behavior provides the ability to verify possible GTP-C path failures detected as a result of spurious restart counter change messages received from the GGSN. With the default behavior, the session manager informs the SGTPC manager about a changed restart counter value. The SGTPC manager responds by verifying the PDP context status by performing an Echo Request / Echo Response with the GGSN. If the Echo Response includes a new restart counter change value, then the session manager considers the path failure confirmed and begins the PDP context deactivation sequence.
Use this command to avoid unnecessary path failures and deactivations by setting a restart counter change value 'window' or range of values. With this window, the gateway only accepts linearly increasing values for restart counter change values that are within the specified range of accepted changes before the SGTPC manager verifies. For example, if the allowed window for restart counter change value is set to 32 and the last learnt restart counter change value from the GGSN is 15, then the gateway should detect a restart only if the new restart counter value is between 16 and 47 (range of 32) and then the gateway would verify with the Echo Request/Response. If the received restart counter change value was 200 and the current learnt value was 15 with a window of 32, then the 200 would be ignored as a spurious value.

Also, use this command to set a restart counter change values window to avoid possible 'race conditions' (as defined in 3GPP TS 23.007 v8.7.0) where a new message arrives prior to an older message. This 'race condition' occurs when the gateway's stored restart counter value for the GGSN is larger than the restart counter value received in the messages received from the GGSN.

Related commands:

- disable-remote-restart-counter-verification - also part of the SGTP service configuration mode, this command allows the operator to disable the default behavior.

- pdp-deactivation-rate, in the SGSN Global configuration mode, this allows the operator to modify the rate the gateway deactivates PDP connections when GPT-C path failure is detected.

- ignore-remote-restart-counter, also part of the SGTP service configuration mode.

Example

Use the following command to configure an allowed restart counter change value window of 32:

```
max-remote-restart-counter-change 32
```
mbms

Enables / disables the Multimedia Broadcast Multicast Service.

**Important:** The mbms command and parameter-configuring keywords are under development for future release and should not be used or included in your configuration at this time.
path-failure

This command specifies the method for determining if path failure has occurred.

Product

eWAG
SGSN

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > Context Configuration > SGTP Service Configuration
configure > context context_name > sgtp-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-sgtp-service)#

Syntax

path-failure detection-policy gtp { echo | non-echo } +
{ default | no } path-failure detection-policy

- default
  Resets the specified path failure parameter to default.
  Default: echo (for both GTPC and GTPU)

- no
  Deletes the path-failure definition from the configuration.

- echo
  Path failure is detected when the retries of echo messages time out.

- non-echo
  Path failure is detected when the retries of non-echo messages time out.

Usage

Use this command to define the policy to detect gtp path failure.

Example

Set echo as the policy detection type:

    path-failure detection-policy gtp echo
pool

This command enables the default SGSN functionality for (flex) pooling and enables inclusion of the configured pool hop-counter count in new SGSN context/identify request messages.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > SGTP Service Configuration

configure > context context_name > sgtp-service service_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgtp-service)#
```

**Syntax**

```
pool { default-sgsn | hop-counter count }
no pool { default-sgsn | hop-counter }

default pool hop-counter
```

**no**

Disables the default SGSN pooling functionality or removes the SGSN pool hop-counter IE from the GTP Identity/context requests.

**default**

Removes the SGSN pool hop-counter IE from the GTP Identity/context requests.

**default-sgsn**

Enables default SGSN pooling functionality.

**hop-counter count**

Enables and configures the SGSN pool hop-counter to set the number of hops and to include the configured count in the new SGSN Context Requests or the new SGSN Identify Requests.

If `default-sgsn` is enabled, then any messages relayed will have the default value of 4 for the counter if the message does not include this hop-counter ID.

`count`: Enter an integer from 1 to 255.

Default: 4

**Usage**

Use this command to enable the default flex functionality without exposing the pool (flex) structure. This functionality provides a means for SGSNs outside of the pool to reach a pooled SGSN on the basis of its NRI. Once the pooling has been enabled. Repeat the command using the `hop-counter` keyword to enable inclusion of the hop-counter IE in SGSN context/identify request messages and to configure the count for the
pooling hop-counter. If the SGSN is behaving as the ‘default SGSN’, this SGSN will forward (relay) requests with the hop-count included to the target SGSN.

Example

Enable the default pooling functionality which allows an outside SGSN to reach a pooled SGSN:

```
pool default-sgsn
```

Set the hop-count to be included in messages to 25:

```
pool hop-count
```
Chapter 286
S-GW Service Configuration Mode Commands

The S-GW (Serving Gateway) Service Configuration Mode is used to create and manage the relationship between an eGTP service used for either ingress or egress control plane and user data plane network traffic.

Mode

Exec > Global Configuration > Context Configuration > S-GW Service Configuration

configure > context context_name > sgw-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-sgw-service)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
accounting context

Configures the GTPP accounting context and group selection for S-GW service.

Product
S-GW
SAEGW

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > S-GW Service Configuration

configure > context context_name > sgw-service service_name

Entering the above command sequence results in the following prompt:

[context_name] host_name(config-sgw-service)#

Syntax

accounting context name [ gtpp group name ]

no accounting context

no

Removes the configured accounting context from this service.

context name

Specifies the context where GTPP accounting is performed.

name must be an existing context configured on the system expressed as an alphanumeric string of 1 through 79 characters.

If an accounting context name is not configured in the S-GW service, the context where the S-GW service resides is considered the accounting context and the default GTPP group is used.

gtpp group name

Specifies a GTPP group used to perform GTPP accounting.

name must be an existing GTPP group configured on the system expressed as an alphanumeric string of 1 through 79 characters.

If a GTPP group is not configured, the system will use the default GTPP group in the specified accounting context. If the accounting context is not specified, the system will use default GTPP group in the context where the S-GW service resides.

Usage

Use this command to specify the accounting context and/or GTPP accounting group the S-GW service will use to perform GTPP accounting.

Example

The following command specifies a GTPP accounting context named acct-2 and a GTPP accounting group named gtpp-grp-3 as the context and group the S-GW service will use:
accounting context acct-2 gtp-p group gtpp-grp-3
accounting mode

Configures the mode to be used for accounting – GTPP (default), RADIUS/Diameter or None for S-GW service.

Product
S-GW
SAEGW

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > S-GW Service Configuration

configure > context context_name > sgw-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-sgw-service)#

Syntax

[ default ] accounting mode { gtpp | none | radius-diameter }

default
Sets the accounting mode to GTPP.

gtpp
Specifies that GTPP accounting is performed. This is the default mode.

none
Specifies that no accounting will be performed for the S-GW service.

radius-diameter
Specifies that RADIUS/Diameter will be performed for the S-GW service.

Usage
Use this command to specify the accounting mode for the S-GW service. However, an accounting mode configured for the call-control profile will override this setting. For additional information on accounting mode and its relationship to operator policy, refer to the Serving Gateway Administration Guide.

Example
The following command specifies that RADIUS/Diameter accounting will be used for the S-GW service:

    accounting mode radius-diameter
accounting stop-trigger

Configures the trigger point for accounting stop CDR. Default is on session deletion request.

Product
S-GW
SAEGW

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > S-GW Service Configuration

configure > context context_name > sgw-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-sgw-service)#

Syntax

accounting stop-trigger custom

default accounting stop-trigger

default

Accounting stop CDR triggered once Delete Session/Delete Bearer Request is received at S-GW.

custom

Synchronizes the timestamp in the SGWRECORD CDR and PGWRECORD CDR if the MME cannot reach the UE. When configured, the SGW will also trigger the Accounting stop CDR after receiving the answer (accept for Delete session request) from the MME.

Usage

Use this command to specify the trigger point for accounting stop CDR for this S-GW service.

Example

The following command specifies that accounting stop trigger would be at response of session deletion:

    accounting stop-trigger custom
associate

Associates the S-GW service with QoS and policy control and charging configurations.

Product

S-GW
SAEGW

Privilege

Administrator

Mode

Exec > Global Configuration > Context Configuration > S-GW Service Configuration

configure > context context_name > sgw-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-sgw-service)#

Syntax

associate { access-peer-map | accounting-policy name | egress-proto { gtp | gtp-pmip | pmip } [ egress-context name ] [ egtp-service name ] [ mag-service name ] } | ims-auth-service name | ingress egtp-service name | qci-qos-mapping name | subscriber-map name

no associate { access-peer-map | accounting-policy | egress-proto [ egress-context [ egtp-service ] [ mag-service ] ] | ims-auth-service | ingress egtp-service | peer-map | qci-qos-mapping | subscriber-map }

no

Removes the specified association form the S-GW service.

access-peer-map name

Associates the access/ingress side of the peer-map to the configured S-GW service.

name must be an existing peer-map expressed as an alphanumeric string of 1 through 63 characters.

accounting-policy name

Associates the S-GW service with an accounting policy configured in the same context.

name must be an existing accounting policy expressed as an alphanumeric string of 1 through 63 characters.

Accounting policies are configured through the policy accounting command in the Context Configuration Mode.

egress-proto { gtp | gtp-pmip | pmip } [ egress-context name ] [ egtp-service name ] [ mag-service name ]

Associates and configures the egress protocol for this S-GW service.

gtp: Specifies that GTP is to be used for the S-GW service egress.
gtp-pmip: Specifies that either GTP or PMIP is to be used for the S-GW service egress.

pmip: Specifies that PMIP is to be used for the S-GW service egress.
egress-context name: Specifies that the context in this keyword is to be used for the S-GW service egress.
name must be an existing context on this system expressed as an alphanumeric string of 1 through 63 characters.

egtp-service name: Specifies that the service in this keyword is to be used for the S-GW service egress.
name must be an existing eGTP service on this system expressed as an alphanumeric string of 1 through 63 characters.

mag-service name: Specifies that the service in this keyword is to be used for the S-GW service egress.
name must be an existing MAG service on this system expressed as an alphanumeric string of 1 through 63 characters.

ims-auth-service name
Associates the S-GW service with an IMS authorization service configured in the same context.
name must be an existing IMS auth service and be from 1 to 63 alphanumeric characters.
IMS authorization services are configured through the ims-auth-service command in the Context Configuration Mode.

ingress egtp-service name
Associates and configures the eGTP service ingress for this S-GW service.
name must be an existing eGTP service on this system expressed as an alphanumeric string of 1 through 63 characters.

peer-map name
Associates the access/ingress side of the peer-map to the configured S-GW service
name must be an existing peer-map configuration expressed as an alphanumeric string of 1 through 63 characters.

qci-qos-mapping name
Associates the S-GW service with QCI to QoS mapping parameters.
name must be an existing QCI-QoS mapping configuration expressed as an alphanumeric string of 1 through 63 characters.
QCI-QoS mapping is configured through the qci-qos-mapping command in the Global Configuration Mode.

subscriber-map name
Associates the S-GW service with subscriber map parameters.
name must be an existing subscriber map configuration expressed as an alphanumeric string of 1 through 63 characters.
Subscriber maps are configured through the subscriber-map command in the LTE Policy Configuration Mode.

Usage
Use this command to select a pre-configured QoS mapping and/or policy control and charging configuration to be used by the S-GW service.

Example
The following command associates the S-GW service with an IMS authorization service named ims-23:

```
associate ims-auth-service ims-23
```
**ddn failure-action**

Configures a timer value to delay paging for this UE when the S-GW has initiated a Downlink Data Notification (DDN) to the MME and has received back a DDN failure.

**Product**

S-GW
SAEGW

**Privilege**

Administrator

**Mode**

Exec > Global Configuration > Context Configuration > S-GW Service Configuration

```
configure > context context_name > sgw-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgw-service)#
```

**Syntax**

```

ddn failure-action pkt-drop-time seconds

default ddn failure-action pkt-drop-time
```

**ddn failure-action pkt-drop-time**

```
default
```

Sets the command to its default setting of 300 seconds.

```
failure-action pkt-drop-time seconds
```

Default: 300

Configures a timer that determines how long the S-GW will discard downlink data packets so the MME has enough time to receive the Modify Bearer Request and prevent further errors being sent to the S-GW in the DDN Ack message.

`seconds` must be an integer value from 1 to 300.

**Usage**

Use this command to set a timer value to delay the sending of excessive Downlink Data Notification messages to the MME (and receiving excessive DDN Ack message with errors from the MME) in cases when downlink data is arriving before the Modify Bearer Request is received. During the delay, downlink data packets are discarded until the timer has expired. This timer is triggered upon receiving the first error in a DDN Ack message from the MME.

**Related Functionality**

DDN Delay: By default, the S-GW supports the delay value IE included in a DDN acknowledgement message. The S-GW automatically multiplies this value by 50 ms, then applies the calculated delay for DDN for the UE.

**Example**

---

---
The following command configures the S-GW to discard downlink data packets for 200 seconds after the S-GW receives an error in a DDN Ack message from the MME:

```
.ddn failure-action pkt-drop-time 200
```
ddn isr-sequential-paging

Configures the delay time in 100 millisecond increments between paging of different RAT types in support of the Intelligent Paging for ISR feature.

Product
S-GW
SAEGW

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > S-GW Service Configuration

Syntax

ddn isr-sequential-paging delay-time delay

default ddn isr-sequential-paging

default
Returns the delay time to its default value of 10 (10 * 100 ms = 1 second).

delay-time delay
Configures delay between paging of different RAT types.
delay must be an integer from 1 to 255, representing increments of 100 milliseconds (delay = 1-255 * 100 ms).
Default: 10 (10 * 100 ms = 1 second)

Usage
Use this command to configure the delay time in (100 millisecond increments) between paging of different RAT types in support of the Intelligent Paging for ISR feature.

Example
The following command configures the delay timer to 5 seconds

ddn isr-sequential-paging delay-timer 50
**ddn throttle**

Configures Downlink Data Notification throttle parameters.

**Product**
S-GW
SAEGW

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > S-GW Service Configuration
configure > context context_name > sgw-service service_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgw-service)#
```

**Syntax**

```
ddn throttle arp-watermark arp_value [ rate-limit limit time-factor seconds throttle-factor percent increment-factor percent [ poll-interval seconds ] throttle-time-sec seconds [ throttle-time-min minutes ] [ throttle-time-hour hour ] stab-time-sec seconds [ stab-time-min minutes ] [ stab-time-hour hour ]
```

```
no ddn-throttle
```

**no**

Disables the DDN throttling feature.

```
throttle arp-watermark arp_value
```

If ARP watermark is configured and if an MME/SGSN sends the throttling factor and delay in a DDN ACK message, all the DDNs which have an ARP value greater than the configured value will be throttled by the throttle factor for the specified delay.

`arp_value` is an integer from 1 through 15.

```
rate-limit limit
```

Configures the rate limit (Use this and subsequent tokens to rate-limit only if the MME is a Non-Release 10 MME).

`limit` is an integer from 1 through 999999999.

```
time-factor seconds
```

Configures the time duration during which the S-GW makes throttling decisions.

`seconds` is an integer from 1 to 300.

```
throttle-factor percent
```

Configures the DDN throttling factor. Enter the percentage of the DDN to be dropped upon detecting a DDN surge.

`percent` is an integer from 1 through 100.
**increment-factor** `percent`

Configures the DDN throttling increment factor. Enter the percentage by which the DDN throttling should be increased.

`percent` is an integer from 1 through 100.

**poll-interval** `seconds`

Configures the polling interval in DDN throttling.

`seconds` is an integer from 2 through 999999999.

**throttle-time-sec** `seconds`

Configures the DDN throttling time in seconds. Enter time period in seconds over which DDN are throttled at the S-GW.

`seconds` is an integer from 0 through 59.

**throttle-time-min** `minutes`

Configures the DDN throttling time in minutes. Enter time period in minutes over which DDN are throttled at the S-GW.

`minutes` is an integer from 0 through 59.

**throttle-time-hour** `hour`

Configures the DDN throttling time in hours. Enter time period in hours over which DDN are throttled at the S-GW.

`hour` is an integer from 0 through 310.

**stab-time-sec** `seconds`

Configures the DDN throttling stabilization time in seconds. Enter a time period in seconds over which if the system is stabilized, throttling will be disabled.

`seconds` is an integer from 0 through 59.

**stab-time-min** `minutes`

Configures the DDN throttling stabilization time in minutes. Enter a time period in minutes over which if the system is stabilized, throttling will be disabled.

`minutes` is an integer from 0 through 59.

**stab-time-hour** `hour`

Configures the DDN throttling stabilization time in hours. Enter a time period in hours over which if the system is stabilized, throttling will be disabled.

`hour` is an integer from 0 through 310.

**Usage**

Use this command to throttle DDNs to allow for the creation of the tunnel and avoid unnecessary DDNs.

For a UE in idle mode, S1U bearers are not established. In such a case, if a downlink packet arrives for the UE, the S-GW initiates a paging procedure towards the MME. The MME in turn pages the UE in its tracking area to search for the UE. Upon receiving the paging request, the UE establishes S1U bearers. Too many DDN requests towards the MME from the S-GW could overload the MME. To reduce this load, the MME
can dynamically request S-GW to reduce a certain percentage of DDN messages sent towards it for a given period time.
The S-GW supports the following IEs for this feature:

- ARP IE in Downlink Data Notification
- DL Low Priority Traffic Throttling IE in DDN Acknowledge Message

More information is available in Release 10 of 3GPP 29.274, section 5.3.4.3.
The S-GW supports DDN throttling for up to 24 MMEs. DDNs for additional MMEs (25+) will be sent as normal and will not be throttled.
Throttling statistics can be viewed by issuing the Exec mode command:

`show sgw-service statistics all`

**Example**

The following command sets the ARP watermark lowest priority to 10 seconds:

```
.ddn throttle arp-watermark 10
```

If the ARP value provided is 10, all bearers with ARP value between 10-15 are treated as low priority bearers and are given throttling treatment. Throttling would not be enabled if the ARP value is not provided through S-GW service configuration. Also, the ARP IE in DDN message towards MME would not be included unless DDN throttling is configured in S-GW service.
egtp-service

Configures an eGTP service to use as either an ingress (S1-U) or egress (S5/S8) service for the S-GW.

Product
S-GW
SAEGW

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > S-GW Service Configuration
configure > context context_name > sgw-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-sgw-service)#

Syntax

egtp-service { egress { context name | service name } | ingress service name }

no egtp-service { egress { context | service } | ingress service }

no

Removes the selected EGTP service from this service.

egress { context name | service name }

Specifies the egtp-service to be used as the egress eGTP service on a GTP-based S5/S8 interface.
context name: Specifies the name of the context where the eGTP service resides.
name must be an existing context name where an eGTP service resides expressed as an alphanumeric string of 1 through 63 characters.

service name: Specifies the name of the egress eGTP service.
name must be an existing eGTP service name expressed as an alphanumeric string of 1 through 63 characters.

ingress service name

Specifies the egtp-service to be used as the ingress eGTP service on the S11 interface.
name must be an existing eGTP service name expressed as an alphanumeric string of 1 through 63 characters.

Usage
Use this command to configure the eGTP service to use with this S-GW service. The eGTP service must be existing and be configured with the appropriate parameters supporting the intended service type.

Example
The following command configures the S-GW service to use an eGTP service named slu-egtp as its ingress service:

    egtp-service ingress service slu-egtp
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**
Use this command to return to the Exec mode.
**exit**

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
```
exit
```

**Usage**
Use this command to return to the parent configuration mode.
gtpu-error-ind

Configures the actions to be taken upon receiving a GTP-U error indication from an RNC, eNodeB, SGSN, or P-GW.

**Product**

S-GW  
SAEGW

**Privilege**

Administrator

**Mode**

Exec > Global Configuration > Context Configuration > S-GW Service Configuration

```bash
configure > context context_name > sgw-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgw-service)#
```

**Syntax**

```bash
 gtpu-error-ind { { s12 | s1u } { local-purge | page-ue [ custom1-behavior ] } | { s4u | s5u } { local-purge | signal-peer } }

default gtpu-error-ind { s12 | s1u | s4u | s5u }
```

**default**

Resets the command to the default action for the specified interface. For S12 and S1-U, `page-ue` is the default action. For S4-U and S5-U, `local-purge` is the default action.

```bash
{ s12 | s1u } { local-purge | page-ue [ custom1-behavior ] } 
```

Specifies the action to take when a GTP-U error indication is received from a Radio Network Controller (RNC) over an S12 interface or from an eNodeB over the S1-U interface.

**local-purge:** The S-GW clears the affected bearer (or PDN if error-indication is received on default bearer) locally without informing peer.

**page-ue [ custom1-behavior ]:** The S-GW moves the complete UE state to S1-Idle and starts paging for this UE. If the custom1-behavior option is specified, the S-GW will guard the paging attempt with a timer of 60 seconds. Within this time the bearer must have the eNodeB TEID refreshed by an MME. Otherwise, the S-GW will clear the affected bearer with signaling. This is the default action for GTP-U error indication messages received on the S12 and S1-U interfaces.

```bash
{ s4u | s5u } { local-purge | signal-peer }
```

Specifies the action to take when a GTP-U error indication is received from an SGSN over an S4-U interface or from a P-GW over the S5-U interface.

**local-purge:** The S-GW clears the affected bearer (or PDN if error-indication is received on a default bearer) locally without informing the peer. This is the default action for GTP-U error indication messages received on the S4-U and S5-U interfaces.

**signal-peer:** The S-GW initiates control signalling towards the peer MME and P-GW. When signalling:

- For a bearer deletion, the S-GW sends a Delete-Bearer-Command message to the P-GW and a Delete-Bearer-Request (with EBI) message to the MME.
For PDN deletion, the S-GW sends a Delete-Session-Request message to the P-GW and a Delete-Bearer-Request (with LBI) message to the MME.

The S-GW will not wait for Delete replies from the peer. The request will be sent only once and local resources will be reset.

**Usage**

Use this command to specify the action to taken upon receiving a GTP-U error indication from an RNC over an S12 interface, an eNodeB across an S1-U interface, an SGSN over an S4-U interface, or from a P-GW across an S5-U interface.

**Example**

The following command sets the action to take upon receipt of a GTP-U error indication from the eNodeB to clear affected bearer:

```
gtpu-error-ind s1u local-purge
```
**mag-service**

Identifies the Mobile Access Gateway (MAG) egress service through which calls are to be routed for this S-GW service.

**Product**

S-GW

**Privilege**

Administrator

**Mode**

Exec > Global Configuration > Context Configuration > S-GW Service Configuration

```bash
configure > context context_name > sgw-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgw-service)#
```

**Syntax**

```bash
mag-service egress service name
no mag-service egress service
```

**no**

Removes the configured MAG egress service from this service.

```bash
egress service name
```

Specifies the MAG service name to be used as the egress MAG service on a Proxy Mobile IPv6 (PMIP) based S5/S8 interface.

`name` must be an existing MAG service expressed as an alphanumeric string of 1 through 63 characters.

**Usage**

Use this command to specify the name of the MAG service where calls are to be routed.

**Example**

The following command specifies that an existing MAG service named `mag3` is to be used to route call through for this S-GW service:

```bash
mag-service egress service mag3
```
ntsr session-hold timeout

Configures a timer to hold the session after path failure is detected at the MME (for Network Triggered Service Restoration).

Product
S-GW

Privilege
Administrator, Security Administrator

Mode
Exec > Global Configuration > Context Configuration > S-GW Service Configuration

`configure > context context_name > sgw-service service_name`

Entering the above command sequence results in the following prompt:

```
[context_name] host_name(config-sgw-service)#
```

Syntax

```
[ no ] ntsr session-hold timeout seconds
```

`no`

Disables the NTSR session-hold timeout.

```
ntsr session-hold timeout seconds
```

Configures the timer duration, in seconds, that determines how long the session will be held after path failure is detected during MME restoration. Valid entries are from 1 to 3600 seconds.

Usage

Use this command to configure the timer duration, in seconds, that determines how long the session will be held after path failure is detected during MME restoration.

Example

To configure the ntsr session-hold timeout for 10 seconds.

```
ntsr session-hold timeout 10
```
page-ue

Allows the S-GW to page the UE for P-GW-initiated procedures (Create Bearer Request (CBR)/Modify Bearer Request (MBR)/Update Bearer Request (UBR)) when the UE is idle, and sends a failure response to the P-GW with the cause code 110 (Temporary Failure) when the UE is idle or a collision is detected at the S-GW.

Product
S-GW
SAEGW

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > S-GW Service Configuration
configure > context context_name > sgw-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-sgw-service)#

Syntax

[ default | no ] page-ue pgw-initiated-proc

- **default**
  Returns the command to its default setting of disabled.

- **no**
  Disables the feature.

- **pgw-initiated-proc**
  Sets the command to page the UE for P-GW initiated MBR, UBR, and CBR procedures.

Usage

Use this command to allow the S-GW to page a UE for P-GW-initiated procedures (CBR/MBR/UBR) when the UE is idle, and sends a failure response to the P-GW with the cause code 110 (Temporary Failure) when the UE is idle or a collision is detected at the S-GW.

Example

The following command enable the S-GW to page the UE
path-failure

Configures the action to take upon the occurrence of a path failure between the S-GW and the MME, P-GW, RNC, SGSN, or eNodeB.

**Product**
S-GW
SAEGW

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > S-GW Service Configuration

```
configure > context context_name > sgw-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgw-service)#
```

**Syntax**

```
path-failure { s11 | s12 | s1u | s4 | s4u | s5 | s5u } ( local-purge | signal-peer )
```

```
default path-failure { s11 | s12 | s1u | s4 | s4u | s5 | s5u }
```

**default**

Returns the command to the default setting of “local purge” for the selected interface.

```
{ s11 | s12 | s1u | s4 | s4u | s5 | s5u }
```

Specifies the interface to which the action will be applied.

- **s11**: Applies the path failure action to the S11 interface between the S-GW and the MME.
- **s12**: Applies the path failure action to the S12 interface between the S-GW and the RNC.
- **s1u**: Applies the path failure action to the S1-U interface between the S-GW and the eNodeB.
- **s4**: Applies the path failure action to the S4 control plane interface between the S-GW and the SGSN.
- **s4u**: Applies the path failure action to the S4-U user plane interface between the S-GW and the SGSN.
- **s5**: Applies the path failure action to the S5 interface between the S-GW and the P-GW.
- **s5u**: Applies the path failure action to the S5-U user plane interface between the S-GW and the P-GW.

```
{ local-purge | signal-peer }
```

Specifies the action to apply to the selected interface.

- **local-purge**: The S-GW clears the affected bearer (or PDN if path failure is received on a default bearer) locally without informing the peer. This is the default action for all interface.
- **signal-peer**: The S-GW initiates control signalling towards the peer MME and P-GW. When signalling:
  - For a bearer deletion, the S-GW sends a Delete-Bearer-Command message to the P-GW and a Delete-Bearer-Request (with EBI) message to the MME.
  - For PDN deletion, the S-GW sends a Delete-Session-Request message to the P-GW and a Delete-Bearer-Request (with LBI) message to the MME.
The S-GW will not wait for Delete replies from the peer. The request will be sent only once and local resources will be reset.

**Usage**

Use this command to specify the type of action to take when a path failure occurs on one of the supported interfaces.

**Example**

The following command sets the path failure action for the S5 interface to “signal peer”:

```
path-failure s5 signal-peer
```
pgw-fteid-in-relocation-cs-rsp

Controls the sending of the PGW Fully Qualified Tunnel Endpoint Identifier (FTEID) for relocation Create Session Response procedures with an S-GW change.

**Product**
S-GW

**Privilege**
Administrator, Security Administrator

**Mode**
Exec > Global Configuration > Context Configuration > S-GW Service Configuration

```plaintext
configure > context context_name > sgw-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgw-service)#
```

**Syntax**

```plaintext
[no] pgw-fteid-in-relocation-cs-rsp
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>no</code></td>
<td>Disables the sending of the P-GW FTEID in Create Session Response procedures where there is an S-GW relocation change. This is the default setting.</td>
</tr>
<tr>
<td><code>pgw-fteid-in-relocation-cs-rsp</code></td>
<td>Enables the sending of the P-GW FTEID in Create Session Response procedures where there is an S-GW relocation change.</td>
</tr>
</tbody>
</table>

**Usage**

Use this command to control the sending of the PGW Fully Qualified Tunnel Endpoint Identifier (FTEID) for relocation Create Session Response procedures with an S-GW change. For backward compatibility with earlier 3GPP release peer nodes requiring the P-GW FTEID in the Create Session Response procedures, this configurable can be enabled.

**Example**

To enable the sending of the FTEID for relocation Create Session REsponse procedures with an S-GW change..

```plaintext
pgw-fteid-in-relocation-cs-rsp
```
plmn

Configures the public land mobile network (PLMN) identifiers for this S-GW service.

**Product**
S-GW
SAEGW

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > S-GW Service Configuration

```
configure > context context_name > sgw-service service_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-sgw-service)#
```

**Syntax**

```
plmn id mcc number mnc number [ primary ]
no plmn id mcc number mnc number
```

<table>
<thead>
<tr>
<th>no</th>
</tr>
</thead>
</table>
| Removes the configured PLMN ID for this S-GW service.

<table>
<thead>
<tr>
<th>mcc number</th>
</tr>
</thead>
</table>
| Configures the Mobile Country Code for this PLMN ID.  
*number* must be an integer from 100 through 999.

<table>
<thead>
<tr>
<th>mnc number</th>
</tr>
</thead>
</table>
| Configures the Mobile Network Code for this PLMN ID.  
*number* must be a 2- or 3-digit integer from 00 through 999.

<table>
<thead>
<tr>
<th>primary</th>
</tr>
</thead>
</table>
| Specifies that this is the primary PLMN ID for this S-GW service.

**Usage**

The PLMN identifier is used by the S-GW service to determine whether or not a mobile station is visiting, roaming, or home. Multiple S-GW services can be configured with the same PLMN identifier. Up to five PLMN IDs can be configured for each S-GW Service. In Release 15.0 and later, up to 15 PLMN IDs can be configured.

**Example**

The following command configures a “primary” PLMN ID for this S-GW service with an MCC of 123 and an MNC of 12:

```
plmn id mcc 123 mnc 12 primary
```
reporting-action

Configures the system to start reporting session events.

Product
S-GW
SAEGW

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > S-GW Service Configuration

configure > context context_name > sgw-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-sgw-service)#

Syntax

[ no ] reporting-action event-record [ trigger active-idle ]

default reporting-action event-record

default

Returns the command to its default setting of disabled.

no

Disables session event reporting.

trigger active-idle

Specifies that the event is only to be reported upon the going from active to idle.

Usage

Use this command to enable the session event reporting feature on the S-GW.

Example

The following command enables event reporting but does not limit it to events triggered by going active to idle:

reporting-action event-record
timeout idle

This command removes S-GW sessions that remain idle for longer than the configured time limit.

Product
S-GW
SAE-GW

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > S-GW Service Configuration

configure > context context_name > sgw-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-sgw-service)#

Syntax

timeoutidle dur_seconds

timeout idle

 Enables the S-GW session idle timer.

dur_seconds

 Specifies the time limit, in seconds, after which the SGW session will be torn down. Valid entries are from 0 to 4294967295.

Usage

The S-GW session idle timer removes stale sessions in those cases where the session is removed on the other nodes but due to some issue remains on the S-GW. Once configured, the session idle timer will tear down such sessions that remain idle for longer than the configured time limit. The implementation of the session idle timer allows the S-GW to more effectively utilize system capacity.

Example

The following example configures the S-GW session idle timer 3600 seconds (one minute).

timeout idle 3600
Chapter 287
SMS Service Configuration Mode Commands

The SMS (short message service) Service configuration mode is used to create and manage properties of the SMS Service configuration.

The SGSN uses the SMS Service component to communicate via the Gd interface with a gateway message service controller (GMSC) to send short text messages (up to 140 octets in length) to a mobile (SMS-MT) and/or receive messages from a mobile (SMS-MO).

**Mode**

Exec > Global Configuration > Context Configuration > MAP Service Configuration > SMS Service Configuration

```
configure > context context_name > map-service service_name > short-message-service
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-map-service-service_name-sms-service)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
**cp-data**

Enables the SGSN to send and/or receive cp-data (text messages).

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > MAP Service Configuration > SMS Service Configuration

configure > context context_name > map-service service_name > short-message-service

Entering the above command sequence results in the following prompt:

```plaintext
[context_name]host_name(config-map-service-service_name-sms-service)#
```

**Syntax**

```plaintext
cp-data max-retransmission retries_num

default cp-data max-retransmissions
```

- **default**
  
  This keyword resets the SGSN’s max-retransmission to the default number of retries.

- **max-retransmission retries_num**
  
  ```plaintext
  retries_num: enter an integer from 1 to 3.
  ```

**Usage**

Use this command to configure the number of times the SGSN will attempt to retransmit a message.

**Example**

```plaintext
cp-data max-retransmission 2
```
**end**

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
ext
```

**Usage**
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Use this command to return to the parent configuration mode.
mo-message-forwarding-destination

This command defines the SGSN’s handling policy for MO (mobile originating) message.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > MAP Service Configuration > SMS Service Configuration
configure > context context_name > map-service service_name > short-message-service

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-map-service-service_name-sms-service)#`

**Syntax**

```
[ default ] mo-message-forwarding-destination { gmsc-selected-from-imsi | smsc-supplied-by-subscriber }
```

---

**default**

Resets the SMS service configuration to the default message forwarding technique.

---

**gmsc-selected-from-imsi**

Entering this keyword enables SMS-MO messages to be forwarded on the basis of their IMSI prefix.

---

**smsc-supplied-by-subscriber**

Entering this keyword enables SMS-MO messages to be forwarded on the basis of the SMSC (SMS controller) address provided by the subscriber.

---

**Usage**

Use this command to define how the mobile originated SMS are to be routed.

**Example**

```
mo-message-forwarding-destination gmsc-selected-from-imsi
```
smsc-address-restriction-list

Define the list of SMS-C addresses to be screened.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > MAP Service Configuration > SMS Service Configuration

```
configure > context context_name > map-service service_name > short-message-service
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-map-service-service_name-sms-service)#
```

**Syntax**

```
smisc-address-restriction-list isdn-no +

no smisc-address-restriction-list isdn-no
```

- **no**
  - Delete an SMS-C address (ISDN number) from the list.

  ```
isdn-no +
  ```

- **isdn-no +**
  - Enter up to 10 ISDN numbers, each up to 15 digits. Put a single space, without a comma, between each ISDN number being added to the list with one command.

**Usage**

Use this command to identify a list of SMS-C that are to be screened and restricted from receiving forwarded SMS. This list is part of the SMS-C address denial mechanism. For the mechanism to actually function, a second command must be configured, the `smsc-address-restriction-list` command.

**Example**

Add 3 ISDN numbers to the list of restricted SMS-C addresses.

```
smsc-address-restriction-list 443719933751427 422311198977765 901231445513131
```

Remove an ISDN number from the list of restricted SMS-C addresses.

```
no smisc-address-restriction-list 443719933751427
```
smsc-address-restriction-type

Define the list of SMS-C addresses to be screened.

Product
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > MAP Service Configuration > SMS Service Configuration
configure > context context_name > map-service service_name > short-message-service

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-map-service-service_name-sms-service)#

Syntax

smsc-address-restriction-type { mo-mt-sms | mo-sms | mt-sms }

default smsc-address-restriction-type

default
Resets the restriction type to the default of both MT and MO types.

mo-mt-sms
Sets the restriction for both types of messages - mobile-originated (MO-SMS) and mobile-terminated (MT-SMS).

mo-sms
Sets the restriction for the mobile-originated (MO-SMS) messages.

mo-mt-sms
Sets the restriction for the mobile-terminated (MT-SMS) messages.

Usage

Use this command to identify the types of messages that are to be denied to the SMS-C identified in the
smsc-address-restriction-type. Both commands must be configured for the SMS-C address denial
mechanism to function.

Example

Restrict MO-SMS messages from being forwarded to the SMS-C listed in the restriction list:

smsc-address-restriction-type mo-sms

Reset the restriction to both types of messages:

default smsc-address-restriction-type
**smsc-address-selection-prioritization**

Define the routing selection priority for the SMSC (short message service center) address to be used for all MO-SMS.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > MAP Service Configuration > SMS Service Configuration
configure > context context_name > map-service service_name > short-message-service

Entering the above command sequence results in the following prompt:

```
<context_name>host_name(config-map-service-service_name-sms-service)#
```

**Syntax**

```plaintext
smsc-address-selection-prioritization from-ms priority imsi-prefix priority msisdn-prefix priority

default smsc-address-selection-prioritization
```

**from-ms priority**

Configures a priority for the SMSC address send from the MS.

**priority** : Value must be a single digit, range 1-3.

**imsi-prefix priority**

Configures a priority for the SMSC address that is based on the IMSI-prefix.

**priority** : Value must be a single digit, range 1-3.

**msisdn-prefix priority**

Configures a priority for the SMSC address that is based on the MSISDN-prefix.

**priority** : Value must be a single digit, range 1-3.

**default**

By including the `default` keyword with the command, the SGSN knows to use the encoded default priorities for SMSC address selection for SMSC routing:

- `from-ms` priority 1,
- `imsi-prefix` priority 2,
- `msisdn-prefix` priority 3.

**Usage**

Use this command to define SMSC address routing priorities. Priorities must be defined for all parameters, all keywords, but they can be entered in any order. The addresses for the SMSCs are defined with the `smsc-routing` command.
An operator can use this configuration to prevent subscribers from using unauthorized SMSC addresses, for example, an unauthorized international SMSC.

**Example**

The keywords can be entered in any order but all keywords must be included in the command:

```
smisc-address-selection-prioritization msisdn-prefix 3 from-ms 1 imsi-prefix 2
```
smsc-routing

This command configures the routing to the short message service center (SMSC).

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > MAP Service Configuration > SMS Service Configuration

**Syntax**

```
[ no ] smsc-routing { { any | imsi-starts-with | msisdn-starts-with } { isdn isdn_number | mobile-global-title mgt_number [ max-gt-address-len max_gt_length ] | point-code pt_code } }
```

- **any**
  Configures routing according to any IMSI prefix.

- **imsi-starts-with** **IMSI_prefix**
  Defines the IMSI prefix. Enter a string of up to 15 digits.

- **msisdn-starts-with** **msisdn_prefix**
  Defines the MSISDN prefix. Enter a string of up to 15 digits.

- **isdn** **isdn_number**
  Defines the ISDN E.164 number (up to 15 digits) of the SMSC.

- **mobile-global-title** **mgt_number** [ **max-gt-address-len** max_gt_length ]
  Defines the mobile global title (MGT) E.214 address to be used for IMSI conversion. Optionally, the maximum length of the GT address can be defined. If the length of the MGT string is greater than the defined max, then the least significant digits will be omitted. **mgt_number** is a string of digits, up to 18 digits. **max_gt_address** is an integer from 1 to 32.

- **point-code** **pt_code**
  Defines the point code for the SMSC. Enter a string of up to 11 digits in SS7 dotted decimal or decimal format.
Usage

This command defines the address format (IMSI, point code, mobile global title) and the address for SMSC routing.

Example

Use this command to define routing to the SMSC based on any point code.

```
smsc-routing any point-code 1.222.1
```
timeout

This command defines the SMS service timers.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > MAP Service Configuration > SMS Service Configuration

`configure > context context_name > map-service service_name > short-message-service`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-map-service-service_name-sms-service)#
```

**Syntax**

```
timeout { tcln-timer time | trl1n-timer time | tr2n timer time }
```

```
default timeout { tcln-timer | trl1n-timer | tr2n timer }
```

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>default</code></td>
<td>Resets the configuration to the default value for the specified timer.</td>
</tr>
</tbody>
</table>
| `tcln-timer time` | Configures the TC1N timer in seconds.  
  `time`: Must an integer from 1 to 255. The default is 5 seconds. |
| `trl1n-timer time` | Configures the TR1N timer in seconds.  
  `time`: Must an integer from 1 to 255. The default is 30 seconds. |
| `tr2n-timer time` | Configures the TR2N timer in seconds.  
  `time`: Must an integer from 1 to 255. The default is 30 seconds. |

**Usage**

Use this command to set SMS service timers. The command can be repeated to set all of the timers, one-at-a-time.

**Example**

```
trl1n-timer 25
```
The SS7 Routing Domain configuration mode is used to configure Signaling System 7 (SS7) parameters. For convenience in configuration management, all SS7 parameters have been collected into a proprietary grouping called an SS7 routing domains.

Mode

Exec > Global Configuration > SS7 Routing Domain Configuration

configure > ss7-routing-domain routing_domain_id variant variant_type

Entering the above command sequence results in the following prompt:

[local]host_name(config-ss7-routing-domain-ss7rd_id)#

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
asp

This command creates or removes an M3UA Application Server Process (ASP) instance and enters the ASP configuration mode. See the SGSN ASP Configuration Mode chapter in the Command Line Interface Reference for command details.

Product
SGSN
HNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > SS7 Routing Domain Configuration
configure > ss7-routing-domain routing_domain_id variant variant_type

Entering the above command sequence results in the following prompt:

[local]host_name(config-ss7-routing-domain-ss7rd_id)#

Syntax

asp instance asp_inst
no asp instance asp_inst

default asp instance asp_inst end-point port

no
Deletes the ASP instance for the SS7 routing domain configuration.

default
Sets the ASP instance parameters to the end-point port value of 2905.

instance asp_inst
Identifies a specific ASP configuration. Up to four ASP instances can be configured for a single SS7 routing domain.

asp_inst: instance must be an integer from 1 through 4. For SGSN with release 15.0, the instance must be an integer from 1 to 12.

Usage
Use this command to create an ASP instance or enter the ASP configuration mode.

Example
The following command enters the ASP configuration mode for a specific ASP.

asp instance 1
**description**

This command defines an alphanumeric string that describes the current SS7 routing domain. This is used for operator reference only.

**Product**
- SGSN
- HNB-GW

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration > SS7 Routing Domain Configuration

```
configure > ss7-routing-domain routing_domain_id variant variant_type
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ss7-routing-domain-ss7rd_id)#
```

**Syntax**

```
description string

no description
```

- **no**
  - Removes the description string from the current SS7 routing domain configuration.

- **string**
  - Specifies the alphanumeric string that is stored. Strings with spaces must be enclosed in double-quotes (see the example below).
  - **string**: Must be from 1 to 255 alphanumeric characters.

**Usage**

Use this command to set a description for reference by operators.

**Example**

The following command sets the description to identify a routing domain for messages transmitted within a national boundary.

```
description "National Service Routing Domain"
```
end

Exits the current configuration mode and returns to the Exec mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

```plaintext
end
```

**Usage**

Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**
Use this command to return to the parent configuration mode.
inbound-asp-identifier validate

This command enables validation of ASP identifiers inbound to the SGSN via routes defined with this SS7 routing domain.

**Important:** This command is only available in Release 8.1 and higher releases.

**Product**
SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > SS7 Routing Domain Configuration

```
configure > ss7-routing-domain routing_domain_id variant variant_type
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ss7-routing-domain-ss7rd_id)#
```

**Syntax**

- `inbound-asp-identifier validate`
- `default inbound-asp-identifier validate`
- `no inbound-asp-identifier validate`

**Usage**

The standard is to validate the ASP Id. However, in some circumstances it is necessary to skip such validation. For example, if the same ASP Id is assigned to more than one RNC (peer-server).

**Example**

Use the following command to skip validation of inbound ASP IDs:

```
no inbound-asp-identifier validate
```

Use either of the following commands to enable validation if it has been disabled:

```
default inbound-asp-identifier validate
inbound-asp-identifier validate
```
linkset

This command creates an instance of an MTP3 linkset and enters the Linkset configuration mode. See the Linkset configuration mode chapter for the commands to configure the linkset.

Product
SGSN
HNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > SS7 Routing Domain Configuration
`configure > ss7-routing-domain routing_domain_id variant variant_type`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ss7-routing-domain-ss7rd_id)#
```

Syntax

```
linkset id id
no linkset id id
```

`no`

Removes the identified linkset definition from the system configuration.

`id`

This value uniquely identifies a linkset for the specific SS7 routing domain.

`id`: Must be an integer of 1 to 49.

Usage

This command creates instances of linkset configurations and provides access to the linkset configuration mode.

Example

Use the following command to create the 12th linkset:

```
linkset id 12
```
MTU-size

This command has been deprecated.
peer-server

This command creates a peer-server instance to setup a SIGTRAN peer for sending and receiving M3UA traffic. Completing the command automatically enters the peer-server configuration mode. To define 1 or more (up to 145) peer servers, use the commands documented in the Peer-Server Configuration Mode chapter in this reference.

Product
SGSN
HNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > SS7 Routing Domain Configuration

configure > ss7-routing-domain routing_domain_id variant variant_type

Entering the above command sequence results in the following prompt:

[local]host_name(config-ss7-routing-domain-ss7rd_id)#

Syntax

peer-server id srvr_id

no peer-server id srvr_id

no

Removes the identified peer-server definition from the system configuration.

srvr_id

srvr_id uniquely identifies a peer-server. The id must be an integer from 1 to 144. For SGSN Release 15.0, the id must be an integer from 1 to 256.

Usage
Use the following command to create a definition for peer-server 2 and enter the configuration mode to configure the communication parameters for peer-server 12.

Example

peer-server id 12
route

This command configures SS7 routes for the current SS7 routing domain.

Product
SGSN
HNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > SS7 Routing Domain Configuration
configure > ss7-routing-domain routing_domain_id variant variant_type

Entering the above command sequence results in the following prompt:

[local]host_name(config-ss7-routing-domain-ss7rd_id)#

Syntax

route destination-point-code dp_code { linkset id id [ priority pri_value ] | peer-server-id srvr_id }

no route destination-point-code dp_code { linkset id id | peer-server-id srvr_id }

no

Removes the SS7 route from the current SS7 routing domain configuration.

destination-point-code dp_code

Specifies the SS7 destination point code for this route.
Reminder: the point-code structure must match the variant defined for the SS7 routing domain when the SS7RD was configured in the global configuration mode.

linkset id id

This keyword identifies a linkset instance, created and configured with the linkset command.
This keyword identifies a linkset instance, created and configured with the linkset command.
id: Must be an integer from 1 to 49.

peer-server-id srvr_id

This keyword identifies a peer-server configuration instance, created and configured with the peer-server command.
srvr_id must be an integer from 1 to 49.

Usage

This command associates the previously configured linksets and peer servers and the destination point codes with a specified SS7 route.

Example

Define a route setting an ITU-type destination point-code address for the linkset Id 12:
route destination-point-code 6.211.6 linkset id 12
routing-context

Identifies the routing context for this SS7 routing domain.

Product
SGSN
HNB-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > SS7 Routing Domain Configuration
configure > ss7-routing-domain routing_domain_id variant variant_type

Entering the above command sequence results in the following prompt:
[local]host_name(config-ss7-routing-domain-ss7rd_id)#

Syntax
routing-context value
default routing-context

default
Resets the local routing context value to the index (instance ID) for this SS7 routing domain.

value
An integer that uniquely identifies the routing context for this SS7 routing domain.
value: Must be integers from 1 to 65535 (for releases 8.0) or 1 to 4294967295 (for releases 8.1 to 17.0) or 0 to 4294967295 (for releases 17.1 and higher).

Usage
Use this command to set the routing context IDs for a specific SS7 routing domain configuration.

Example
routing-context 2355
This command sets the network indicator in the subservice field for SS7 message signal units (MSUs).

**Product**
SGSN
HNB-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > SS7 Routing Domain Configuration

`configure > ss7-routing-domain routing_domain_id variant variant_type`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-ss7-routing-domain-ss7rd_id)#
```

**Syntax**

```
ssf ( international | national | reserved | spare )
```

---

**international**
The network indicator identifies the message as international with a point code structure that does not match the national point code structure.

---

**national**
The network indicator identifies the messages as having a national point code structure.

---

**reserved**
Provides an alternate network indicator for national messages.

---

**spare**
Provides an alternate network indicator for international messages.

**Usage**
In SS7 signaling, the Message Transfer Part (MTP) Level 2 message signal units (MSUs) contain a service information octet (SIO). The SIO field in an MSU contains a 4-bit subservice field (SSF) followed by a 4-bit service indicator. The indicator carried in the message’s routing information typically identifies the structure of the point code as a message from within a nation or as a message coming from outside the nation - international. As well, the 4-bit SSF determines the point code structure of the messages transmitted from the SGSN.

**Example**
For messages being transmitted within a country, set the indicator to national with the following command.

```
ssf national
```
Chapter 289
SSH Configuration Mode Commands

The Secure Shell Configuration Mode is used to manage the SSH server options for the current context.

**Important:** You must use the `ssh generate key` command in Context Configuration Mode to generate the sshd keys before you can configure the sshd server.

**Mode**

Exec > Global Configuration > Context Configuration > SSH Configuration

`configure > context context_name > server sshd`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sshd)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
**authorized-key**

Sets or removes a user name having authorized keys for access to the sshd server in the current context.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > SSH Configuration

```
configure > context context_name > server sshd
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-sshd)#
```

**Syntax**

```
authorized-key username user_name host host_name [ type { v2-dsa | v2-rsa } ]
```

- **default**
  Resets the parameter to the default value.

- **username**
  Sets a username as having authorized keys for access to the sshd server.

- **user_name**
  Specifies the username entered as an alphanumeric string of 1 through 255 characters.

- **host**
  Associates an SSH host having the authorization keys for the username.

- **host_name**
  Specifies the host name entered as an alphanumeric string of 1 through 255 characters.

  [ type { v2-dsa | v2-rsa } ]

  Specifies which type of SSH authorization key will be accepted instead of all key types. The options are: `v2-dsa` (SSHv2 Digital Signature Algorithm), or `v2-rsa` (SSHv2 Rivest, Shamir and Adleman).

**Usage**

Use this command to set a username with authorized keys for access to the sshd server within the current context.

**Important:** Only 10 sshd authorization-keys can be configured per context.
Example

The following command specifies that username *dbailey* with authorization keys at *sshserver* can access the system with all types of authorization keys:

```
authorized-key username dbailey host sshserver
```
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

```
exit
```

Usage
Use this command to return to the parent configuration mode.
listen

Configures the SSH server in the current context to only listen for connections from the interface with the specified IP address. The default behavior is to listen on all interfaces.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > SSH Configuration

configure > context context_name > server sshd

Entering the above command sequence results in the following prompt:

[local]host_name(config-sshd)#

**Syntax**

```plaintext
listen ip_address

no listen

no

Disable listening for a specific interface address and enable listening on all interfaces.

ip_address

Enables listening only on the interface with the specified IP address. ip_address must be entered using IPv4 dotted-decimal notation.
```

**Usage**

Use this command to configure the SSH server for the current context to only listen for connections from the interface with the specified IP address. Only one IP address may be set for listening.

**Example**

The following command specifies that the Server should only listen for connections in the interface with the IP address of 192.168.0.10:

```plaintext
listen 192.168.0.10
```
max servers

Configures the maximum number of SSH servers that can be started within any 60-second interval. If this limit is reached, the system waits two minutes before trying to start any more servers.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > SSH Configuration

configure > context context_name > server sshd

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-sshd)#
```

**Syntax**

```
max servers number
```

- **number**

  Default: 40

  Specifies the maximum number of servers that can be spawned in any 60-second interval. *number* must be an integer from 1 through 100.

**Usage**

Set the number of servers to tune the system response as a heavily loaded system may need more servers to support the incoming requests.

The converse would be true as well in that a system can benefit by reducing the number of servers such that telnet services do not cause excessive system impact to other services.

**Example**

```
max servers 50
```
subsystem

Configures the system to perform file transfers using Secure FTP (SFTP) over ssh v2. Administrators must be configured with the FTP attribute privilege to issue this command.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > SSH Configuration
configure > context context_name > server sshd

Entering the above command sequence results in the following prompt:

[local]host_name(config-sshd)#

Syntax

subsystem { cli | sftp }

no subsystem { cli | sftp }

no

Disables the SFTP ssh file transfer method or access to the CLI via ssh.

cli

Default: Enabled
Configures the SSH system for the current context to allow access to the CLI.

sftp

Default: Disabled
Enables the SSH system for the current context to perform file transfers using Secure FTP (SFTP) over ssh v2.

Usage

Use this command to enable or disable file transfers using SFTP over an ssh v2 tunnel. Also use this command to enable or disable access to the CLI over an SSH connection.

Example

The following command enables SFTP for the current context:

subsystem sftp

The following command disables access to the CLI through an SSH session for the current context:

no subsystem cli
Chapter 290
Subscriber Configuration Mode Commands

The Subscriber Configuration Mode is used to create local subscribers as well as to set default subscriber options for the current context.

Mode

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context context_name > subscriber { default | name subscriber_name }

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-subscriber)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
aaa

This command configures authentication, authorization and accounting (AAA) functionality at the subscriber level.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context context_name > subscriber { default | name subscriber_name }

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-subscriber)#

Syntax

[ no ] aaa { accounting interim { interval-timeout interval_timeout | normal | suppress } | group aaa_group_name | secondary-group aaa_secondary_group_name }

default aaa { accounting interim [ interval-timeout ] | group | secondary-group }

no aaa { accounting interim [ interval-timeout ] | group [ aaa_group_name ] | secondary-group }

default

Configures the default setting for the specified parameter.

• accounting: Enables AAA accounting for subscribers.

• group: Uses the default AAA group—the one specified at the context level or in the default subscriber profile.

• secondary-group: Removes the secondary AAA group from the subscriber configuration.

no

• accounting: Disables AAA accounting for subscribers.

• group: Uses the default AAA group—the one specified at the context level or in the default subscriber profile.

• secondary-group: Removes the secondary AAA group from the subscriber configuration.

accounting interim { interval-timeout interval_timeout | normal | suppress }

Specifies when system should send an interim accounting record to the server.

• interval-timeout: Specifies the time interval (in seconds) at which to send an interim accounting record.

  interval_timeout must be an integer from 50 through 40000000.

• normal: If RADIUS accounting is enabled, send this Acct-Status-Type message when normally required by operation.

• suppress: If RADIUS accounting is enabled, suppress the sending of Acct-Status-Type message.
group aaa_group_name
Specifies the AAA server group for the subscriber for authentication and/or accounting.
aaa_group_name must be an alphanumeric string of 1 through 63 characters.

secondary-group aaa_secondary_group_name
Specifies the secondary AAA server group for the subscriber.
aaa_secondary_group_name must be an alphanumeric string of 1 through 63 characters.

Usage
Use this command to configure AAA functionality at the subscriber level.
Instead of having a single list of servers per context, this feature configures multiple server groups within a context and applies individual server group for subscribers in that context. Each server group consists of a list of AAA servers for each AAA function (accounting, authentication, charging, etc.).
The AAA secondary server group supports the No-ACK RADIUS Targets feature in conjunction with PDSN/HA for secondary accounting (with different RADIUS accounting group configuration) to the RADIUS servers without expecting the acknowledgement from the server, in addition to standard RADIUS accounting. This secondary accounting will be an exact copy of all the standard RADIUS accounting message (RADIUS Start/Interim/Stop) sent to the standard AAA RADIUS server.
If the same AAA group is configured with both the aaa group aaa_group_name and the aaa secondary-group aaa_group_name commands, then this configuration will have no effect and secondary accounting will not happen.
The AAA secondary server group configuration takes effect only when used with subscriber accounting-mode set to radius-diameter. The RADIUS accounting triggers for both standard RADIUS accounting and secondary accounting will be taken from the AAA group configured with the aaa group aaa_group_name command. On the fly change of this configuration is not supported. Any change to the configuration will have effect only for new calls.

Example
The following command applies the AAA server group star1 to subscribers:

    aaa group star1
**access-link ip-fragmentation**

Configures IP fragmentation processing over the Access-link.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Subscriber Configuration
```
configure > context context_name > subscriber { default | name subscriber_name }
```

Entering the above command sequence results in the following prompt:
```
[context_name]host_name(config-subscriber)#
```

**Syntax**
```
access-link ip-fragmentation { normal | df-ignore | df-fragment-and-icmp-notify }
```

---

**df-ignore**
Default: Enabled
Ignores the DF (Don’t Fragment) bit setting. Fragments and forwards the packet over the access link.

---

**df-fragment-and-icmp-notify**
Default: Disabled
Partially ignores the DF bit. Fragments and forwards the packet, but also returns an ICMP error message to the source of the packet. The number of ICMP errors sent like this is rate-limited to one ICMP error packet per second per session.

---

**normal**
Default: Disabled
Normal processing. Drops the packet and sends an ICMP unreachable message to the source of packet. This is the default behavior.

---

**Usage**
If the IP packet to be forwarded is larger than the access-link MTU and if the DF (Don't Fragment) bit is set for the packet, then the fragmentation behavior configured by this command is applied. Use this command to fragment packets even if they are larger than the access-link MTU.

**Example**
Set fragmentation so that the DF bit is ignored and the packet is forwarded anyway by entering the following command:
```
access-link ip-fragmentation df-ignore
```
accounting-mode

Sets the accounting mode for the current local subscriber configuration.

Product
PDSN
HA
ASN-GW
SAEGW
S-GW

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context context_name > subscriber { default | name subscriber_name }

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-subscriber)#

Syntax

accounting-mode { flow-based | gtp [ radius-diameter ] | none | radius-diameter [ gtp ] | rf-style }

default accounting-mode

---

Sets the type of accounting to be performed for the current local subscriber to the default setting.
Default: radius-diameter

---

flow-based

Diameter flow-based accounting is enabled for the current local subscriber.

---

gtp [ radius-diameter ]

GTPP CDR RADIUS accounting is enabled for the current local subscriber. The radius-diameter keyword is available if both GTPP RADIUS and RADIUS-Diameter accounting are to be used.

---

none

Accounting is disabled for the current local subscriber and no charging records will be generated.

---

radius-diameter [ gtp ]

RADIUS-Diameter accounting is enabled for the current local subscriber. The gtp keyword is available if both GTPP RADIUS and RADIUS-Diameter accounting are to be used.
rf-style
Diameter Rf interface accounting is enabled for the current local subscriber.

Usage
This command specifies which protocol, if any, will be used to provide accounting for PDP contexts accessing the APN profile.
Use this command to enable or disable RADIUS/Diameter accounting for any subscribers that use the current local subscriber configuration.
If the gtpp option is used, then GTPP RADIUS is used as configured in the Context Configuration mode or the AAA Server Group Configuration mode and GTPP charging records will be enabled.
If the radius-diameter option is used, either the RADIUS or the Diameter protocol is used as configured in the Context Configuration mode or the AAA Server Group Configuration mode.
RADIUS accounting can also be enabled and disabled at the context level with the aaa accounting command in the Context Configuration Mode. If RADIUS accounting is enabled at the context level, the accounting-mode command can be used to disable RADIUS accounting for individual local subscriber configurations.
If the accounting mode is set to rf-style, then BM will generate accounting records corresponding to AIMS RF.

Example
To disable accounting for the current subscriber, enter the following command:

    accounting-mode none
active-charging bandwidth-policy

Configures the bandwidth policy to be used for the subscriber.

**Product**  
ACS

**Privilege**  
Security Administrator, Administrator

**Mode**  
Exec > Global Configuration > Context Configuration > Subscriber Configuration

```
configure > context context_name > subscriber { default | name subscriber_name }
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

**Syntax**

```
active-charging bandwidth-policy bandwidth_policy_name
{ default | no } active-charging bandwidth-policy
```

---

**default**

Specifies that the default bandwidth policy configured in the rulebase be used for this subscriber.

---

**no**

Disables bandwidth control for this subscriber.

---

```
active-charging bandwidth-policy bandwidth_policy_name
```

Specifies name of the bandwidth policy.

*bandwidth_policy_name* must be an alphanumeric string of 1 through 63 characters.

---

**Usage**

Use this command to configure bandwidth policy to be used for subscribers.

**Example**

The following command configures a bandwidth policy named *standard* for the subscriber:

```
active-charging bandwidth-policy standard
```
active-charging link-monitor tcp

Enables the TCP link monitoring feature on the Mobile Video Gateway. This command can be configured in either APN Configuration Mode or Subscriber Configuration Mode.

Product
MVG

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context context_name > subscriber { default | name subscriber_name }

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-subscriber)#

Syntax


default
Sets TCP link monitoring to its default value, which is the same as [ no ].

no
Deletes the TCP link monitoring settings and disables TCP link monitoring if previously configured.

active-charging link-monitor tcp

Enables the TCP link monitoring feature on the Mobile Video Gateway. Note that TCP link monitoring is not enabled by default. Also note that when this command is configured without the log option, TCP link monitoring is enabled without logging, and the output from TCP link monitoring is only used by the dynamic translating feature.

log [ rtt [ histogram | time-series ] ] [ bitrate [ histogram | time-series ] ] [ rtt [ histogram | time-series ] ]

This option enables statistical logging for TCP link monitoring.
The rtt option can be used to enable either histogram or time-series logging for round-trip time (RTT).
Similarly, the bitrate option can be used to enable either histogram or time-series logging for bit rate.
When rtt and bitrate options are used without additional options, histogram and time-series logging are enabled for round-trip time (RTT) and/or bit rate respectively.

-noconfirm
Specifies that the command must execute without prompting for confirmation.
Usage

Use this command to enable TCP link monitoring on the Mobile Video Gateway.

Examples

The following command enables TCP link monitoring with statistical logging, with histogram and time-series logging enabled for both RTT and bit rate:

```
active-charging link-monitor tcp log
```

The following command enables TCP link monitoring with statistical logging, with histogram and time-series logging enabled for RTT:

```
active-charging link-monitor tcp log rtt
```

The following command enables TCP link monitoring with statistical logging, with histogram logging enabled for RTT:

```
active-charging link-monitor tcp log rtt histogram
```

The following command enables TCP link monitoring with statistical logging, with histogram logging enabled for RTT and time-series logging enabled for bit rate:

```
active-charging link-monitor tcp log rtt histogram bitrate time-series
```
active-charging rulebase

Specifies the rulebase to be used for this subscriber.

**Product**
ACS

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Subscriber Configuration
configure > context context_name > subscriber { default | name subscriber_name }

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

**Syntax**

- `active-charging rulebase rulebase_name`
- `no active-charging rulebase`
- `no

  Removes the previously configured rulebase for the subscriber.

  `active-charging rulebase rulebase_name`

  Specifies name of the ACS rulebase.

  `rulebase_name` must be the name of an ACS rulebase expressed as an alphanumeric string of 1 through 63 characters.

**Usage**

This command specifies the name of the rulebase for specific subscriber (reals).
If the specified rulebase does not exist in the Active Charging service, the call will be rejected.

**Example**

The following command configures the ACS rulebase named `rule1` for the subscriber:

```
active-charging rulebase rule1
```
always-on

Once the idle timeout limit is reached, keeps the current subscriber session connected as long as the subscriber is reachable.

⚠️ Caution: When always-on is enabled, the subscriber must have an idle time-out period configured (default is 0, no time-out). Failure to configure an idle time-out results in a subscriber session that is indefinite.

Two timers and a counter are associated with this feature. Refer to the `timeout` command in this chapter and the `ppp echo-retransmit-timeout msec` and `ppp echo-max-retransmissions num_retries` commands.

Default: Disabled.

**Product**
PDSN
ASN-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Subscriber Configuration
`configure > context context_name > subscriber { default | name subscriber_name }`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

**Syntax**

```
always-on
no always-on
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>always-on</td>
<td>Specifies that the user will remain connected after the idle time expires.</td>
</tr>
<tr>
<td>no always-on</td>
<td>Disables always-on. The user is disconnected after the idle time expires.</td>
</tr>
</tbody>
</table>

**Usage**

If this parameter is enabled for a subscriber, when the idle time-out limit is reached the subscribers IP/PPP session remains connected as long as the subscriber is reachable. This is true even if the airlink between the mobile device and the RN (Radio Node) is moved from active to dormant (inactive) status. When the idle timeout limit is reached, the PDSN determines availability using link control protocol (LCP) keepalive messages. A response to these messages indicates that the “always-on” status should be maintained. Failure to respond to a predetermined number of LCP keepalive messages causes the PDSN to tear-down (disconnect) the subscriber session.

**Example**

Enable always on for the current subscriber by entering the following command:
always-on

always-on
asn-header-compression-rohc

Negotiates Robust Header Compression (ROHC) support for subscriber calls with AAA and WiMAX. This configuration indicates the type of header compression supported and enabled on the ASN.

Product
ASN-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Subscriber Configuration
configure > context context_name > subscriber { default | name subscriber_name }

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-subscriber)#

Syntax

[ no | default ] asn-header-compression rohc

---
no

Removes or disables the configured identifiers for ROHC in ASN-GW service.

---
default

The default is disabled.

Usage

Network Attached Storage (NAS) uses this configuration to indicate and pack ROHC support the subscriber TLV in the WiMAX-capability attribute in the Access Request. The ROHC header compression is applied only when the ROHC is supported on the ASNGW and ROHC support is indicated by the AAA.
**asn nspid**

Specifies the network service provider (NSP) associated with a WiMAX subscriber in an ASN-GW service. When configured, the NSP ID is sent in the Access-Request and Accounting messages.

**Product**
ASN-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Subscriber Configuration

```configure > context context_name > subscriber { default | name subscriber_name }
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

**Syntax**

```
[ no ] asn nspid nsp_id
```

**no**
Removes or disables the configured identifiers for this network service provider in ASN-GW service.

```
asn nspid nsp_id
```

Specifies the network service provider for this subscriber. This enables the MS to discover all accessible NSPs, and to indicate the NSP selection during connectivity to the ASN.

**Usage**

Use this command to specify the NSP associated with a subscriber in an ASN-GW service.

`nsp_id` is three bytes in hexadecimal format. For example: FF-EE-01

**Example**

The following command specifies the NSP for a subscriber in an ASN service:

```
asn nspid 0F-01-FE
```
## asn-pdfid

Configures the identifiers for packet data flow, service data flow, and service profile in an ASN-GW service.

### Product
ASN-GW

### Privilege
Security Administrator, Administrator

### Mode
Exec > Global Configuration > Context Configuration > Subscriber Configuration

```
configure > context context_name > subscriber { default | name subscriber_name }
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

### Syntax

```
[ no ] asn-pdfid pdf_id asn-service-profile-id svc_profile_id asn-sdfid sdf_id
```

- **no**
  - Removes/disables the configured identifiers for this subscriber in ASN-GW service.

- **asn-pdfid pdf_id**
  - Specifies the an unique ASN Packet Data Flow identifier for this subscriber.
    - `pdf_id` must be an integer from 1 through 65535.

- **asn-service-profile-id svc_profile_id**
  - Specifies a unique ASN Service Profile Identifier for this subscriber.
    - `svc_profile_id` is a Service Profile Identifier configured in the Context Configuration Mode.

- **asn-sdfid sdf_id**
  - Specifies the an unique ASN Service Data Flow identifier for this subscriber.
    - `sdf_id` must be an integer from 1 through 65535.

### Usage

Use this command to configure subscriber profile for QoS parameters in an ASN-GW service. A maximum of four QoS profiles can be configured for a subscriber.

### Example

The following command configures the QoS profile for a subscriber as PDF id 1, Service Profile id 3, and Service Data Flow id 2:

```
asn-pdfid 1 asn-service-profile-id 3 asn-sdfid 2
```
asn-policy

Configures the identifiers for packet data flow, service data flow, and service profile in an ASN-GW service.

**Product**

ASN-GW

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

```bash
configure > context context_name > subscriber { default | name subscriber_name }
```

Entering the above command sequence results in the following prompt:

```bash
[context_name]host_name(config-subscriber)#
```

**Syntax**

```bash
asn-policy [classifiers downlink { strict | loose} | idle-mode { allow | disallow } | notification-idle-mode {allow | disallow} | notification-handoff { allow | disallow } | auth-only {allow | disallow } | ms-requested-classifiers {allow | dissalow}]
[ default ] asn-policy classifiers downlink idle-mode
no
```

- Removes or disables the configured policy for this subscriber in ASN-GW service.
- **default**
  
  Sets the ASN policy to default for this subscriber.
  For downlink traffic classifier default policy is “loos” and for idle mode policy the default action is to allow idle mode operation in an ASN-GW service.

- **idle-mode**
  
  Sets the idle mode policy for this subscriber in an ASN-GW service. If enabled, Interim-Update is sent with the BSID and WiMAX-Idle_Mode_Transition as Idle. If disabled, the Interim can be sent when the call is in the idle mode based on the interim timer. At this point, the last known BSID is reported to the RADIUS server.

- **notification-idle-mode**
  
  Default: allow
  Use to enable or disable Idle-Mode-Notification capabilities. When you enable this command, when the call moves from active to idle, or idle to active, Accounting Interim is sent.

- **notification-handoff**
  
  Default: allow
  If enabled, the Interim-Update is sent with the BSID and SN-Handoff-Indicator as Active Handoff.
allow
Default: enabled
Enables the policy for this subscriber to allow idle mode operation in an ASN-GW service.

disallow
Default: disabled
Enable the policy for this subscriber to disallow idle mode operation in an ASN-GW service.

classifiers downlink
Sets the classifier policy for all service flows coming from HA to FA for this subscriber’s matching classifier.

strict
Default: disabled
This option discards all the service flows coming from HA to FA and any other packets not matching to any of the classifiers set for this subscriber.

loose
Default: enabled
This option allows all the service flows coming from HA to FA and any other packet does not matching to any of the classifiers set for this subscriber and sent to the BS/MS over downlink flow

auth-only
Specifies whether the call is Auth only or not.

allow
Enables the policy for this subscriber to allow auth-only in an ASN-GW service.

disallow
Default
Disables the policy for this subscriber to allow auth-only in an ASN-GW service.

ms-requested classifiers
Default: allow
By default ASNGW allows dynamic addition of classifiers by the MS during MS-initiated service flow creation or modification.

Usage
Use this command to configure subscriber policy to allow/disallow the idle mode operation or the downlink traffic flow for a subscriber in an ASN-GW service.
For authentication configuration, the ASN-GW supports the Initial Network Entry (INE) for Ethernet CS calls. The base station supports Ethernet CS traffic to the network. The INE procedure includes the Authentication of the service flows and IP-Address allocation through DHCP. Authentication is based on the Extensible Authentication Protocol (EAP).
This command allows MS to transition to idle mode with an ASN-GW.

Example
The following command configures the policy to allow the idle mode for an MS with an ASN-GW:
default asn-policy idle-mode
associate accounting-policy

Associates the subscriber with specific pre-configured policies configured in the same context.

Product
- P-GW
- SAEGW

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > Subscriber Configuration

```
configure > context context_name > subscriber { default | name subscriber_name }
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber) #
```

Syntax

```
[ no ] associate accounting-policy name
```

- **no**
  - Removes the selected association from this subscriber.

- **name**
  - Associates the subscriber with an accounting policy configured in the same context.
  
  *name* must be an existing accounting policy expressed as a string of 1 through 63 characters.

  Accounting policies are configured through the `policy accounting` command in the Context Configuration mode.

Usage

Use this command to associate the subscriber with an accounting policy configured in this context.

Example

The following command associates this subscriber with an accounting policy called `acct1`:

```
associate accounting-policy acct1
```
authorized-flow-profile-id

When a profile ID is requested by the Mobile Node (MN), this command sets the value that is authorized by the Access Gateway (AGW).

Product
- PDSN
- ASN-GW

Privilege
Security Administrator, Administrator

Mode
- Exec > Global Configuration > Context Configuration > Subscriber Configuration
- configure > context context_name > subscriber { default | name subscriber_name }

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-subscriber)#

Syntax

authorized-flow-profile-id profile_id direction { bidirectional | forward | reverse }

no authorized-flow-profile-id profile_id

no

Removes the existing profile ID setting specified by profile_id.profile_id must be an integer from 0 through 65535.

authorized-flow-profile-id profile_id

The profile ID number that is authorized for the current subscriber. profile_id must be an integer from 0 through 65535.

direction { bidirectional | forward | reverse }

This specifies in which data direction the profile ID should be applied.

- bidirectional: This profile ID pertains to both the forward and reverse directions.
- forward: This profile ID pertains to data going to the MN.
- reverse: This profile ID pertains to data coming from the MN.

Usage
Use this command to set the profile ID that the AGW will authorize for a subscriber.

Example
Set the profile ID for both directions to 3 for the current subscriber by entering the following command:

authorized-flow-profile-id 3 direction bidirectional
content-filtering category

Enables or disables the specified preconfigured Category Policy Identifier for policy-based Content Filtering support to the subscriber.

**Product**
CF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Subscriber Configuration
configure > context context_name > subscriber { default | name subscriber_name }

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

**Syntax**

```
content-filtering category policy-id cf_policy_id

no content-filtering category policy-id
```

**no**
Disables the configured category policy ID for content filtering support to the subscriber. This is the default setting.

**content-filtering category policy-id cf_policy_id**

Applies the content filtering category policy ID, configured in ACS Configuration Mode, to this subscriber. *cf_policy_id* must be a category policy ID expressed as an integer from 1 through 4294967295.
If the specified category policy ID is not configured in the ACS Configuration Mode, all packets will be passed regardless of the categories determined for such packets.

**Important:** Category Policy ID configured through this mode overrides the Category Policy ID configured using the `content-filtering category policy-id` command in the ACS Rulebase Configuration Mode.

**Usage**
Use this command to enter the Content Filtering Policy Configuration Mode and enable or disable the Content Filtering Category Policy ID for a subscriber.

**Important:** If Content Filtering Category Policy ID is not specified here, the similar command in the ACS Rulebase Configuration Mode determines the policy.

**Example**
Up to 64 different policy identifier can be defined in a Content Filtering support service.

The following command enters the Content filtering Policy Configuration Mode and enables the Category Policy ID 101 for Content Filtering support:
content-filtering category policy-id 101
credit-control-client

Configures the credit-control client parameters for the subscriber.

Product
- GGSN
- HA
- IPSG
- PDSN
- P-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Subscriber Configuration
configure > context context_name > subscriber { default | name subscriber_name } 

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-subscriber)#

Syntax
credit-control-client { event-based-charging | override session-mode { per-sub-session | per-subscriber } } 

no credit-control-client { event-based-charging | override session-mode }

default credit-control-client event-based-charging

no
Disables the configured setting.

default
Resets the command to its default setting of disabled.

event-based-charging
Enables event-based charging.

override session-mode { per-sub-session | per-subscriber }

Overrides the session-mode configured through the CLI command “require ecs credit-control session-mode per-subscriber” in Global Configuration mode so that different subscriber groups can operate in different modes. For example, one subscriber group can be configured to work in per-subscriber mode, while another in per-sub-session mode. This keyword is used to switch between subscriber level Gy and sub-session level Gy.
**Important:** This CLI can be changed on the fly. The modified values will be reflected only in the new subscriber session.

The `no` command removes the override CLI and makes the subscriber group fall back to the configuration specified through the CLI command “`require ecs credit-control session-mode per-subscriber`”.

**Usage**

Use this command to configure the credit-control client parameters for the subscriber. This configuration should be enabled to report UE’s PLMN, timezone and ULI changes through Event-based-Gy session. In the event that both Gy Online charging and Gy event reporting are enabled, the P-GW shall send only CCR-Update requests to the OCS and shall not send CCR-Event requests.

With the inclusion of this keyword `override session-mode` ... in 14.1 release, it is possible to seamlessly change the configuration from bearer level to subscriber level and vice-versa without requiring a system reboot.

**Example**

The following command enables event-based Gy support for the subscriber:

```
credit-control-client event-based-charging
```
credit-control-group

Configures the credit-control group for this subscriber.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Subscriber Configuration
configure > context context_name > subscriber { default | name subscriber_name }

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-subscriber)#

Syntax

credit-control-group cc_group_name

no credit-control-group

_____________________________

no

Removes the credit-control group from the subscriber configuration, if configured.

_____________________________

credit-control-group cc_group_name

Specifies name of the credit-control group.

cc_group_name must be an alphanumeric string of 1 through 63 characters.

Usage

Use this command to configure the credit-control group for the subscriber.

Example

The following command configures the credit-control group named test12 for the subscriber:

    credit-control-group test12
credit-control-service

Configures the credit-control service for this subscriber.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Subscriber Configuration
configure > context context_name > subscriber { default | name subscriber_name }

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-subscriber)#

Syntax

[ no ] credit-control-service cc_service_name

__no__
Disables the credit-control service, if configured.

credit-control-service cc_service_name
Specifies the name of the credit-control service.
cc_service_name must be an alphanumeric string of 1 through 63 characters.

Usage
Use this command to configure the credit-control service for subscribers.

Example
The following command configures the credit-control service named test12 for the subscriber:

credit-control-service test12
cscf core-service

CSCF/A-BG core service that maps to the current domain.

Product
SCM (CSCF, A-BG)

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context context_name > subscriber { default | name subscriber_name }

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-subscriber)#

Syntax

```
cscf core-service name name

no cscf core-service
```

```
cscf core-service name name

Specifies the name of the CSCF/A-BG core service.
name must be an alphanumeric string of 1 through 63 characters.

no cscf core-service

Removes the CSCF/A-BG core service from the domain.
```

Usage

Use this command to map a CSCF/A-BG core service to the current domain.

Example

The following command creates a CSCF core service named cs1:

```
cscf core-service name cs1
```

The following command removes the CSCF core service from this domain:

```
o cscf core-service
```
cscf county-name

Assigns a Last Routing Option (LRO) profile county name to the subscriber for finding the correct Public Safety Answering Point (PSAP) during emergency calls.

Product
SCM (S-CSCF)

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context context_name > subscriber { default | name subscriber_name }

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-subscriber)#

Syntax

[ no ] cscf county-name name

---

cscf county-name name

Specifies the LRO profile county name of the subscriber.

name must be an existing LRO profile county name expressed as an alphanumeric string of 1 through 127 characters.

no

Removes the LRO profile county name from the subscriber.

---

Usage

Use this command to assign an LRO profile county name to the subscriber.

Example

The following command assigns county name norfolk to the subscriber:

    cscf county-name norfolk

The following command removes county name norfolk from the subscriber:

    no cscf county-name norfolk
cscf nat-applicable

Indicates if NAT (Network Address Translation) processing is required for this domain.

Product
SCM (CSCF/A-SBC)

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Subscriber Configuration

**configure > context context_name > subscriber { default | name subscriber_name }**

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax

```
[ no ] cscf nat-applicable
```

---

no

Disables NAT processing for this domain.

---

cscf nat-applicable

Enables NAT processing for this domain.

---

Usage

Use this command to indicate whether NAT processing is required for this domain.

Example

The following command indicates NAT processing is required for this domain:

```
cscf nat-applicable
```

The following command disables NAT processing for this domain:

```
no cscf nat-applicable
```
cscf private-user-id

Assigns a private user identity to the subscriber.

**Product**
SCM (P-CSCF, S-CSCF, SIP Proxy)

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Subscriber Configuration

```
configure > context context_name > subscriber { default | name subscriber_name }
```

Entering the above command sequence results in the following prompt:

```
[context_name] host_name(config-subscriber)#
```

**Syntax**

```
[ no ] cscf private-user-id user_id
```

- **no**
  Removed the private user identity of the subscriber.

- **cscf private-user-id user_id**
  Specifies the private user identity of the subscriber.
  *user_id* must be an alphanumeric string of 1 through 127 characters.

**Usage**

Use this command to assign a private user identity to the subscriber.

**Example**

The following command assigns a private user identity named *user007* to the subscriber:

```
cscf private-user-id user007
```

The following command removes private user identity named *user007* from the subscriber:

```
no cscf private-user-id user007
```
cscf session-template

Assigns a CSCF session template to the subscriber profile.

**Product**
SCM (P-CSCF, S-CSCF, SIP Proxy)

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Subscriber Configuration

```plaintext
configure > context context_name > subscriber { default | name subscriber_name }
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

**Syntax**

```plaintext
cscf session-template name name

no cscf session-template
```

**Usage**

Use this command to bind a CSCF session template to a subscriber profile.

**Example**

The following command assigns a CSCF session template named `template4` to the subscriber profile:

```
cscf session-template name template4
```

The following command removes the assignment of a session template to the subscriber profile:

```
no cscf session-template
```
data-tunneling ignore df-bit

Controls the handling of the DF (Don't Fragment) bit present in the user IPv4/IPv6 packet for GRE, IP-in-IP tunneling used for the MIP data path. If this feature is enabled, and fragmentation is required for the tunneled user IPv4/IPv6 packet, then the DF bit is ignored and the packet is fragmented. Also the DF bit is not copied to the outer header. Default is enabled.

Product
PDSN
HA
FA
ASN-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Subscriber Configuration
configure > context context_name > subscriber { default | name subscriber_name }

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-subscriber)#

Syntax

data-tunneling ignore df-bit

no data-tunneling ignore df-bit

no

Disables this option. The DF bit in the tunneled IP packet header is not ignored during tunneling.

data-tunneling ignore df-bit

Ignores the DF bit in the tunneled IP packet header.

Usage

Use this command to configure a user so that during Mobile IP tunneling the DF bit is not ignored and packets are not fragmented.

Example

To disable fragmentation of a subscribers packets over a MIP tunnel even when the DF bit is present, enter the following command:

no data-tunneling ignore df-bit
**dcca origin host**

This command is obsolete. Refer to the `dcca origin endpoint` command.
dcca origin endpoint

This command is obsolete. To configure the Diameter Credit Control Origin Endpoint, in the Credit Control Configuration Mode, use the diameter origin endpoint command.
dcca peer-select

Specifies the Diameter credit control primary and secondary peer for credit control.

**Product:**
ACS

**Privilege:**
Security Administrator, Administrator

**Mode:**
Exec > Global Configuration > Context Configuration > Subscriber Configuration

```cpp
configure > context context_name > subscriber { default | name subscriber_name }
```

Entering the above command sequence results in the following prompt:

```plaintext
[context_name]host_name(config-subscriber)#
```

**Syntax**

```cpp
dcca peer-select peer host_name [ realm realm_name ] [ secondary-peer host_name [ realm realm_name ] ]
```

```cpp
no dcca peer-select
```

- **no**
  Removes the previously configured Diameter credit control peer selection.

- **peer host_name**
  Specifies a unique name for the peer. `peer_name` must be an alphanumeric string of 1 through 63 characters that allows punctuation marks.

- **secondary-peer host_name**
  Specifies a back-up host that is used for fail-over processing. When the route-table does not find an available route, the secondary host performs a fail-over processing. `host_name` must be an alphanumeric string of 1 through 63 characters that allows punctuation marks.

- **realm realm_name**
  The `realm_name` must be an alphanumeric string of 1 through 63 characters that allows punctuation marks. The realm may typically be a company or service name.

**Usage**

Use this command to select a Diameter credit control peer and realm.

⚠️ **Caution:** This configuration completely overrides all instances of `diameter peer-select` that have been configured with in the Credit Control Configuration Mode for an Active Charging service.

**Example**

The following command selects a Diameter credit control peer named `test` and a realm of `companyx:`

```plaintext
```
dcca peer-select peer test realm companyx
default

Restores the default value for the option specified for the current subscriber.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Subscriber Configuration

```bash
configure > context context_name > subscriber { default | name subscriber_name }
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax

```bash
```

---

**access-link ip-fragmentation**

Sets the method for fragmenting packets over the MN access link to its default of normal. Drop the packet and send ICMP unreachable to the source of packet.

---

**accounting-mode**

Enables Radius accounting for the current local subscriber configuration.

---

**data-tunneling ignore df-bit**

Sets this option to the default behavior, which is to send an ICMP unreachable - need to frag message back to the sender and drop the packet, in the case that fragmentation is required but the DF bit is set.

---

**idle-timeout-activity dormant-downlink-data**

Sets this option to the default behavior. When downlink data packets are transmitted to the Mobile node and the session is in dormant mode the session idle timer is reset.

---

**inter-pdsn-handoff**

During a handoff from one PDSN to another, if the Mobile requests an IP address of 0.0.0.0 or a mismatched IP address the PDSN will not disconnect the session immediately. The PDSN tries to assign the proposed address of the session in the IPCP configuration NAK.
ip { allowed-dscp | dhcp-relay | header-compression | hide-service-address | multicast discard | qos-dscp | source-validation | user-datagram-tos copy }

**allowed-dscp**: resets the allowed DSCP parameters to the system defaults: class none, max-class be.

**hide-service-address**: specifies the default setting for hide the ip-address of the service from the subscriber. Default is Disabled

**dhcp-relay**: Configured with the DHCP server address during MS authentication. The AAA server sends the address of the DHCP server in the Access-Accept message. The DHCP relay uses this address to relay the DHCP messages from the MS to the DHCP server.

**multicast discard**: Configures the default multicast settings which is to discard PDUs

**qos-dscp**: Sets the quality of service setting to the system default.

**source-validation**: Specifies the default IP source validation. Default is Enabled.

**user-datagram-tos copy**: Disables copying of the IP TOS octet value to all tunnel encapsulation IP headers.

loadbalance-tunnel-peers
Sets the tunnel load balancing algorithm to the system default.

long-duration-action
Sets the action that is taken when the long duration timer expires to the default: detection.

mobile-ip { home-agent | mn-aaa-removal-indication | mn-ha-hash-algorithm | reverse-tunnel | security-level | send { dns-address | terminal-verification } }

**allow-aaa-address-assignment**: Disables the FA from accepting a home address assigned by an AAA server.

**home-agent**: Sets home agent IP address to its default of 0.0.0.0.

**match-aaa-assigned-address**: Disables the FA validating the home address in the RRQ against the one assigned by AAA server.

**mn-aaa-removal-indication**: Sets this parameter to its default of disabled.

**mn-ha-hash-algorithm**: Sets the encryption algorithm to the default of hmac-md5.

**reverse-tunnel**: Sets this parameter to its default of enabled.

**security-level**: Sets this parameter to its default of none.

**send dns-address**: Disables the HA from sending the DNS address NVSE in the RRP.

**send terminal-verification**: Disables the FA from sending the terminal verification NVSE in the RRQ.

permission
Restores the subscriber’s service usage defaults.

ppp { always-on-vse-packet | data-compression { mode | protocols } | ip-header-compression negotiation | keepalive | min-compression-size | mtu }

Sets the point-to-point protocol option defaults.

**always-on-vse-packet**: Re-enables the PDSN to send special 3GPP2 VSE PPP packets to the Mobile Node with a max inactivity timer value for always on sessions. This configuration is applicable only for PDSN sessions.

**data-compression { mode | protocols }**: restores the default value for either the data compression mode or compression protocols as follows:

- mode stateless
all protocols enabled

**ip-header-compression negotiation** : Sets the IP header compressions negotiation to the system default: force.

**keepalive** : sets the subscriber’s PPP keep alive option to the system default: 30 seconds.

**min-compression-size** : Restores the PPP minimum packet size for compression: 128 octets.

**mtu** : Sets the maximum message transfer unit packet size to the system default: 1500 octets.

---

**radius accounting interim interval-timeout**

Disables the RADIUS accounting interim interval for the current subscriber.

---

**timeout [ absolute | idle | long-duration ]**

When a keyword is entered, this command resets the specified timeout to the system default: 0. When no keyword is specified, all timeouts are reset to the system defaults: 0.

---

**Usage**

Use this keyword to reset subscriber data to the system defaults. This is useful in setting the subscriber back to the basic values to possibly aid in trouble shooting or tuning a subscriber’s access and options.

**Example**

```
default ip qos-dscp
default permission
default data-compression mode
```
dhcp dhcv6

Specifies the DHCPv6 service to be used for this subscriber.

**Product**
- GGSN
- P-GW
- SAEGW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Subscriber Configuration
`configure > context context_name > subscriber { default | name subscriber_name }`

Entering the above command sequence results in the following prompt:
```
[context_name]host_name(config-subscriber)#
```

**Syntax**

```
dhcp dhcv6 service-name service_name
```

```
no dhcp dhcv6 service-name
```

Removes the DHCPv6 service for the subscriber.

```
dhcv6 service-name service_name
```

Specifies the name of an existing DHCPv6 service to be used for this subscriber.
`service_name` must be the name of a DHCPv6 service expressed as an alphanumeric string of 1 through 63 characters.

**Usage**
Use this command to apply or remove an existing DHCPv6 service to a subscriber template.

**Example**
The following command applies a previously configured DHCPv6 service named `dhcv6_1` to a subscriber template:
```
dhcp dhcv6 service-name dhcv6_1
```
**dhcp options**

Specifies the DHCP options which can be sent from the DHCP server for this subscriber.

**Product**
- GGSN
- P-GW
- SAEGW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Subscriber Configuration

```bash
configure > context context_name > subscriber { default | name subscriber_name }
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

**Syntax**

```bash
dhcp options code 43 hex-values hex_values
```

**Usage**
Use this command to specify the DHCP options which can be sent from the DHCP server for this subscriber.

**Example**
The following command applies hex values ff-fe for DHCP option 43:

```bash
dhcp options code 43 hex-values ff-fe
```
**dhcp parameter-request-list-option**

Enables the sending of DHCP parameter request list option(s) in all outgoing messages for this subscriber.

**Product**

- P-GW
- SAEGW

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

```bash
configure > context context_name > subscriber { default | name subscriber_name }
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

**Syntax**

```
[ no ] dhcp parameter-request-list-option [ options ]
```

**no**

Disables the sending of DHCP parameter request list option(s) in all outgoing messages.

**options**

Specifies the value of particular DHCP parameter request list option(s).

`options` must be an integer from 1 through 254.

**Important:** Multiple options may be selected in the same command.

**Usage**

Use this command to enable or disable the sending of DHCP parameter request list option(s) in all outgoing messages for this subscriber.

**Example**

The following command enables DHCP parameter request list option inclusion in outgoing messages:

```
dhcp parameter-request-list-option
```
**dhcp service**

Enables DHCP service configuration accessible to the Se-GW context for subscriber. The specified DHCP service will be used for performing DHCP procedures between HNB-GW and HMS.

**Product**

HNB-GW

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > Subscriber Configuration
configure > context context_name > subscriber { default | name subscriber_name }

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

**Syntax**

```
dhcp service dhcp_svc_name context ctxt_name
```

```
no dhcp service
```

**no**

Removes the specified DHCP service from the subscriber template configuration.

**dhcp_svc_name**

Specifies name of the DHCP service configured in Context configuration mode for DHCP proxy support on HNB-GW.

dhcp_svc_name must be an alphanumeric string of 1 through 63 characters preconfigured within the same context of this subscriber.

**context ctxt_name**

Specifies the name of the context where DHCP service is configured for HNB-GW subscribers. ctxt_name must be an alphanumeric string of 1 trough 79 characters.

**Usage**

This command associates the subscriber template with pre-configured DHCP service configuration to provide accessibility to Se-GW with HNB-GW.

**Example**

Following command applies a previously configured DHCP service named dhcp_hnb1 to a subscriber template within the context named femto_hnb.

```
dhcp service dhcp_hnb1 context femto_hnb
```
dns

Configures the domain name servers for the current subscriber.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Subscriber Configuration
configure > context context_name > subscriber { default | name subscriber_name }

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-subscriber)#

Syntax

[ no ] dns { primary | secondary } ip_address

no
Indicates the IP address is to be removed as either a primary or secondary domain name server.

dns primary | secondary
dns primary: Updates the primary domain name server for the subscriber.
dns secondary: Updates the secondary domain name server for the subscriber.

ip_address
Specifies the IP address of the domain name server using IPv4 dotted-decimal notation.

Usage
Set the subscriber DNS server lists as not all users will have the same set of servers.

Example

dns primary 10.2.3.4
no dns primary 10.2.3.4
dns secondary 10.2.5.6
no dns secondary 10.2.5.6
eap

Specifies the lifetime for a master session key (MSK) for extensible authentication protocol (EAP) authentication.

**Product**
ASN-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Subscriber Configuration

```
configure > context context_name > subscriber { default | name subscriber_name }
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

**Syntax**

```
[ default ] eap msk-lifetime dur
```

**default**
Sets the lifetime duration to default value of 3600 seconds for master session key.

**msk-lifetime dur**
Specifies the lifetime duration (in seconds) on Master Session Key (MSK) in seconds for a WiMAX subscriber EAP authentication. 

*dur* is an integer from 60 through 65535.

**Usage**

This command is used to set the lifetime for MSK in EAP authentication for WiMAX subscriber.

**Example**

The following command sets the lifetime for MSK key to 4800 seconds for a WiMAX subscriber through EAP authentication:

```
eap msk-lifetime 4800
```
encrypted password

Designates use of password encryption.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Subscriber Configuration

```bash
configure > context context_name > subscriber { default | name subscriber_name }
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

**Syntax**

```
encrypted password password
```

- `encrypted password password`
- `password` is the encrypted password and must be an alphanumeric string of 1 through 132 characters.

**Usage**

This command is normally used only inside configuration files.

**Example**

The following command sets an encrypted password of `qsdf12d4`:

```
encrypted password qsdf12d4
```
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
end
```

**Usage**

Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Use this command to return to the parent configuration mode.
external-inline-server

This is a restricted command.
### firewall policy

**Important:** This command is only available in StarOS 8.0. In StarOS 8.1 and later releases, this configuration is available in the ACS Rulebase Configuration Mode.

This command enables or disables Stateful Firewall support for the subscriber.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

```bash
configure > context context_name > subscriber { default | name subscriber_name }
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

**Syntax**

```
firewall policy firewall-required

{ default | no } firewall policy
```

- **no**
  
  Disables Stateful Firewall support for this subscriber.

- **default**

  Configures the default setting for Stateful Firewall support.

  Default: Disabled

- **firewall-required**

  Enables Stateful Firewall support for this subscriber.

**Usage**

Use this command to enable or disable Stateful Firewall support for this subscriber.

**Important:** Unless Stateful Firewall support for this subscriber is enabled using this command, firewall processing for this subscriber is disabled.

**Important:** If firewall is enabled, and the rulebase has no firewall configuration, Stateful Firewall will cause all packets to be discarded.

**Example**
The following command enables Stateful Firewall support for this subscriber:

```
firewall policy firewall-required
```

The following command disables Stateful Firewall support for this subscriber:

```
no firewall policy
```
fw-and-nat policy

**Important:** This command is only available in StarOS 8.1. This customer-specific command must be used to configure the Policy-based Firewall-and-NAT feature.

**Product**
PSF
NAT

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Subscriber Configuration

```
configure > context context_name > subscriber { default | name subscriber_name }
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

**Syntax**

```
fw-and-nat policy fw_nat_policy
{ default | no } fw-and-nat policy
```

- **default**
  Specifies that the default Firewall-and-NAT policy configured in the rulebase be used for the subscriber.

- **no**
  Disables Firewall and NAT processing for the subscriber.

- **fw_nat_policy**
  Specifies the Firewall-and-NAT policy for the subscriber.
  `fw_nat_policy` must be an alphanumeric string of 1 through 63 characters. Note that this policy will override the default Firewall-and-NAT policy configured in the ACS rulebase.

**Usage**

Use this command to configure the Firewall-and-NAT policy for subscribers. Note that the policy configured in the subscriber mode will override the default policy configured in the ACS rulebase. If a policy is not configured in the subscriber mode, the default policy configured in the ACS rulebase will be applied.

**Example**

The following command configures a Firewall-and-NAT policy named `standard` for the subscriber:

```
fw-and-nat policy standard
```
**gtpp group**

This command enables/disables eG-CDR generation for CDMA subscribers.

**Product**
IPSG

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Subscriber Configuration

```
configure > context context_name > subscriber { default | name subscriber_name }
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

**Syntax**

```
gtpp group group_name
```

**Usage**

Use this command to enable or disable the generation of eG-CDRs for CDMA traffic observed in customer network during IPSG deployment.
idle-timeout-activity

Defines whether downlink (towards Mobile Node) data packets transmitted when the session is dormant are treated as activity for the idle-timer (inactivity timer).

By default, downlink data transmitted over a dormant session restarts the idle-timer for that session; it is treated as activity for the session.

Product
PDSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Subscriber Configuration
configure > context context_name > subscriber { default | name subscriber_name }

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-subscriber)#

Syntax

[ no ] idle-timeout-activity dormant-downlink-data

no
Dormant mode downlink data is not treated as activity for the session idle-timer. The session idle timer is not reset.

idle-timeout-activity dormant-downlink-data
Treats dormant mode downlink data as activity for the session idle-timer. The session idle timer is reset.

Usage
Use this command to disable or re-enable restarting the session idle timer when downlink data packets are transmitted to the Mobile Node when the session is in dormant mode.

Example
Use the following command to disable restarting the session idle timer when downlink data packets are transmitted to the Mobile Node when the session is in dormant mode:

no idle-timeout-activity dormant-downlink-data

Use the following command to re-enable restarting the session idle timer when downlink data packets are transmitted to the Mobile Node when the session is in dormant mode:

idle-timeout-activity dormant-downlink-data
ikev2 tsr

Configures the Traffic Selector responder (TSr) negotiation behavior during IKEv2 Security Association (SA) establishment.

**Product**
PDG/TTG

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Subscriber Configuration

```
configure > context context_name > subscriber { default | name subscriber_name }
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

**Syntax**

```
[ default ] ikev2 tsr { wildcard | user-specified }
```

- **default**
  Specifies the default behavior, which is wildcard TSr negotiation.

- **ikev2 tsr**
  Specifies ???.

- **wildcard**
  Specifies that during TSr negotiation, the PDG/TTG always returns an any-to-any IP address range, an any-to-any port range, and allows any protocol, irrespective of the traffic selector ranges received from the UE. This is the default behavior.

- **user-specified**
  Specifies that during TSr negotiation, the PDG/TTG responds to each UE request with the UE-specified IP address ranges. This enables split tunneling on the PDG/TTG, and enables the UE to tunnel only a specified traffic range to the PDG/TTG and send other traffic directly out the WLAN.

**Usage**

Use this command to specify the TSr negotiation behavior on the PDG/TTG.

**Example**

The following command enables user-specified TSr negotiation on the PDG/TTG:

```
ikev2 tsr user-specified
```


**ims application-manager**

Specifies the IP Multimedia Subsystem (IMS) application manager for the subscriber.

**Product**
PDSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Subscriber Configuration

```
configure > context context_name > subscriber { default | name subscriber_name }
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

**Syntax**

```
[ no ] ims application-manager { domain-name domain-name | ipv4-address ipv4_address }
```

- **no**
  
  Disables the IMS application manager for this subscriber.

- **ims application-manager**
  
  Enables the IMS application manager for this subscriber.

- **domain-name domain-name**
  
  Specifies the domain name of the application manager.
  
  **domain-name** must be an alphanumeric string of 1 through 63 characters.

- **ipv4-address ipv4_address**
  
  Specifies the IP address of the application manager using IPv4 dotted-decimal notation.

**Usage**

The IMS application manager address is returned by HA to MN in DHCP Ack when it receives the DHCP inform from an AIMS subscriber.

**Example**

```
ims application-manager domain-name domain23
ims application-manager ipv4-address 192.168.23.1
```
ims-auth-service

Enables IP Multimedia Subsystem (IMS) authorization support for subscriber. The specified IMSA service will be used for performing IMS authorization and flow-based charging procedures.

Product
PDSN
GGSN
P-GW
SAEGW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context context_name > subscriber { default | name subscriber_name }

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-subscriber)#

Syntax

[ default | no ] ims-auth-service auth_svc_name

- **default**
  - Configures default setting.
  - Default: Disabled or as specified at the context or network access service level or in subscriber template.

- **no**
  - Removes the specified IMS authorization service from the subscriber configuration.

- **ims-auth-service auth_svc_name**
  - Specifies name of the IMS authorization service.
  - auth_svc_name must be an alphanumeric string of 1 through 63 characters preconfigured within the same context of this subscriber.

Usage
This feature provides the IMS authorization service configuration for Gx interface in IMS service node.

Example
Following command applies a previously configured IMS authorization service named ims_interface1 to a subscriber within the specific context.

```plaintext
ims-auth-service ims_interface1
```
inter-pdsn-handoff

Configure the system to force the MN to use its assigned IP address during Internet Protocol Control Protocol (IPCP) negotiations resulting from inter-PDSN handoffs.

Product
PDSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context context_name > subscriber { default | name subscriber_name }

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-subscriber)#

Syntax

[ no ] inter-pdsn-handoff require ip-address

no
Disables the rejecting of sessions when the MN uses a non-allocated IP address during IPCP re-negotiations.

inter-pdsn-handoff require ip-address
Rejects sessions when the MN uses a non-allocated IP address during IPCP re-negotiations.

Usage
This command is used to configure the system to reject sessions that are re-negotiating IPCP after an inter-PDSN handoff if the IP address they propose does not match the one initially provided by the PDSN. The session would be rejected even if the proposed address was 0.0.0.0.
If this parameter is disabled, the PDSN will attempt to re-assign the IP address initially provided.

Example
To set the PDSN to not allow a mismatched IP address during a PDSN to PDSN handoff of a MIP call, use the following command:

inter-pdsn-handoff require ip-address

To set the PDSN so that it will not disconnect the session immediately, if the Mobile requests an IP address of 0.0.0.0 or a mismatched IP address after inter-pdsn handoff, use the following command:

no inter-pdsn-handoff require ip-address
ip access-group

Configures IP access group for the current subscriber.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Subscriber Configuration
configure > context context_name > subscriber { default | name subscriber_name }

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-subscriber)#

Syntax

[ no ] ip access-group group_name [ in | out ]

no
Indicates the access group specified is to be cleared from the subscribers configuration.

ip access-group group_name
Specifies the name of the IPv4/IPv6 access group. acl_group_name is a configured ACL group expressed as an alphanumeric string of 1 through 79 characters.

in | out
Default: both (in and out)
Specifies the access-group as either inbound or outbound by the keywords in and out, respectively. If neither of these key words is specified, the command associates the group_name access group with the current subscriber for both inbound and outbound access.

Usage
Set the subscriber access group to manage the access control for subscribers as a logical group.

Example
The following command associates the sampleGroup access group with the current subscriber for both inbound and outbound access:

    ip access-group sampleGroup

The following removes the outbound access group flag for sampleGroup:

    no ip access-group sampleGroup out
ip address

Configures a static IPv4 address for use by the subscriber.

Product
PDSN
GGSN
HA
ASN-GW
P-GW
SAEGW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Subscriber Configuration
configure > context context_name > subscriber { default | name subscriber_name }

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-subscriber)#

Syntax

[ no ] ip address ip_address netmask

no
Removes a previously configured IP address assignment.

ip address ip_address
Specifies the IP address assigned to the subscriber using IPv4 dotted-decimal notation.

netmask
The subnet mask that corresponds to the assigned IPv4 address.

Usage
Use this command to assign a static IPv4 address to the subscriber. This address will be used each time the subscriber establishes data sessions.

Example
The following command configures a static IP address of 192.168.1.15 with a subnet mask of 255.255.255.0 to the subscriber:

ip address 192.168.1.15 255.255.255.0
ip address pool

Configures IP address pool properties for the subscriber.

**Product**
PDSN
GGSN
HA
ASN-GW
P-GW
SAEGW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Subscriber Configuration

```
configure > context context_name > subscriber { default | name subscriber_name }
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

**Syntax**

```
[ no ] ip address pool name pool_name
```

- **no**
  
  Removes a previously configured static address.

- **ip address pool name pool_name**

  Specifies the IP address pool or IP address pool group from which the subscribers IP address is assigned. 
  `pool name` must be the name of an existing IP pool or IP pool group expressed as an alphanumeric string of 1 through 31 characters.

**Usage**

Use this command to specify the name of an IP address pool configured on the system from which IP addresses are to be dynamically assigned to sessions from this subscriber.

This command can be issued multiple times to specify multiple address pools for the subscriber. If multiple pools are specified, addresses are assigned for subscriber sessions from the pools based on the order in which the pools were configured.

If an address cannot be provided from the first-specified pool for whatever reason, the system attempts to assign an address from the second-specified pool, and so on. This operation is independent of the priorities configured for the pools. For example, if pool1 was specified for the subscriber first, and pool2 second, the system always attempts to assign addresses from pool1. If an address can not be assigned from pool1 (i.e. all addresses are in use), the system then attempts to assign an address from pool2.

**Example**
The following command configures the subscriber to receive IP addresses from an IP address pool named `public1`:

```
  ip address pool name public1
```
ip address secondary-pool

Configures secondary IP address pool properties for the subscriber to provide multiple IP host configuration behind one WiMAX Customer Premise Equipment (CPE).

Product
ASN-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context context_name > subscriber { default | name subscriber_name }  

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-subscriber)#

Syntax

[ no ] ip address secondary-pool name aux_pool_name

- no
  Remove a previously configured auxiliary pool named aux_pool_name for multiple host support in ASN-GW service.

- ip address secondary-pool name aux_pool_name
  Specifies the secondary/auxiliary IP address pool or IP address pool group from which the IP address is assigned to host behind a WiMAX CPE having primary IP address. pool_name must be the name of an existing IP pool or IP pool group expressed as an alphanumeric string of 1 through 31 characters.

Usage
Use this command to specify the name of an IP address pool configured on the system from which IP addresses are to be dynamically assigned to host behind a WiMAX CPE for multiple host session support. This command designates the IP address to secondary hosts from locally configured secondary IP address pool. To enable multiple host support behind a WiMAX CPE and configure maximum number of supported hosts use secondary-ip-host command in ASN Gateway Service Configuration mode.

Example
The following command configures the subscriber to receive IP addresses from a secondary IP address pool named auxiliary1 for secondary hosts behind the WiMAX CPE:

  ip address secondary-pool name auxiliary1
ip allowed-dscp

Sets the Quality of Service (QoS) Differentiated Services (DiffServ) marking that a subscriber session is allowed. The DSCP is disabled by default.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Subscriber Configuration

`configure > context context_name > subscriber { default | name subscriber_name }`

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-subscriber)#`

Syntax

```
ip allowed-dscp class class max-class maxclass [ rt-marking marking ]

no ip allowed-dscp class
```

---

**ip allowed-dscp class class**

Specifies the Differentiated Services Codepoint (DSCP) class with which the subscriber session may mark its packets. If the subscriber sessions packets request a code point class higher than the code point class specified, the PDSN service re-marks the packets with the QoS-DSCP value specified by the `ip qos-dscp` command.

Default: none

*class* must be one of the following:

- **a**: allow packets with AF DSCPs
- **e**: allow packets with EF DSCP
- **o**: allow packets for experimental or local use
- **ae**: allow packets with AF and EF DSCPs
- **ao**: allow packets with AF DSCPs or packets for experimental or local use
- **eo**: allow packets with EF DSCPs or packets for experimental or local use
- **aeo**: allow packets with AF or EF DSCPs or packets for experimental or local use
- **none**: allow only the **be** and **sc1** through **sc7** code points

---

**max-class maxclass**

This parameter specifies the maximum code point with which a subscriber session may mark its packets. The subscriber sessions packets must be marked with a code point equal to or less than the code point specified. If the subscriber sessions packets request a code point higher than the code point specified, the PDSN service re-marks the packets with the QoS-DSCP value specified by the lower of the max-class and the `ip qos-dscp` command.
The list below identifies the code points from lowest to highest precedence. For example, if the `maxclass` is set to `af22`, that becomes the maximum code point that the subscriber session may mark its packets with and only `be`, `af13`, `af12`, `af11`, `af23`, and `af22` are allowed. If a subscriber session marks its packets with anything after `af22` in this list, the PDSN service re-marks the packets with the QOS-DSCP value specified by the lower of the maxclass and the `ip qos-dscp` command.

If class is set to none only the `be` and `sc1` through `sc7` codepoints are allowed. For example; if `class` is set to none and you set `max-class` to `sc1`, only the `sc1` and `be` codepoints are allowed.

Default: `be`

The `maxclass` must be one of the following:
- `be`: best effort forwarding
- `af13`: assured Forwarding 13
- `af12`: assured Forwarding 12
- `af11`: assured Forwarding 11
- `af23`: assured Forwarding 23
- `af22`: assured Forwarding 22
- `af21`: assured Forwarding 21
- `af31`: assured Forwarding 31
- `af32`: assured Forwarding 32
- `af33`: assured Forwarding 33
- `af41`: assured Forwarding 41
- `af42`: assured Forwarding 42
- `af43`: assured Forwarding 43
- `ef`: expedited forwarding
- `sc1`: selector class 1
- `sc2`: selector class 2
- `sc3`: selector class 3
- `sc4`: selector class 4
- `sc5`: selector class 5
- `sc6`: selector class 6
- `sc7`: selector class 7

The `rt-marking marking` parameter is used for Mobile IP (MIP) reverse tunnels. When MIP session packets do not have a DSCP marking, the Foreign Agent (FA) marks the packets with the value specified by `rt-marking marking`. If MIP session packets have a DSCP marking, the marking is subjected to the conformance rules for the values of class and max-class; the final DSCP marking is then copied from the inner IP header to the outer IP header.

Default: `be`

The `marking` must be one of the following:
- `be`: best effort forwarding
- `af11`: assured Forwarding 11
- `af12`: assured Forwarding 12
- `af13`: assured Forwarding 13
- `af21`: assured Forwarding 21
- `af22`: assured Forwarding 22
- `af23`: assured Forwarding 23
- `af31`: assured Forwarding 31
- `af32`: assured Forwarding 32
- `af33`: assured Forwarding 33
- `af41`: assured Forwarding 41
- `af42`: assured Forwarding 42
**af43**: assured Forwarding 43  
**ef**: expedited forwarding  
**sc1**: selector class 1  
**sc2**: selector class 2  
**sc3**: selector class 3  
**sc4**: selector class 4  
**sc5**: selector class 5  
**sc6**: selector class 6  
**sc7**: selector class 7

**Usage**

Use this command to configure Quality of Service (QoS) for a subscriber session to allow a Differentiated Services (DiffServ) Code Point (DSCP) marker in the header of each IP packet that prompts network routers to apply differentiated grades of service to various packet streams.

This command uses `class` and type of marker (rt-marking for reverse tunnels) for configuration with `max-class` maximum code point that a subscriber session may mark its packets with.

**Example**

The following command will allow 0 packets for experimental or local use with best effort forwarding `be`:

```
ip allowed-dscp class 0 max-class be
```
ip context-name

Configures the context to which the subscriber is assigned upon authentication. The assigned context is considered the destination context that provides the configuration options for the services the subscriber is allowed to access.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Subscriber Configuration

`configure > context context_name > subscriber { default | name subscriber_name }`

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-subscriber)#`

**Syntax**

```
[ no ] ip context-name  name
```

- **no**
  Removes the current assigned context from the subscriber’s data.

- **ip context-name  name**
  Specifies the name of the context to assign the subscriber to once authenticated. `name` must be an alphanumeric string of 1 trough 79 characters.

**Usage**
Set the subscriber IP context to a common context when all subscribers from one or more contexts will use the same egress context.

**Example**

```
ip context-name sampleName

no ip context-name sampleName
```
ip header-compression

Configures the IP packet header compression options for the current subscriber. Although this command configures IP header compression algorithms, the Internet Protocol Control Protocol (IPCP) negotiations determine when the header compression algorithm is applied.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Subscriber Configuration

```bash
configure > context context_name > subscriber { default | name subscriber_name }
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax

```bash
ip header-compression { rohc [ any [ mode { optimistic | reliable | unidirectional } ] ] | cid-mode { { large | small } [ marked-flows-only | max-cid | max-hdr value | mrru value ] } | marked flows-only | max-hdr value | mrru value | downlink | uplink ] | vj } +
```

```bash
[ default | no ] ip header-compression
```

- **default**
  Restores this command’s default setting to the Van Jacobsen (VJ) header compression algorithm.

- **no**
  Disables all IP header compression.

```bash
ip header-compression { rohc [ any [ mode { optimistic | reliable | unidirectional } ] ] | cid-mode { { large | small } [ marked-flows-only | max-cid | max-hdr value | mrru value ] } | marked flows-only | max-hdr value | mrru value | downlink | uplink ] | vj }
```

Specifies that the Robust Header Compression (ROHC) algorithms is used for data.

**Important:** ROHC is only supported for use with the PDSN.

- **any:** Apply ROHC header compression in both the uplink and downlink directions.
- **mode { optimistic | reliable | unidirectional }**:
  - **optimistic:** Sets the ROHC mode to Bidirectional Optimistic mode (O-mode). In this mode packets are sent in both directions. A feedback channel is used to send error recovery requests and (optionally) acknowledgments of significant context updates from decompressor to compressor. Periodic refreshes are not used in the Bidirectional Optimistic mode.
  - **reliable:** Sets the ROHC mode to Bidirectional Reliable mode (R-mode). This mode applies an intensive usage of a feedback channel and a strict logic at both the compressor and the decompressor.
that prevents loss of context synchronization between the compressor and the decompressor. Feedback is sent to acknowledge all context updates, including updates of the sequence number field.

- **unidirectional**: Sets the ROHC mode to Unidirectional mode (U-mode). With this mode packets are sent in one direction only, from the compressor to the decompressor. This mode therefore makes ROHC usable over links where a return path from the decompressor to the compressor is unavailable or undesirable.

```
cid-mode { { large | small } [ marked-flows-only | dm | max-hdr value | mrru value ] } : Specifies the ROHC packet type to be used.
  * large | small [ marked-flows-only | max-cid | max-hdr value | mrru value ] : Defines the ROHC packet type as large or small and optionally sets the following parameters for the packet type selected:
  * marked-flows-only: Specifies that ROHC is to be applied only to marked flows.
  * max-cid integer: Default: 0 The highest context ID number to be used by the compressor. integer must be an integer from 0 through 15 when small packet size is selected and must be an integer from 0 through 31 when large packet size is selected.
  * max-hdr value: Specifies the maximum header size to use. Default: 168. value must be an Integer from 0 through 65535.
  * mrru value: Specifies the maximum reconstructed reception unit to use. Default: 65535. value must be an Integer from 0 through 65535.
```

- **downlink**: Apply the ROHC algorithm only in the downlink direction.
- **uplink**: Apply the ROHC algorithm only in the uplink direction.

**Important**: When ROHC is enabled for downlink or uplink only the operational mode is Unidirectional.

```
vj
```

Specifies that the VJ algorithm is used for header compression.

```
+
```

Either one or both of the keywords may be entered in a single command. If both vj and rohc are specified, vj must be specified first.

**Important**: If both VJ and ROHC header compression are specified, the optimum header compression algorithm for the type of data being transferred is used for data in the downlink direction.

**Usage**

Header compression can be used to provide a higher level of security in IP traffic enhance bandwidth usage and lower bit errors. By default the header compression algorithm is set to vj.

**Example**
The following command disables all IP packet header compression:

   no ip header-compression

The following command sets IP header compression to default vj algorithm:

   default ip header-compression

The following command also sets the IP header compression to the vj algorithm:

   ip header-compression vj

The following command enables the Internet Protocol Control Protocol (IPCP) to determine which protocol is the optimum algorithm for data in the downlink direction and use either VJ or ROHC as needed:

   ip header-compression vj rohc

The following command enables ROHC for the downlink direction only:

   ip header-compression rohc downlink

The following command enables ROHC in any direction using Bidirectional Optimistic mode:

   ip header-compression rohc any mode Optimistic
ip hide-service-address

Hide the IP address of the service from the subscriber.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context context_name > subscriber { default | name subscriber_name }

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-subscriber)#

Syntax

[ no ] ip hide-service-address

    no

    Does not hide the IP address of the service from the subscriber. This is the default behavior.

    ip hide-service-address

    Hides the IP address of the service from the subscriber.

Usage

Use this command to prevent subscribers from using traceroute to discover the network addresses that are in the public domain and configured on services. This prevent users from pinging such addresses.
**ip local-address**

Configures the local-side IP address of the subscriber's point-to-point connection.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Subscriber Configuration
```
configure > context context_name > subscriber { default | name subscriber_name }
```

Entering the above command sequence results in the following prompt:
```
[context_name]host_name(config-subscriber)#
```

**Syntax**

```
ip local-address ip_address
no ip local-address
```

- **no**
  
  Removes a previously configured IP local-address.

```
ip_address ip_address
```

- Specifies an IP address configured in a destination context on the system through which a packet data network can be accessed. *ip_address* is entered using IPv4 dotted-decimal notation.

**Usage**

This parameter specifies the IPv4 address on the system that the MS uses as the remote-end of the PPP connection. If no local address is configured, the system uses an "unnumbered" scheme for local-side addresses.

**Example**

The following command configures a local address of 192.168.1.23 for the MS:

```
local-address 192.168.1.23
```
ip multicast discard

Configures the IP multicast discard packet behavior.

**Product**
GGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Subscriber Configuration

```
configure > context context_name > subscriber { default | name subscriber_name }
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

**Syntax**

```
[ no ] ip multicast discard
```

- **no**
  
  Does not discard IP multicast packets.

- **ip multicast discard**
  
  Discards IP multicast packets.

**Usage**

This command specifies if IP multicast packets will be discarded.
ip qos-dscp

Configures quality of service (QoS) options for the current subscriber using the differentiated services code point (DSCP) method. This functionality is disabled by default.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Subscriber Configuration
configure > context context_name > subscriber { default | name subscriber_name }

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

**Syntax**

```
ip qos-dscp option

no ip qos-dscp
```

Sets the quality of service option to its default value.

```
ip qos-dscp option

Default: be (Best Effort)
```

Specifies the subscriber’s per hop quality of service setting as one of:

- **af11**: assured Forwarding 11
- **af12**: assured Forwarding 12
- **af13**: assured Forwarding 13
- **af21**: assured Forwarding 21
- **af22**: assured Forwarding 22
- **af23**: assured Forwarding 23
- **af31**: assured Forwarding 31
- **af32**: assured Forwarding 32
- **af33**: assured Forwarding 33
- **af41**: assured Forwarding 41
- **af42**: assured Forwarding 42
- **af43**: assured Forwarding 43
- **be**: best effort forwarding
- **ef**: expedited forwarding
**Usage**

Set the quality of service for a subscriber based upon the service level agreements.

**Example**

```
ip qos-dscp ef
no ip qos-dscp
```
**ip route**

Configures the static route to use to reach the subscriber’s network.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Subscriber Configuration

`configure > context context_name > subscriber { default | name subscriber_name }`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

**Syntax**

```
[ no ] ip route ip_address ip_mask [ gateway_address ]
```

- **no**
  Removes the configured route information from the subscriber data.

- **ip route ip_address**
  Specifies the target IP address for which the route information applies using IPv4 dotted-decimal notation.

- **ip_mask**
  Specifies the networking mask for the route.
  1 bits in the `ip_mask` indicate that bit position in the `ip_address` must also have a value of 1.
  0 bits in the `ip_mask` indicate that bit position in the `ip_address` does not need to match, such as the bit can be either a 0 or a 1.
  For example, if the IP address and mask were specified as 172.168.10.0 and 255.255.255.224, respectively, the network mask will be 172.168.0.0 (obtained by logically ANDing the IP address with the IP mask).

- **gateway_address**
  Default: assigned remote IP address will be used as the gateway address.
  Specifies the IP address of the next hop gateway for the route using IPv4 dotted-decimal notation.

**Usage**
The static routes are also known as framed IP routes for subscribers. Static routes are typically applicable for subscribers connecting via other networks or when the mobile device acts as a gateway to a network on the far side of the device.

For example, if the mobile device is assigned IP address 10.2.3.4 and it acts as a gateway for the network 10.2.3.0 (with a network mask of 255.255.255.0) a static route would be configured with the `ip_address` being 10.2.3.0, `ip_mask` being 255.255.255.0, and `gateway_address` being 10.2.3.4.

**Example**

```
no ip route 10.2.3.4 255.255.255.0
```
ip source-validation

Enables or disables packet source validation for the current subscriber. Source validation requires that the source address of the received packets match the IP address assigned to the subscriber (either statically or dynamically) during the session.

If an incorrect source address is received from the mobile node, the system attempts to renegotiate the PPP session. The parameters for IP source validation can be set by the `ip source-violation` command.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Subscriber Configuration

```
configure > context context_name > subscriber { default | name subscriber_name }
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

**Syntax**

```
[ no ] ip source-validation
```

- `no`
  Disables source validation.

- `ip source-validation`
  Enables source validation.

**Usage**

Source validation is useful if packet spoofing is suspected or for verifying packet routing and labeling within the network.

**Example**

The following command enables IP source validation:

```
ip source-validation
```

The following command disables IP source validation:

```
no ip source-validation
```
ip user-datagram-tos copy

Controls copying of the IP TOS octet value from IPv4/IPv6 datagrams to the IP header in tunnel encapsulation. This is disabled by default.

Product
PDSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context context_name > subscriber { default | name subscriber_name }

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-subscriber)#

Syntax

ip user-datagram-tos copy [ access-link-tunnel | both | data-tunnel ]

no ip user-datagram-tos copy

no
Disable copying of the IP TOS octet value to all tunnel encapsulation IP headers.

ip user-datagram-tos copy
Enables copying of the IP TOS octet value to all tunnel encapsulation IP headers.

access-link-tunnel
Copies the IP TOS octet value to the tunnel encapsulation IP header on the access side (RP) tunnel.

both
Uses both the access-link-tunnel and data-tunnel.

data-tunnel
Copies the IP TOS octet value to the tunnel encapsulation IP header on the MIP data tunnel or L3 tunnel (IP-in-IP, GRE).

Usage
Use this command to enable the copying of the IP TOS octet value to the tunnel encapsulation IP header. This functionality allows PCF to detect special TOS marking in the outer IP header of A11 packets and to identify certain packets as QChat control messages. The Base Station Controller/Packet Control Function (BSC/PCF) must give higher priority to QChat control messages.

Example
The following command enables copying of the IP TOS octet value to the tunnel encapsulation IP header for the access side tunnel:

```
ip user-datagram-tos copy access-link-tunnel
```

The following command disables copying of the IP TOS octet value to all tunnel encapsulation IP headers:

```
no ip user-datagram-tos copy
```
**ip vlan**

Configures subscriber-to-Virtual LAN (VLAN) associations.

**Product**
- PDSN
- HA

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration > Context Configuration > Subscriber Configuration

```
configure > context context_name > subscriber { default | name subscriber_name }
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

**Syntax**

```
ip vlan vlan-id
[ default | no ] ip vlan
```

- **default**
  - Resets the VLAN ID to the default setting.

- **no**
  - Disables the VLAN ID for the subscriber.

```
ip vlan vlan-id
```

- Specifies the VLAN ID that is associated with the IP address for that session. `vlan-id` is an integer from 1 through 4094.

**Usage**

This command configures the subscriber vlan ID which is used with the assigned address for the subscriber session to receive packets. If the IP pool from which the address is assigned is configured with a VLAN ID, this subscriber configured VLAN ID overrides it.

Subscriber traffic can be routed to specific VLANs based on the configuration of their user profile. Using this functionality provides a mechanism for routing all traffic from a subscriber over the specified VLAN. All packets destined for the subscriber must also be sent using only IP addresses valid on the VLAN or they will be dropped.

**Example**

Set the vlan ID to the default setting by entering the following command:

```
default ip vlan
```
ipv6 access-group

Configures the IPv6 access group for a subscriber.

Product
PDSN
GGSN
ASN-GW
P-GW
SAEGW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Subscriber Configuration
configure > context context_name > subscriber { default | name subscriber_name }

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-subscriber)#

Syntax
ipv6 access-group name [ in | out ]

ipv6 access-group name
Defines the access group name. name is an alphanumeric string of 1 through 47 characters.
in
Defines the access group as inbound.
out
Defines the access group as outbound.

Usage
Used to create an access group for a subscriber.

Example
The following command provides an example of an IPv6 access group with the name list_1:

ipv6 access-group list_1
ipv6 address

Configures a static IP address for use by the subscriber.

Product
PDSN
GGSN
ASN-GW
P-GW
SAEGW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Subscriber Configuration
configure > context context_name > subscriber { default | name subscriber_name }

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-subscriber)#

Syntax
[ no ] ipv6 address { prefix address | prefix-pool name }

no
Deletes a previously configured ipv6 address.

ipv6 address address
Specifies an IPv6 address. address is entered using IPv6 colon-separated-hexadecimal notation.

prefix
Specifies a static IPv6 address.

prefix-pool name
Specifies an IPv6 prefix pool name. name is an alphanumeric string of 1 through 31 characters.

Usage
Use this command to assign a static IPv6 address to the subscriber. This address will be used each time the subscriber establishes data sessions.

Example
The following command configures a static IP address of 2001:4A2B::1f3F with a mask length of 24 to the subscriber:

ipv6 address 2001:4A2B::1f3F/24
**ipv6 dns**

Configures the IPv6 Domain Name Service (DNS) servers.

**Product**

- PDSN
- GGSN
- ASN-GW
- P-GW
- SAEGW

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

```
configure > context context_name > subscriber { default | name subscriber_name }
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

**Syntax**

```
[ no ] ipv6 dns { primary | secondary } { ipv6_dns_address }
```

- **no**
  
  Deletes a previously configured DNS server.

- **ipv6 dns ipv6_dns_address**

  Specifies an IP address for the DNS server. `ipv6_dns_address` is entered using IPv6 colon-separated-hexadecimal notation.

- **primary**

  Configures the primary DNS server for the subscriber.

- **secondary**

  Configures the secondary DNS server for the subscriber. Only one secondary DNS server can be configured.

- **ipv6_dns_address**

  Configures the IP address of the DNS server.

**Usage**

DNS servers are configured on a per subscriber basis. This allows each subscriber to use specific servers.

**Example**

The following command provides an example of setting the primary IPv6 DNS server:
ipv6 dns primary fe80::c0a8:a04
**ipv6 dns-proxy**

Configures the system to act as a domain name server proxy for the current subscriber.

**Product**
- PDSN
- GGSN
- ASN-GW
- P-GW
- SAEGW

**Privilege**
Security Administrator, Administrator

**Mode**
**Exec > Global Configuration > Context Configuration > Subscriber Configuration**
```sh
configure > context context_name > subscriber { default | name subscriber_name }
```

Entering the above command sequence results in the following prompt:
```
[context_name]host_name(config-subscriber)#
```

**Syntax**
```
[ default | no ] ipv6 dns-proxy
```

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Disables IPv6 DNS proxy functionality for a subscriber.</td>
</tr>
<tr>
<td>no</td>
<td>Removes the pre-enabled functionality of IPv6 DNS proxy for a subscriber.</td>
</tr>
<tr>
<td>ipv6 dns-proxy</td>
<td>Enables IPv6 DNS proxy functionality for a subscriber. If enabled, the system will act as proxy DNS server. Default: disabled.</td>
</tr>
</tbody>
</table>

**Usage**
Used to enable or disable IPv6 DNS proxy for the subscriber. When enabled, the PDSN acts as a proxy DNS server for DNS IPv6 queries coming from the mobile station to the PDSN’s local PPP link address.

**Example**
The following command disables the IPv6 DNS proxy function for the subscriber:
```
no ipv6 dns-proxy
```
ipv6 egress-address-filtering

Configures the system to perform egress address filtering for the subscriber.

Product
- PDSN
- GGSN
- ASN-GW
- P-GW
- SAEGW

Privilege
- Security Administrator, Administrator

Mode
- Exec > Global Configuration > Context Configuration > Subscriber Configuration
- configure > context context_name > subscriber { default | name subscriber_name }

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-subscriber)#

Syntax

[ no ] ipv6 egress-address-filtering

- no
  - Disables IPv6 egress address filtering.

- ipv6 egress-address-filtering
  - Enables IPv6 egress address filtering.

Usage

Used to enable the filtering of packets that arrive from the Internet to a particular site.

Example

The following command disables egress address filtering:

  no ipv6 egress-address-filtering
**ipv6 initial-router-advt**

Creates an IPv6 initial router advertisement interval for the subscriber.

**Product**

- PDSN
- GGSN
- ASN-GW
- HSGW
- P-GW
- SAEGW

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

```
configure > context context_name > subscriber { default | name subscriber_name }
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

**Syntax**

```
ipv6 initial-router-advt { interval value | num-advts value | router-solicit-wait-timeout value }
```

```
default ipv6 initial-router-advt { interval | num-advts | router-solicit-wait-timeout }
```

```
no ipv6 initial-router-advt router-solicit-wait-timeout
```

---

**default**

Resets the command to its default settings.

---

**no ipv6 initial-router-advt router-solicit-wait-timeout**

Disables running timer to wait for router solicit and sends the initial router advertisement immediately once session is up.

---

**ipv6 initial-router-advt**

Enables an initial router advertisement interval in milliseconds.

---

**interval value**

Default: 3000

The time interval the initial IPv6 router advertisement is sent to the mobile node in milliseconds.

`value` is an integer between 100 and 16000 milliseconds.
num-advts value value
Default: 3
The number of initial IPv6 router advertisements sent to the mobile node. value is an integer between 1 to 16.

router-solicit-wait-timeout value
Default: 3000
The time interval to wait for router solicit before sending the initial IPv6 router advertisement. value is an integer between 1 and 30000 milliseconds.

Usage
This command is used to set the advertisement interval and the number of advertisements. Using a smaller advertisement interval increases the likelihood of router being discovered more quickly when it first becomes available.
If timer is enabled and router solicit is received before timeout, then RA will be sent in response to RS and no further RA will be sent. If timer is enabled and no router solicit is received after timeout, initial RAs will be sent as configured and IPv6 capability indication will be sent in S2a to P-GW to indicate that P-GW should drop any IPv6 traffic for this PDN.

Example
The following command specifies the initial ipv6 router interval to be 2000ms:
```
ipv6 initial-router-advt interval 2000
```
**ipv6 interface-id**

Provides an IPv6 interface identifier for the subscriber.

**Product**

- PDSN
- GGSN
- ASN-GW
- P-GW
- SAEGW

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

```
configure > context context_name > subscriber { default | name subscriber_name }
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

**Syntax**

```
ipv6 interface-id ifid

[ default | no ] ipv6 interface-id

default
No interface ID set for IPv6CP negotiation to subscriber.

no
Deletes a previously configured IPv6 interface ID.

interface-id ifid
Specifies the interface ID assigned to the Mobile during IPv6 Control Protocol (IPv6CP) negotiation. *ifid* is a 64-bit unsigned integer.
```

**Usage**

Used to provide a IPv6 ifid for the subscriber when using IPv6-to-IPv4 (6to4) routing.

**Example**

The following command provides an example of assigning an IPv6 interface ID of `00-00-00-05-47-00-37-44` to the subscriber:

```
ipv6 interface-id 00-00-00-05-47-00-37-44
```
**ipv6 minimum-link-mtu**

Configures the IPv6 minimum link maximum transmission unit (MTU) value.

**Product**
- PDSN
- GGSN
- ASN-GW
- P-GW
- SAEGW

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration > Context Configuration > Subscriber Configuration
- configure > context context_name > subscriber { default | name subscriber_name }

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

**Syntax**

```
ipv6 minimum-link-mtu value
```

```
default ipv6 minimum-link-mtu
```

---

**default ipv6 minimum-link-mtu**

- **default**

  Resets minimum link MTU to its default setting: 1280.

---

```
ipv6 minimum-link-mtu value
```

**value** specifies the MTU (in bytes) as a minimum link value. `value` is an integer between 100 and 2000.

---

**Usage**

Used to override the IPv6 minimum link MTU values recommended by the standard.

**Example**

The following command provides an example of assigning an IPv6 minimum link MTU to 1580 to the subscriber:

```
ipv6 minimum-link-mtu 1580
```
**ipv6 secondary-address**

Configures additional IPv6 4-bit prefixes to the subscriber session.

**Product**
- PDSN
- GGSN
- ASN-GW
- P-GW
- SAEGW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Subscriber Configuration

```
configure > context context_name > subscriber { default | name subscriber_name }
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

**Syntax**

```
[ no ] ipv6 secondary-address { prefix ipv6_address_prefix | prefix-pool pool_name }
```

- **no**
  Deletes a previously configured ipv6 secondary address.

- **ipv6 secondary-address ipv6_address_pref**
  Specified the secondary IPv6 address using IPv6 colon-separated-hexadecimal notation.

- **pool_name**
  Specifies the name given to the secondary address prefix pool as an alphanumeric string of of 1 through 31 characters.

**Usage**

An IPv6 prefix pool name may be configured for a dynamic prefix, while the prefix is static. This command may be executed multiple times to configure multiple prefixes.

**Example**

The following command assigns an IPv6 secondary address prefix-pool name of `eastcoast` to the subscriber:

```
ipv6 secondary-address prefix-pool eastcoast
```
l2tp send accounting-correlation-info

Enables the sending of accounting correlation information (Correlation-Id, NAS-IP-Address and NAS-ID) by the L 2TP Access Concentrator (LAC) in L2TP control messages (ICRQ) during session setup to an L2TP Network Server (LNS).

Product
PDSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context context_name > subscriber { default | name subscriber_name }

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-subscriber)#

Syntax

[ no | default ] l2tp send accounting-correlation-info

no
Disables the sending of accounting correlation information by the LAC.

default
Sets the setting to default mode: disable.

l2tp send accounting-correlation-info

Enables the sending of accounting correlation information by the LAC.

Usage

Use this command to enable the LAC to send accounting correlation information (Correlation-Id, NAS-IP-Address and NAS-ID) in L2TP control message (ICRQ) during session setup to LNS for this subscriber. LNS can be configured to include this information in ACS billing records, so that billing servers can easily correlate accounting records from PDSN/LAC and LNS.

By default, this mode is disabled.

Example

The following command disables the inclusion of accounting correlation information in control messages during session setup to an LNS for a subscriber:

    default l2tp send accounting-correlation-info
I3-to-l2-tunnel address-policy

Configure the subscriber address allocation/validation policy, when subscriber Layer 3 (IPv4) sessions are tunneled using Layer 2 tunneling protocol (L2TP).

Product
HA
GGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Subscriber Configuration
configure > context context_name > subscriber { default | name subscriber_name }

Syntax
l3-to-l2-tunnel address-policy { alloc-only | alloc-validate | no-alloc-validate }

default l3-to-l2-tunnel address-policy

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Restores the default value for Layer 3-to-Layer 2 tunnel addressing: no-alloc-validate.</td>
</tr>
<tr>
<td>l3-to-l2-tunnel address-policy</td>
<td>Sets the policy for Layer 3-to-Layer 2 sessions to one of the following options.</td>
</tr>
<tr>
<td>alloc-only</td>
<td>Only allocates an address in the case of dynamic address assignment. Does not validate static addresses.</td>
</tr>
<tr>
<td>alloc-validate</td>
<td>Locally allocates and validates the subscriber addresses.</td>
</tr>
<tr>
<td>no-alloc-validate</td>
<td>Does not allocate or validate subscriber addresses locally for current subscribers sessions. Passes the address between the remote tunnel terminator and the Mobile Node. This is the default behavior.</td>
</tr>
</tbody>
</table>

Usage
Use this command to configure the L3 to L2 tunnel address policy for MIP HA sessions tunneled from the system using L2TP tunnels or for GGSN IP Context sessions tunneled using L2TP to a remote LNS. Also refer to the resource keyword of the Context Configuration mode ip pool command.

Example
the following command sets the L3-to-L2 tunnel address policy so that the current subscriber must have IP addresses allocated and validated locally on the system:
13-to-12-tunnel address-policy alloc-validate
loadbalance-tunnel-peers

Configures the load balancing of traffic bound for L2TP tunnels configured on the system for the selected subscriber.

**Product**
L2TP

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Subscriber Configuration
configure > context context_name > subscriber { default | name subscriber_name }

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

**Syntax**

```
loadbalance-tunnel-peers { balanced | prioritized | random }
```

- **loadbalance-tunnel-peers**
  Enables load balancing of L2TP traffic using one of the methods described below.

- **balanced**
  Enables the equal use of all configured tunnel peers (LNSs) for the selected subscriber.

- **prioritized**
  Enables the use of all configured tunnel peers (LNSs) for the selected subscriber based on the preference number assigned to the peer address.

- **random**
  Default: Enabled
  Enables the random use of all configured tunnel peers (LNSs) for the selected subscriber.

**Usage**

Use to manage traffic loads on L2TP Access Concentrator (LAC) ports and their respective L2TP Network Servers (LNSs).

**Example**

Use the following command to randomly use all configured tunnel peers (LNSs):

```
loadbalance-tunnel peers random
```
long-duration-action

Specifies what action is taken when the long duration timer expires.

**Product**
All

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Subscriber Configuration

**Syntax**

```
long-duration-action { detection | disconnection [ dormant-only ] [ suppress-notification ] }
```

- **detection**
  Default: Enabled
  Detects long duration sessions and sends SNMP TRAP and CORBA notification. This is the default behavior. Use this command to detect a session exceeding the limit set by the long duration timer.

- **disconnection [ dormant-only ] [ suppress-notification ]**
  Default: Disabled
  Detects a long duration session and disconnects the session after sending SNMP trap and CORBA notification.
  
  **suppress-notification**: Suppresses the SNMP trap and CORBA notification after detecting and disconnecting a long duration session. Default: Disabled
  
  **dormant only**: Disconnects the dormant sessions after long duration timer and inactivity time with idle time-out duration expires. If the long duration timeout is fired and the call is not dormant, the call is disconnected when the call later moves to dormancy.

**Important**: For HA calls, the inactivity-time is considered as gauge for dormancy.

It sends the SNMP trap and CORBA notification after disconnecting a long duration session. Default: Disabled

**Usage**
Use this command to determine what action is taken when a session exceeds the limit set by the long duration timer.

**Example**
Use the following command to enable disconnecting sessions that exceed the long duration timer:

```
long-duration-action disconnection
```
Use the following command to disconnect the session that exceed the long duration timer without sending SNMP trap and CORBA notification:

```
long-duration-action disconnection suppress-notification
```

Use the following command to disconnect the session that is in dormant and exceed the long duration timer and send SNMP trap and CORBA notification:

```
long-duration-action disconnection dormant-only
```

Note that in case of HA calls, the inactivity-time is considered as gauge for dormancy.
max-pdn-connections

Specifies the maximum number of connections to packet data networks (PDNs) supported per eHRPD session.

Product
HSGW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Subscriber Configuration
configure > context context_name > subscriber { default | name subscriber_name }

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-subscriber)#

Syntax

max-pdn-connections eHRPD_PDNs

default max-pdn-connections

default

Resets the maximum number of PDN connections supported per eHRPD session to 3.

max-pdn-connections eHRPD_PDNs

Specifies the maximum number of PDN conceivedness allowed per eHRPD session. eHRPD_PDNs must be an
integer from 1 to 14. Default is 3.

Usage
This command is used to specify the maximum number of PDN connections supported per eHRPD session.

Example
The following command specifies a maximum of 5 PDNs per eHRPD session:

max-pdn-connections 5
mediation-device

Enables the use of a mediation device for subscribers, and specifies the system context to use for communicating with the device. A mediation device can be the initial point of contact for all IT systems that need to receive Charging Data Records (CDRs). Mediation devices can also be deep-packet inspection servers or transaction control servers.

Product

- GGSN
- P-GW
- PDG/TTG
- SAEGW

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > Context Configuration > Subscriber Configuration

```
configure > context context_name > subscriber { default | name subscriber_name }
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

Syntax

```
mediation-device context-name <context-name> [ no interims ]
[ no | default ] mediation-device
```

---

no

Deletes the mediation-device configuration.

---

default

Changes the mediation device to no context-name configured and restores the mediation device’s default properties.

---

```
mediation-device context-name context-name
```

Default: The subscriber’s destination context.
Configures the mediation VPN context for the subscriber.
`context-name` must be an alphanumeric string of 1 through 79 characters that is case sensitive. If not specified, the mediation context is same as the destination context of the subscriber.

---

no-interims

Disables sending of Interim messages to the mediation device.
Default: Disabled
**Usage**

This command is used to enable mediation device support for subscribers. Keywords to this command can be used in combination to each other, depending on configuration requirements.

**Example**

The following command enables mediation device support for the subscriber and uses the protocol configuration located in an system context called `ggsn1`:

```
mediation-device context-name ggsn1
```
mobile-ip

Enables or disables access to mobile IP services by the subscriber.

Product
HA
FA

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Subscriber Configuration

class > context context_name > subscriber { default | name subscriber_name }

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-subscriber)#

Syntax

[ no ] mobile-ip { allow-aaa-address-assignment | dns-address source-priority { aaa | home-agent } | gratuitous-arp aggressive | home-agent ip_address [alternate] | match-aaa-assigned-address | min-reg-lifetime-override [value | infinit] | mn-aaa-removal-indication | mn-ha-hash-algorithm { hmac-md5 | md5 | rfc2002-md5 } | mn-ha-shared-key key | mn-ha-spi spi_num | reverse-tunnel | security-level { ipsec | none } | send {access-technology | accounting-correlation-info bsid | dns-address | host-config | imsi | terminal-verification } }

no

Disables the mobile IP option specified.

allow-aaa-address-assignment

Default: Disabled.

Enables the FA to accept a home address assigned by an AAA server. This should only be configured on the FA side.

dns-address source-priority { aaa | home-agent }

Sets the priority behavior on the FA to use either the DNS IP address information from the HA or the AAA server to include in the RRP to the MN.

When the no keyword is used in conjunction with the dns-address keyword, information received from both the home-agent and the AAA server is sent if available.

DNS IP address information from the HA comes from the DNS Normal Vendor/Organization Specific Extension (NVSE) in the Registry Registrar Protocol (RRP).

DNS IP address information from the AAA server is in the access accept message.

home-agent: If the DNS address is received from the home-agent only that information is sent to the MN.

Otherwise the DNS address received from the AAA server is sent.

aaa: If the DNS address is received from the AAA server only that information is sent to MN. Otherwise the DNS address received from the home-agent is sent.
gratuitous-arp aggressive

Default: Disabled.
When enabled, this mode will cause the HA to send out gratuitous ARP (Address Resolution Protocol) messages for all Mobile IP (MIP) registration renewals and handoffs.
To disable this mode, use the no form of this command.

Important: This mode will only work for IP addresses that have been assigned from a static IP address pool.

home-agent ip_address [alternate]

Specifies the IP address of the mobile IP user’s home agent. ip_address must be entered using IPv4 dotted-decimal or IPv6 colon-separated notation.
alternate - Specifies the secondary, or alternate, Home Agent to use when Proxy Mobile IP HA Failover is enabled.

match-aaa-assigned-address

Default: Disabled.
Enables the FA to validate the home address in the RRQ against the one assigned by AAA server. This should only be configured on the FA side.

min-reg-lifetime-override [value | infinit ]

Default: 0.
Configures the subscriber for minimum registration lifetime parameter on HA service. By default it uses the value configured on HA service where value must be the minimum registration lifetime that the HA service allows in any Registration Request message from the mobile node. An infinite registration lifetime can be configured by setting the value as “infinite”.
value is a minimum registration lifetime value in seconds and must be an integer between 1 through 65534.

mn-aaa-removal-indication

Default: Disabled.
When enabled, the MN-FA challenge and MN-AAA Authentication extensions are removed when relaying a Registration Request (RRQ) to the Home Agent (HA)

mn-ha-hash-algorithm { hmac-md5 | md5 | rfc2002-md5 }

Specifies the encryption algorithm to use.
Default: hmac-md5
hmac-md5: Uses HMAC-MD5 hash algorithm, as defined in RFC-2002bis. This is the default algorithm.
md5: Uses the MD-5 hash algorithm.
rfc2002-md5: Uses the MD-5 hash algorithm variant as defined in RFC-2002.

mn-ha-shared-key key

Verifies the MN-HA Authentication for a local subscriber in the current context. key is an alphanumeric string or a hexadecimal number beginning with "0x" up to 127 bytes

mn-ha-spi spi_num

Specifies the Security Parameter Index (SPI) number. spi_num must be an integer from 256 through 4294967295.
### reverse-tunnel

Default: enabled.
All the mobile IP user to use reverse IP tunnels. The `no` keyword disables this option.

### security-level \{ ipsec | none \}

Default: none
Configures the security level needed for the subscriber's traffic.
- `ipsec`: secures both MIP control and data traffic with IPsec.
- `none`: none of the traffic is secured

**Important**: This keyword corresponds to the 3GPP2-Security-Level RADIUS attribute. This attribute indicates the type of security that the home network mandates on the visited network.

**Important**: For this attribute, the integer value “3” enables IPsec for tunnels and registration messages, “4“ Disables IPsec

### send \{ access-technology | accounting-correlation-info bsid | dns-address | host-config | imsi | terminal-verification \}

- `access-technology`: Configures FA to sends the access-technology type extension in the RRQ, by default it is disabled.
- `accounting-correlation-info`: Configures whether the FA sends the correlation info to the NVSE in the RRQ. Default is disabled.
- `dns-address`: Enables the HA to send the DNS address NVSE in the RRP. Default is disabled. This should only be enabled on the HA side.
- `host-config`: Configures by sending the Host Config NVSE in RRQ. By default it is disabled.
- `imsi`: Configures sending the IMSI NVSE in the RRQ. Default is sending IMSI in custom-1 format.
- `terminal-verification`: Enables the FA to send the terminal verification NVSE in the RRQ. Default is disabled. This should only be enabled on the FA side.

**Important**: `send dns-address` is a proprietary feature developed for a specific purpose and requires the MN to be able to renegotiate IPCP for DNS addresses and reregister MIP if necessary. Since this feature needs the MN to support certain PPP/MIP behavior, and not all MNs support that particular behavior, `send dns-address` should be enabled only after careful consideration.

### Usage

Use as subscriber service contracts change.

### Example

```plaintext
  mobile-ip home-agent 10.2.3.4

  no mobile-ip reverse-tunnel
```
**mobile-ip ha**

Accommodates two Mobile IP (MIP) Home Agent (HA) options in subscriber mode.

**Product**
- PDSN
- HA
- ASN-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Subscriber Configuration

```
configure > context context_name > subscriber { default | name subscriber_name }
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

**Syntax**

```
[ no ] mobile-ip ha { assignment-table name | ignore-unknown-ha-addr-error }
```

- **no**
  Disables the mobile IP HA option specified.

  **assignment-table name**
  Specifies the name of an existing MIP HA Assignment table. *name* must be an alphanumeric string of 1 through 63 characters.

  **ignore-unknown-ha-addr-error**
  Default is disabled.
  Enables or disables the HA to accept or reject the RRQ from a particular subscriber.

**Usage**

Use this command to assign a MIP HA Assignment table to the current subscriber.

Use this command to disable or enable the HA to accept or reject the RRQ from a particular subscriber when the HA address in the incoming MIP RRQ is not the same as the HA service address. The feature is off by default which causes the RRQ to be rejected with the error code UNKNOWN_HOME_AGENT.

**Example**

The following command assigns the MIP HA Assignment table named *Atable1* to the current subscriber:

```
mobile-ip ha assignment-table Atable1
```

The following command sets *ignore-unknown-ha-addr-error* to its default disabled state:

```
no mobile-ip ha ignore-unknown-ha-addr-error
```
mobile-ip reg-lifetime-override

Overrides the Mobile IP (MIP) registration lifetime from HA with value configured for subscriber.

Product
- PDSN
- HA
- ASN-GW

Privilege
- Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Subscriber Configuration
configure > context context_name > subscriber { default | name subscriber_name }

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-subscriber)#

Syntax

mobile-ip reg-lifetime-override [ dur | infinite ]

[ default | no ] mobile-ip reg-lifetime-override

---

mobile-ip reg-lifetime-override dur

Default: 100 seconds.
Overrides the MIP registration lifetime from HA for the specified period of time in seconds. dur must be an integer from 1 through 65534.

---

infinite

Sets the MIP registration lifetime override value to infinite for a particular subscriber.

---

default

Sets the value of mobile IP registration lifetime override option to 100 seconds.

---

no

Disables the MIP registration lifetime override option.

Usage

Use this command to configure MIP registration-lifetime per realm/domain. This value overrides the default lifetime configured under HA service.

Example

The following command overrides the MIP registration lifetime value from HA service and defaults the MIP registration lifetime to 100 seconds for the current subscriber:

default mobile-ip reg-lifetime-override
**mobile-ip send access-technology**

Enables the sending of the RAT (Radio Access Technology) of the MS to the HA in a PMIP RRQ (Proxy MIP Register Request) message.

**Product**
PDIF
PDSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Subscriber Configuration

```
configure > context context_name > subscriber { default | name subscriber_name }
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

**Syntax**

```
[ default | no ] mobile-ip send access-technology
```

### default

Disables the support for sending the RAT to the HA in a PMIP RRQ.
This is the default mode.

### no

Removes the configured support for sending the RAT to the HA in a PMIP RRQ.

**Usage**

Use this command to send the RAT to the HA in a PMIP RRQ.

**Example**

The following command enables sending the RAT to the HA in a PMIP RRQ:

```
mobile-ip send access-technology
```
**mobile-ip send accounting-correlation-info**

Enables the sending call correlation information Normal Vendor/Organization Specific Extensions (NVSEs) to the HA in the MIP Registry Registrar Protocol (RRP).

**Product**  
PDSN

**Privilege**  
Security Administrator, Administrator

**Mode**  
Exec > Global Configuration > Context Configuration > Subscriber Configuration

```
configure > context context_name > subscriber { default | name subscriber_name }
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

**Syntax**

```
[ default | no ] mobile-ip send accounting-correlation-info
```

**default**  
Disables the support for sending call correlation information NVSEs to the HA in MIP RRQ. This is the default mode.

**no**  
Removes the configured support for sending call correlation information.

**Usage**  
Use this command to support PDSN-Correlation-ID VSE and send the call correlation information.

**Example**  
The following command enables sending call correlation information NVSEs to the HA in MIP RRQ

```
mobile-ip send accounting-correlation-info
```
mobile-ip send bsid

Enables the sending of the BSID (Base Station Identifier) of the WiFi access point/Radio Access Network (RAN) to the HA in a PMIP RRQ (Register Request) message.

Product
PDIF
PDSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context context_name > subscriber { default | name subscriber_name }

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-subscriber)#

Syntax

[ default | no ] mobile-ip send bsid

---

**default**

Disables the support for sending the BSID to the HA in a PMIP RRQ.
This is the default mode.

**no**

Removes the configured support for sending the BSID to the HA in a PMIP RRQ.

---

Usage

Use this command to send the BSID to the HA in a PMIP RRQ.

Example

The following command enables sending the BSID to the HA in a PMIP RRQ:

```plaintext
mobile-ip send bsid
```
mobile-ipv6

Configures Mobile IPv6 related parameters for a subscriber.

**Product**

PDSN

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

```
configure > context context_name > subscriber { default | name subscriber_name }
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

**Syntax**

```
[ default | no ] mobile-ipv6 { home-address ipv6_address | home-agent ipv6_address | home-link-prefix ipv6_address | tunnel mtu value }
```

---

**default**

Disables the support for sending call correlation information NVSEs to the HA in MIP RRQ. This is the default mode.

---

**no**

Removes the configured support for sending call correlation information.

---

**home-address ipv6_address**

Specifies the home address for the subscriber. `ipv6_address` must be entered using IPv6 colon-separated-hexadecimal notation.

---

**home-agent ipv6_address**

Specifies the IPv6 address of the mobile IP user’s home agent. `ipv6_address` must be entered using IPv6 colon-separated-hexadecimal notation.

---

**home-link-prefix ipv6_address**

Specifies the IPv6 address of the mobile IP user’s home link. `ipv6_address` must be entered using IPv6 colon-separated-hexadecimal notation.

---

**tunnel mtu value**

Configures the tunnel MTU (in bytes) for the IPv6 tunnel between the HA and the mobile node. `value` must be an integer from 1024 through 2000. The default is 1500.
Usage
This command sets the mobile-ipv6 parameters for a subscriber. Use this command to set the home-address, home-agent, and home-link prefix.

Example
Use the following command to set the tunnel MTU value to 1800:

```
mobile-ipv6 tunnel mtu 1800
```
nai-construction-domain

After authentication, the domain name specified by this command replaces the Network Access Identifier (NAI) constructed for the subscriber.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context context_name > subscriber { default | name subscriber_name }

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-subscriber)#

Syntax

nai-construction-domain domain_name

no nai-construction-domain

Define or delete a domain name to use to replace the NAI constructed domain name after authentication. The following command sets the domain name to privatel:

nai-construction-domain privatel

To delete the previously configured domain name, use the following command:

no nai-construction-domain
nbns

Configures and enables use of NetBIOS Name Service for the subscriber.

Product
GGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Subscriber Configuration

\texttt{configure > context context\_name > subscriber \{ default | name subscriber\_name \}}

Entering the above command sequence results in the following prompt:

\texttt{[context\_name]host\_name(config-subscriber)\#}

Syntax

\texttt{nbns \{ primary \ IPv4\-address | secondary \ IPv4\-address \}}

\texttt{no nbns \{ primary \ IPv4\-address | secondary \ IPv4\-address \}}

\texttt{nbns primary}

Designates primary NBNS server. Must be followed with IPv4 address in dotted-decimal notation.

\texttt{nbns secondary}

Designates secondary/failover NBNS server. Must be followed with IPv4 address in dotted-decimal notation.

\texttt{IPv4\-address}

Specifies the IP address used for this service using IPv4 dotted-decimal notation.

\texttt{no}

Removes/disables use of a previously configured NetBios Name Service.

Usage

This command specifies NBNS parameters. The NBNS option is present for both PDP type IP and PDP type PPP for GGSN.

The system can be configured to use of NetBIOS Name Service for the Access Point Name (APN).

Example

The following command configures the subscriber’s NetBIOS Name Service to primary IP 192.168.1.15:

\texttt{nbns primary 192.168.1.15}
nexthop-forwarding-address

Configures the next hop forwarding address for the subscriber.

**Product**
- PDSN
- GGSN
- ASN-GW
- P-GW
- SAEGW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Subscriber Configuration
configure > context context_name > subscriber { default | name subscriber_name }

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

**Syntax**

```
nexthop-forwarding-address ip_address

no nexthop-forwarding-address
```

```
nexthop-forwarding-address ip_address

Configures the IP address of the nexthop forwarding address. ip_address must be entered using IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

no

Disables this function. This is the default setting.
```

**Usage**

Use this command to configure the next hop forwarding address for the subscriber.

**Example**

The following command configures the next hop forwarding address to 10.1.1.1 (IPv4):

```
nexthop-forwarding-address 10.1.1.1
```
npu qos

Configures an Network Processing Unit (NPU) QoS priority queue for packets from the subscriber.

**Product**

- PDSN
- GGSN
- ASN-GW
- P-GW
- SAEGW

**Privilege**

- Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

```
configure > context context_name > subscriber { default | name subscriber_name }
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

**Syntax**

```
npu qos traffic priority { best-effort | bronze | derive-from-packet-dscp | gold | silver }
```

- **best-effort**
  
  Assigns the best-effort queue priority. This is the lowest priority.

- **bronze**
  
  Assigns the bronze queue priority. This is the third-highest priority.

- **derive-from-packet-dscp**
  
  Default: Enabled
  
  Specifies that the priority is to be determined from the DS field in the packet's TOS octet.

- **gold**
  
  Assigns the gold queue priority. This is the highest priority.

- **silver**
  
  Assigns the silver queue priority. This is the second-highest priority.

**Usage**

This command is used in conjunction with the Network Processing Unit (NPU) Quality of Service (QoS) functionality.
The system can be configured to determine the priority of a subscriber packet either based on the configuration of the subscriber, or from the differentiated service (DS) field in the packet's TOS octet (representing the differentiated service code point (DSCP) value). Refer to the *System Administration Guide* for additional information on NPU QoS functionality.

**Important:** This functionality is not supported for use with the PDSN at this time.

**Example**

The following command configures the subscriber’s priority queue to be gold:

```
npu qos traffic priority gold
```
nw-reachability-server

Binds the name of a configured network reachability server to the current subscriber and enables network reachability detection.

**Product**
HA

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Subscriber Configuration

```
configure > context context_name > subscriber { default | name subscriber_name }
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

**Syntax**

```
w
t-reachability server server_name

no nw-reachability server
```

- **nw-reachability server** server_name
  - Specifies the name of a network reachability server that has been defined in the current context.
  - server_name is an alphanumeric string of 1 through 16 characters.

- **no nw-reachability server**
  - Deletes the name of the network reachability server from the current subscriber’s configuration and disable network reachability failure detection for the current subscriber.

**Usage**

Use this command to define the network reachability server for the current subscriber and enable network reachability failure detection for the current subscriber. If a network reachability server is defined in an IP pool, that setting takes precedence over this command.

**Important:** Refer to the HA configuration mode command **policy nw-reachability-fail** to configure the action that should be taken when network reachability fails.

**Important:** Refer to the context configuration mode command **nw-reachability server** to configure network reachability servers.

**Important:** Refer to the **nw-reachability server server_name** keyword of the **ip pool** command in the Context Configuration Mode Commands chapter to bind the network reachability server to an IP pool.

**Example**

Cisco ASR 5x00 Command Line Interface Reference
To bind a network reachability server named *InternetDevice* to the current subscriber, enter the following command:

```
nw-reachability server InternetDevice
```
**outbound**

Configures the subscriber host password for use when authenticating PPP sessions.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Subscriber Configuration

```bash
configure > context context_name > subscriber { default | name subscriber_name }
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

**Syntax**

```
outbound [ encrypted ] password pwd

no outbound password
```

```
[ outbound encrypted ] password pwd
```

Specifies the password to use for point-to-point protocol session host authentication. The `encrypted` keyword indicates the password specified uses encryption. The password specified as `pwd` must be an alphanumeric string of 1 through 63 characters without encryption, or 1 through 127 characters with encryption. The `encrypted` keyword is intended only for use by the chassis while saving configuration scripts. The system displays the `encrypted` keyword in the configuration file as a flag that the variable following the `password` keyword is the encrypted version of the plain text password. Only the encrypted password is saved as part of the configuration file.

```
no outbound password
```

Clears the outbound password configuration from the subscriber data.

**Usage**

Sets the outbound (egress) password for increased security.

**Example**

```
outbound password secretPwd

outbound encrypted password scrambledPwd

no outbound password
```
overload-disconnect

Sets the threshold parameter for overload disconnect.

**Product**
ASN-GW
HA
PDIF
PDSN
PHSGW
PDG/TTG

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Subscriber Configuration
configure > context context_name > subscriber { default | name subscriber_name }

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

**Syntax**

```plaintext
overload-disconnect [ threshold { inactivity-time inactivity_time_threshold | connect-time connect_time_threshold } ]

[ default | no ] overload-disconnect [ threshold { inactivity-time | threshold connect-time } ]
```

---

**threshold inactivity-time inactivity_time_threshold**

Sets the inactivity time threshold (in seconds) as an integer from 0 through 4294967295. The default value of zero disables this feature. If inactivity-time for the subscriber’s session is greater than inactivity_time_threshold, the session becomes a candidate for disconnection.

---

**threshold connect-time connect_time_threshold**

Sets the connection time threshold (in seconds) as an integer from 0 through 4294967295. A value of zero disables this feature. If connect-time for the subscriber’s session is greater than connect_time_threshold, the session becomes a candidate for disconnection.

---

**default**

Enables the default condition for this subscriber.

---

**no**

Disables the overload disconnect feature for this subscriber. This is the default condition for PDIF.
**overload-disconnect**

**Usage**

Set a subscriber’s overload disconnect threshold in seconds, based on either inactivity or connection time. When this threshold is exceeded during a session, the subscriber’s session becomes a candidate for disconnection. To set overload-disconnect policies for the entire chassis, see `congestion-control overload-disconnect` in the *Global Configuration Mode Commands* chapter.

**Example**

```plaintext
overload-disconnect threshold inactivity-time 120
default overload disconnect threshold connect-time
no overload-disconnect threshold connect-time
no overload disconnect
```
password

Configures the subscribers password for the current context.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context context_name > subscriber { default | name subscriber_name }

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-subscriber)#

Syntax

[ encrypted ] password pwd

no password

encrypted

Indicates the password provided is encrypted.
The encrypted keyword is intended only for use by the chassis while saving configuration scripts. The system displays the encrypted keyword in the configuration file as a flag that the variable following the password keyword is the encrypted version of the plain text password. Only the encrypted password is saved as part of the configuration file.

pwd

Specifies the user’s password for authentication. pwd must be an alphanumeric string of 1 through 63 characters without encryption, or from 1 through 127 characters with encryption. A “null” password is allowed and is entered as consecutive double quotes (" "). See Example(s) for correct syntax.

Important: Subscribers configured with a null password will be authenticated using PAP and CHAP (MD5) only. Subscribers configured without a password (no password) will only be able to access services if the service is configured to allow no authentication.

no

Used to clear the subscriber password configuration from the subscriber data.

Important: Subscribers with no password will only be able to access services if the service is configured to grant access with no authentication.
Password management is critical to system security and all precautions should be taken to ensure passwords are not shared or to easily deciphered.

**Example**

```
password secretPwd

password ""

no password
```
pdif mobile-ip

Configures PDIF subscriber call setup parameters.

Product
PDIF

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context context_name > subscriber { default | name subscriber_name }

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-subscriber)#

Syntax

[ default | no ] pdif mobile-ip { release-tia | required | simple-ip-fallback }

- [ default | no ]
  Disables the option specified.

- release-tia
  Specifies that after subscriber call setup is complete, the tunnel inner address (TIA) is released. If Simple IP is enabled, the TIA becomes the principal communications tunnel and the restriction that it is only to be used to set up a Mobile-IP call is lifted. This parameter is disabled by default.

- required
  Specifies that Mobile IP is required for this subscriber whenever a call is set up. This parameter is disabled by default.

- simple-ip-fallback
  Specifies that Simple IP should be used when Mobile IP could not be established. This parameter is disabled by default.

Usage

Use this command to configure specific behavior for the PDIF subscriber during call setup.

Example

The following command enables the system to fall back to Simple IP when Mobile IP fails for this subscriber during call setup:

    pdif mobile-ip simple-ip-fallback
permission

Enables or disables the subscriber’s ability to access wireless data services.

Product

- PDSN
- HA

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context context_name > subscriber { default | name subscriber_name }

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-subscriber)#

Syntax

[ no ] permission { ha-mobile-ip | pdsn-mobile-ip | pdsn-simple-ip }

default permission

| no | default
|---|---
| Disables the usage of the specified service.

| ha-mobile-ip | pdsn-mobile-ip | pdsn-simple-ip
|---|---|---
| ha-mobile-ip: Enables or disables the Home Agent (HA) support for Mobile IP (MIP) service.
| pdsn-mobile-ip: Enables or disables packet data and Foreign Agent (FA) support for MIP service.
| pdsn-simple-ip: Enables or disables packet data support for simple IP service.

Usage

Grants the subscriber access to services in the current context.

Example

```
permission pdsn-mobile-ip
no permission ha-mobile-ip
```
policy ipv6 tunnel

Sets maximum transmission unit (MTU) behavior for the IPv6 tunnel between the HA and Mobile Node.

Product
PDSN
HA

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context context_name > subscriber { default | name subscriber_name }

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-subscriber)#

Syntax

policy ipv6 tunnel mtu exceed { fragment | notify-sender }

mtu exceed { fragment | notify-sender }
fragment: Adjusts tunnel MTU and fragment packets
notify-sender: Sends an ICMPv6 Packet Too Big message to the original sender

Usage
Use this command to configure MTU behavior for an IPv6 tunnel between the HA and Mobile Node.

Example

policy ipv6 tunnel mtu exceed fragment
policy-group

Assigns or removes a flow-based traffic policy group to a subscriber.

Product

PDSN
HA
ASN-GW
HSGW

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context context_name > subscriber { default | name subscriber_name }

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-subscriber)#

Syntax

[ no ] policy-group policy_group_name direction { in | out }

| no |

Removes assigned policy group from a subscriber configuration.

| policy-group policy_group_name |

Specifies the traffic policy group name for a subscriber session flow pre-configured within a destination context. policy_group_name is an alphanumeric string of 1 through 15 characters that is case sensitive.

direction { in | out }

Specifies the direction of flow in which the traffic policies need to be applied.

• in: specifies the incoming traffic
• out: specifies the outgoing traffic

Usage

Use this command to assign a traffic policy group to a subscriber for traffic policing.

Example

policy-group traffic_policy_group1 direction in
ppp

Configures the point-to-point protocol (PPP) options for the current subscriber.

Product
PDSN
PDSN Closed R-P
GGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context context_name > subscriber { default | name subscriber_name }

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-subscriber)#

Syntax

ppp { accept-peer-ipv6-ifid | always-on-vse-packet | data-compression { mode { normal | stateless } | protocols { protocols [ protocols ] } | ip-header-compression negotiation { detect | force | vj compress-slot-id { both | none | receive | transmit } } | ipv4 { disable | enable | passive } | ipv6 { disable | enable | passive } | keepalive seconds | min-compression-size min_octets | mtu max_octets | remote-renegotiation disconnect { always | nai-prefix-msid-mismatch } )

default ppp { accept-peer-ipv6-ifid | always-on-vse-packet | data-compression { mode | protocols } | ip-header-compression negotiation [ vj compress-slot-id ] | ipv4 | ipv6 | keepalive | min-compression-size | mtu | remote-renegotiation disconnect }

no ppp { accept-peer-ipv6-ifid | always-on-vse-packet | data-compression protocols | ipv4 | ipv6 | keepalive | mtu | remote-renegotiation disconnect }

default

Restores the default value for the option specified.

no

Resets the option specified to its default.

always-on-vse-packet

Default: Enabled
If this feature is enabled, the PDSN sends special 3GPP2 VSE PPP packets to the Mobile Node with a maximum inactivity timer value. This configuration is applicable only for PDSN sessions.

accept-ipv6-peer-ifield

Default: None
Configures an IPv6-to-IPv4 (6to4) tunnel and controls the behavior of IPv6CP negotiation for the Interface ID. If enabled, PDSN will accept a valid interface-id proposed by the peer.

```
data-compression { mode { normal | stateless } | protocols { protocols } }
```

Default: all protocols enabled. Specifies the subscriber’s mode of data compression or the compression protocol to use.

- **mode**: sets the mode of compression where *modes* must be one of:
  - `normal`: Packets are compressed using the packet history for automatic adjustment for best compression.
  - `stateless`: Each packet is compressed individually.

- **protocols**: sets the compression protocol where *protocols* must be one of:
  - `deflate`: DEFLATE algorithm
  - `mppc`: Microsoft PPP algorithm
  - `stac`: STAC algorithm

```
ip-header-compression negotiation { detect | force | vj compress-slot-id { both | none | receive | transmit } }
```

Default: `force`

- **detect**: The local side does not include the Van Jacobson (VJ) Compression option in its IPCP configuration request unless the peer sends an Internet Protocol Control Protocol (IPCP) NAK including a VJ compression option. If the peer requests the VJ compression option in its IPCP request the local side will ACK/NAK.

- **force**: The IP header compression negotiation in IPCP happens normally. The local side requests the VJ compression option in its IPCP configure request. If the peer side requests VJ compression in its IPCP request, the local side will ACK/NAK the option.

- **vj compress-slot-id**: Configures the direction in which VJ slotid compression should be negotiated.
  - `both`: If the client proposes VJ slotid compression, accept it and propose slotid compression for the downlink and uplink.
  - `none`: If the client proposes VJ slotid compression, NAK the offer, do not propose slotid compression for the downlink.
  - `receive`: (Default) If the client proposes VJ slotid compression in the uplink direction accept the configuration.
  - `transmit`: Propose VJ slotid compression for uplink.

```
ipv4 { disable | enable | passive }
```

Default: `enable`

Controls IPCP negotiation during PPP negotiation.

- **disable**: The PDSN does not negotiate IPCP with the mobile.
- **enable**: The PDSN negotiates IPCP with the mobile.
- **passive**: The PDSN initiates IPCP only when the mobile sends an IPCP request.

```
ipv6 { disable | enable | passive }
```

Default: `enable`

Controls IPv6CP negotiation during PPP negotiation.

- **disable**: The PDSN does not negotiate IPCP with the mobile.
enable: The PDSN negotiates IPCP with the mobile.
passive: The PDSN initiates IPCP only when the mobile sends an IPCP request.

```
keepalive seconds
```

Default: 30
Specifies the frequency of sending the Link Control Protocol keepalive messages. *seconds* must be either 0 or an integer from 5 through 14400. The special value 0 disables the keepalive messages entirely.

```
min-compression-size min_octets
```

Default: 128
Specifies the smallest packet (in octets) to which compression may be applied. *min_octets* must be an integer from 0 through 2000.

```
mtu max_octets
```

Default: 1500
Specifies the maximum transmission unit (MTU) [in octets] for packets. *max_octets* must be an integer from 100 through 2000.

```
remote-renegotiation disconnect { always | nai-prefix-msid-mismatch }
```

Default: Disabled
Terminates the already established PPP sessions if they are renegotiated by the remote side by sending LCP Conf-req/nak/ack. The following termination conditions are available:

- **always**: Automatically disconnects the session.
- **nai-prefix-msid-mismatch**: Disconnects the session only if the MSID of the session does not match NAI-Prefix (prefix before “@” for the NAI). The configuration of the renegotiated (new) NAI is used for the matching process.

**Usage**

Adjust packet sizes and compression to improve bandwidth utilization. Each network may have unique characteristics such that determining the best packet size and compression options may require system monitoring over an extended period of time.

**Example**

```
ppp data-compression protocols mode stateless
ppp mtu 500
no ppp data-compression protocols
no ppp keepalive
```
prepaid 3gpp2

Enables 3GPP2 compliant prepaid billing support for a subscriber to be configured by 3GPP2 attributes sent from a RADIUS server. If not enabled, prepaid attributes received from the RADIUS server are ignored.

Product
PDSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context context_name > subscriber { default | name subscriber_name }

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-subscriber)#

Syntax

prepaid 3gpp2 { accounting [ no-final-access-request ] | duration-quota final-duration-algorithm { current-time | last-airlink-activity-time | last-user-layer3-activity-time } | preference { duration | volume } }

default prepaid 3gpp2 { duration-quota final-duration-algorithm | preference }

no prepaid 3gpp2 accounting

default prepaid 3gpp2 { duration-quota final-duration-algorithm | preference }

Sets the 3GPP2 Pre-paid settings to the default values.

duration-quota final-duration-algorithm: Resets the end of billing duration quota algorithm to the default of current-time.

preference: Resets the preference to duration, If both duration and volume attributes are present.

no prepaid 3gpp2 accounting

Disables 3GPP2 prepaid accounting. All 3GPP2 Prepaid attributes received from a RADIUS server are ignored.

accounting [ no-final-access-request ]

Default: Disabled

Enables 3GPP2 prepaid accounting behavior.

Sets the low-watermark for remaining byte credits. percentage is a percentage of the subscriber sessions total credits. When the low-watermark is reached a new RADIUS access-request is sent to the RADIUS server to retrieve more credits. percentage must be an integer from 1 through 99.

no-final-access-request: Stops sending final online access-request on termination of 3GPP2 prepaid sessions. By default, this option is disabled.
duration-quota final-duration-algorithm { current-time | last-airlink-activity-time | last-user-layer3-activity-time }

Defines what behavior marks the end of the billing duration for duration-based quota usage accounting. The default behavior sets the duration quota algorithm to current-time.
Default: current-time

- **current-time**: Selects the duration quota as the difference between the session termination timestamp and the session setup timestamp.
- **last-airlink-activity-time**: Selects the duration quota as the difference between the last-user-activity timestamp (G17) and the session setup timestamp.
- **last-user-layer3-activity-time**: Selects the duration quota as the difference between the timestamp of the last layer-3 packet sent to or received from the user and the session setup timestamp.

preference { duration | volume }

If both duration and volume RADIUS attributes are present this keyword specifies which attribute has precedence.
Default: duration

- **duration**: The duration attribute takes precedence.
- **volume**: The volume attribute takes precedence

Usage

Use this command to enable prepaid support for a default user or for the default user of a domain alias.

Example

The following command enables 3GPP2 prepaid support for the default user:

```
prepaid 3gpp2 accounting
```
prepaid custom

Enables custom prepaid billing support for a subscriber to be configured by attributes sent from a RADIUS server. If not enabled, prepaid attributes received from the RADIUS server are ignored. The keywords set prepaid values that are used if the corresponding RADIUS attribute is not present. If the RADIUS attribute is present, it takes precedence over these values.

Product
PDSN
HA

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context context_name > subscriber { default | name subscriber_name }

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-subscriber)#

Syntax

prepaid custom { accounting | byte-count compressed | low-watermark percent percentage | renewal interval seconds } | preference { duration | volume }

default prepaid custom { byte-count | low-watermark }

no prepaid custom { accounting | byte-count compressed | low-watermark | renewal }

default prepaid custom { byte-count | low-watermark }

Resets custom prepaid settings to the default values.

byte-count: Resets the default of basing the prepaid byte credits on the flow of uncompressed traffic.

low-watermark: Disables sending an access request to retrieve more credits when a low watermark is reached.

no prepaid custom { accounting | byte-count compressed | low-watermark | renewal }

byte-count compressed: The prepaid byte credits are based on the flow of uncompressed traffic. This is the default.

low-watermark: Disables the low watermark feature. An access-request is not sent to the RADIUS server until the credits granted for the subscriber session are depleted.

renewal: Disables time-based renewals for prepaid accounting.

accounting
Default: Disabled
Enables custom prepaid accounting behavior.

byte-count compressed
Default: uncompressed.
When compression is used, the prepaid byte credits are based on the flow of compressed traffic. The default is to base the prepaid byte credits on the flow of uncompressed traffic.

**low-watermark percent percentage**

Default: Disabled.
Sets the low-watermark for remaining byte credits. *percentage* is a percentage of the subscriber sessions total credits. When the low-watermark is reached a new RADIUS access-request is sent to the RADIUS server to retrieve more credits. *percentage* must be an integer from 1 through 99.

**renewal interval seconds**

Default: The time in seconds to wait before sending a new RADIUS access-request to the RADIUS server to retrieve more credits. *seconds* must be an integer from 60 through 65535.

**preference { duration | volume }**

If both duration and volume RADIUS attributes are present this keyword specifies which attribute has precedence.
Default: duration
duration: The duration attribute takes precedence.
volume: The volume attribute takes precedence

**Usage**

Use this command to enable prepaid support for a default user or for the default user of a domain alias.

**Example**

The following command enables custom prepaid support for the default user:

```
prepaid custom accounting
```
prepaid unclassify

This command provides customer specific functionality.
prepaid voice-push

This command provides customer specific functionality.
**prepaid wimax**

Enables WiMAX prepaid accounting for this subscriber. This feature is disabled by default.

**Product**

ASN-GW

**Privilege**

Administrator

**Mode**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

```
configure > context context_name > subscriber { default | name subscriber_name }
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

**Syntax**

```
[ no ] prepaid wimax accounting
```

no

Disables WiMAX prepaid accounting for this subscriber.

**Usage**

Use this command to enable WiMAX prepaid accounting for this subscriber.
proxy-dns intercept list-name

Identifies a proxy DNS intercept rules list for the selected subscriber.

Product
HA

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context context_name > subscriber { default | name subscriber_name }

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-subscriber)#

Syntax

[ no ] proxy-dns intercept list-name name

no

Removes the intercept list from the subscribers profile.

proxy-dns intercept list-name name

Specifies a name of a proxy DNS intercept list used for the selected subscriber.

name is the name of the intercept list expressed as an alphanumeric string of 1 through 63 characters.

Usage

Use this command to identify a proxy DNS rules list for the selected subscriber. For a more detailed explanation of the HA Proxy DNS Intercept feature, see the proxy-dns intercept-list command in the Context Configuration Mode Commands chapter.
proxy-mip

Configures support for Proxy Mobile IP for the subscriber.

**Product**
- PDSN
- GGSN
- ASN-GW
- PDIF

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Subscriber Configuration
configure > context context_name > subscriber { default | name subscriber_name }

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

**Syntax**

```
[ no ] proxy-mip required
```

- `no`
  Disables support for Proxy Mobile IP.

- `required`
  Enables support for Proxy Mobile IP.

**Usage**
When enabled through the session license and feature use key, the system supports Proxy Mobile IP to provide a mobility solution for subscribers with mobile nodes (MNs) capable of supporting only Simple IP. For subscriber sessions using Proxy Mobile IP, R-P and PPP sessions are established as they would for a Simple IP session. However, the AGW/FA performs Mobile IP operations with an HA (identified by information stored in the subscriber’s profile) on behalf of the MN while the MN performs only Simple IP processes.

**Example**
The following command enables proxy mobile IP for the current subscriber:

```
proxy-mip required
```
qos apn-ambr

Configures the rate limit according to the APN-AMBR to do the session level bandwidth control per direction, according to the QoS information provided by the PCRF on the Gx interface.

Important: This command is customer specific. For more information contact your Cisco account representative.

Product
PDSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Subscriber Configuration
configuration > context context_name > subscriber { default | name subscriber_name }

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-subscriber)#

Syntax

qos apn-ambr rate-limit { downlink | uplink } [ burst-size bytes ] [ violate-action { drop | lower-ip-precedence | transmit } ]

no qos apn-ambr rate-limit

no

Disables the QoS data rate limit configuration for the subscriber.

downlink

Applies the specified limits and actions to the downlink (to the data coming from the GGSN over the Gn’ interface).

uplink

Applies the specified limits and actions to the uplink (to the data coming from the UE over the IPSec tunnel).

Important: If this keyword is omitted, the same values are used for all classes.

burst-size bytes

Default: See the Usage section for this command
The burst size allowed (in bytes) for peak data rate and committed data rate.
bytes must be an integer from 1 through 6000000.

Important: The minimum value of this parameter should be configured to the greater of the following two values: 1) three times greater than the packet MTU for the subscriber connection, OR 2) three seconds worth of token
accumulation within the “bucket” for the configured peak-data-rate. If the committed-data-rate parameter is specified, the burst-size is applied to both the committed and peak rates.

violate-action { drop | lower-ip-precedence | transmit }

Default: See the Usage section for this command
Specifies the action to take on packets that exceed both the committed-data-rate and the peak-data-rate. The following actions are supported:
• drop: Drops the packets.
• lower-ip-precedence: Transmits the packets after lowering the IP precedence.
• transmit: Transmits the packet.

Usage
This command configures the rate limit according to the APN-AMBR to do the session level bandwidth control per direction, according to the QoS information provided by the PCRF on the Gx interface. This command specifies the actions to take on subscriber flows exceeding or violating allowed peak or committed data rates.

Example
The following example configures the rate limit and burst size according to the APN-AMBR for the uplink direction. Policing is done for the traffic based on PCRF value received and traffic is dropped as the violate action is specified as drop.

    qos apn-ambr rate-limit direction uplink burstsize 1 violate-action drop
**qos rate-limit**

Configure the action on subscriber traffic flow that violates or exceeds the peak/committed data rate under traffic policing functionality. When configured, the PDG/TTG performs traffic policing for the subscriber session. If the GGSN changes the QoS via an Update PDP Context Request, the PDG/TTG uses the new QoS values for traffic policing.

**Product**

PDG/TTG

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > Subscriber Configuration

```
configure > context context_name > subscriber { default | name subscriber_name }
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

**Syntax**

```
qos rate-limit { downlink | uplink } [ qci qci_val ] [ burst-size { bytes | auto-readjust [ duration dur ] } ] [ exceed-action { drop | lower-ip-precedence | transmit } ] [ violate-action { drop | lower-ip-precedence | shape [ transmit-when-buffer-full ] | transmit } ] [ violate-action { drop | lower-ip-precedence | shape [ transmit-when-buffer-full ] | transmit } ] [ exceed-action { drop | lower-ip-precedence | transmit } ] [ violate-action { drop | lower-ip-precedence | shape [ transmit-when-buffer-full ] | transmit } ] [ violate-action { drop | lower-ip-precedence | shape [ transmit-when-buffer-full ] | transmit } ]
```

Disables the QoS data rate limit configuration for the subscriber.

```
no qos rate-limit direction { downlink | uplink } [ qci qci_val ]
```

**Important:** If this keyword is omitted, the same values are used for all classes.

```
qci qci_val
```

$qci_val$ is the QoS Class identifier (QCI) for which the negotiate limit is being set expressed as an integer from 1 through 9. If no qci-val is configured, it will be taken as undefined-qci (same as undefined-qos class).

```
burst-size { bytes | auto-readjust [ duration dur ] }
```

Default: See the Usage section for this command

The burst size allowed (in bytes) for peak data rate and committed data rate.
bytes must be an integer from 1 through 6000000.

**Important:** The minimum value of this parameter should be configured to the greater of the following two values: 1) three times greater than the packet MTU for the subscriber connection, OR 2) three seconds worth of token accumulation within the “bucket” for the configured peak-data-rate. If the committed-data-rate parameter is specified, the burst-size is applied to both the committed and peak rates.

auto-readjust [ duration dur ] provides the option to calculate the Burst size dynamically while configuring rate-limit. When enabled, the system calculates the burst size using the GGSN QoS-negotiated rate that will be enforced.

Every time there is a change in the rates (due to an updated QoS), the burst sizes will be updated accordingly. This keyword also provides two different burst sizes. One burst size for peak rate and another for committed rate.

By default this keyword is disabled.

duration dur specifies the duration of burst in seconds. If the duration is not specified, the default is 1 second. dur must be an integer from 1 through 30.

**exceed-action { drop | lower-ip-precedence | transmit }**

Default: See the Usage section for this command

Specifies the action to take on packets that exceed the committed-data-rate but do not violate the peak-data-rate. The following actions are supported:

- drop: Drops the packets.
- lower-ip-precedence: Transmits the packets after lowering the ip-precedence.
- transmit: Transmits the packets.

**violate-action { drop | lower-ip-precedence | transmit }**

Default: See the Usage section for this command

Specifies the action to take on packets that exceed both the committed-data-rate and the peak-data-rate. The following actions are supported:

- drop: Drops the packets.
- lower-ip-precedence: Transmits the packets after lowering the IP precedence.
- transmit: Transmits the packet after lowering the IP precedence.

**shape [transmit-when-buffer-full]:** Enables traffic shaping and buffers user packets when subscriber traffic violates the allowed peak/committed data rate. The [transmit-when-buffer-full] keyword allows the packets to be transmitted when buffer memory is full.

transmit: Transmits the packet

**Usage**

This command configures APN quality of service (QoS) data rate shaping through traffic policing. This command specifies the actions to take on subscriber flows exceeding or violating allowed peak or committed data rates. The shaping function also provides an enhanced function to buffer the excessive user packets and send them to the subscriber when subscriber traffic drops below the committed or peak data rate limit.

**Important:** The buffering of user packets in traffic shaping does not apply for real-time traffic.
**Important:** If the exceed/violate action is set to “lower-ip-precedence”, this command may override the configuration of the `ip qos-dscp` command in the GGSN service Configuration mode for packets from the GGSN to the PDG/TTG. In addition, the GGSN service `ip qos-dscp` command configuration can override the APN setting for packets from the GGSN to the Internet. Therefore, it is recommended that this command not be used in conjunction with this action.

The command can be entered multiple times to specify different combinations of direction and class. If this command is not configured at all, the GGSN does not perform traffic policing or QoS negotiation with the PDG/TTG; it accepts all of the PDG/TTG-provided values for the PDP context.

**Important:** This command should be used in conjunction with the `max-contexts` command to limit the maximum possible bandwidth consumption by the APN.

For additional information on QoS traffic shaping and policing, see the *System Administration Guide*.

### Default Values

The following table displays the default values for each of the traffic classes:

<table>
<thead>
<tr>
<th>Class: Conversational</th>
<th>Uplink Traffic: Disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Downlink Traffic: Disabled</td>
<td>Peaked Data Rate (in bps): 16000000</td>
</tr>
<tr>
<td>Committed Data Rate (in bps): 16000000</td>
<td></td>
</tr>
<tr>
<td>Exceed Action: lower-ip-precedence</td>
<td></td>
</tr>
<tr>
<td>Violate Action: drop</td>
<td></td>
</tr>
<tr>
<td>Peak Data Rate (in bps): 86400000</td>
<td></td>
</tr>
<tr>
<td>Committed Data Rate (in bps): 86400000</td>
<td></td>
</tr>
<tr>
<td>Exceed Action: lower-ip-precedence</td>
<td></td>
</tr>
<tr>
<td>Violate Action: drop</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Class: Streaming</th>
<th>Uplink Traffic: Disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Downlink Traffic: Disabled</td>
<td>Peaked Data Rate (in bps): 16000000</td>
</tr>
<tr>
<td>Committed Data Rate (in bps): 16000000</td>
<td></td>
</tr>
<tr>
<td>Exceed Action: lower-ip-precedence</td>
<td></td>
</tr>
<tr>
<td>Violate Action: drop</td>
<td></td>
</tr>
<tr>
<td>Peak Data Rate (in bps): 86400000</td>
<td></td>
</tr>
<tr>
<td>Committed Data Rate (in bps): 86400000</td>
<td></td>
</tr>
<tr>
<td>Exceed Action: lower-ip-precedence</td>
<td></td>
</tr>
<tr>
<td>Violate Action: drop</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Class: Interactive, Traffic Handling Priority: 1</th>
<th>Uplink Traffic: Disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Downlink Traffic: Disabled</td>
<td>Peaked Data Rate (in bps): 16000000</td>
</tr>
<tr>
<td>Committed Data Rate (in bps): n/a</td>
<td></td>
</tr>
<tr>
<td>Exceed Action: n/a</td>
<td></td>
</tr>
<tr>
<td>Violate Action: drop</td>
<td></td>
</tr>
<tr>
<td>Peak Data Rate (in bps): 86400000</td>
<td></td>
</tr>
<tr>
<td>Committed Data Rate (in bps): n/a</td>
<td></td>
</tr>
<tr>
<td>Exceed Action: n/a</td>
<td></td>
</tr>
<tr>
<td>Violate Action: drop</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Class: Interactive, Traffic Handling Priority: 2</th>
<th>Uplink Traffic: Disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Downlink Traffic: Disabled</td>
<td>Peaked Data Rate (in bps): 16000000</td>
</tr>
<tr>
<td>Committed Data Rate (in bps): n/a</td>
<td></td>
</tr>
<tr>
<td>Exceed Action: n/a</td>
<td></td>
</tr>
<tr>
<td>Violate Action: drop</td>
<td></td>
</tr>
<tr>
<td>Peak Data Rate (in bps): 86400000</td>
<td></td>
</tr>
<tr>
<td>Committed Data Rate (in bps): n/a</td>
<td></td>
</tr>
<tr>
<td>Exceed Action: n/a</td>
<td></td>
</tr>
<tr>
<td>Violate Action: drop</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Class: Interactive, Traffic Handling Priority: 3</th>
<th>Uplink Traffic: Disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Downlink Traffic: Disabled</td>
<td>Peaked Data Rate (in bps): 16000000</td>
</tr>
<tr>
<td>Committed Data Rate (in bps): n/a</td>
<td></td>
</tr>
<tr>
<td>Exceed Action: n/a</td>
<td></td>
</tr>
<tr>
<td>Violate Action: drop</td>
<td></td>
</tr>
<tr>
<td>Peak Data Rate (in bps): 86400000</td>
<td></td>
</tr>
<tr>
<td>Committed Data Rate (in bps): n/a</td>
<td></td>
</tr>
<tr>
<td>Exceed Action: n/a</td>
<td></td>
</tr>
<tr>
<td>Violate Action: drop</td>
<td></td>
</tr>
</tbody>
</table>
Subscriber Configuration Mode Commands

Usage

This command configures the APN quality of service (QoS) data rate shaping through traffic policing/shaping. This command specifies the actions to take on subscriber flows exceeding or violating allowed peak/committed data rates. The shaping function also provides an enhanced function to buffer the excessive user packets and send them to the subscriber when subscriber traffic drops below the committed or peak data rate limit.

**Important:** The buffering of user packets in traffic shaping does not apply for real-time traffic.

**Important:** If the exceed/violate action is set to “lower-ip-precedence”, this command may override the configuration of the `ip qos-dscp` command in the GGSN service configuration mode for packets from the GGSN to the SGSN. In addition, the GGSN service `ip qos-dscp` command configuration can override the APN setting for packets from the GGSN to the Internet. Therefore, it is recommended that command not be used in conjunction with this action.

The command can be entered multiple times to specify different combinations of direction and class. If this command is not configured at all, the GGSN does not perform traffic policing or QoS negotiation with the SGSN (i.e. it accepts all of the SGSN-provided values for the PDP context.

**Important:** This command should be used in conjunction with the `max-contexts` command to limit the maximum possible bandwidth consumption by the APN.

Default Values:

To calculate the burst size dynamically a new optional keyword `auto-readjust [ duration dur ]` is provided with `burst-size` keyword. By default the burst size is fixed if defined in bytes with this command. In other words irrespective of the rate being enforced, burst-size fixed as given in the `burst-size bytes` parameter.

For the need of variable burst size depending on the rate being enforced this new keyword `auto-readjust [ duration dur ]` is provided. Use of this keyword enables the calculation of burst size as per token bucket algorithm calculation as T=B/R, where T is the time interval, B is the burst size and R is the Rate being enforced.

It also provides different burst size for Peak and Committed data rate-limiting.

If `auto-readjust` keyword is not used a fixed burst size must be defined which will be applicable for peak data rate and committed data rate irrespective of rate being enforced.

If `auto-readjust` keyword is provided without specifying the duration a default duration of 1 second will be taken for burst size calculation.
Example

The following command lowers the IP precedence when the committed-data-rate and the peak-data-rate are violated in uplink direction:

```bash
qos rate-limit direction uplink violate-action lower-ip-precedence
```

The following command buffers the excess user packets when the subscriber traffic violates the configured peak or committed data-rate bps in uplink direction. Once the peak/committed data rate for that subscriber goes below the configured limit it transmit them. It also transmits them if buffer memory is full:

```bash
qos rate-limit direction uplink violate-action shape transmit-when-buffer-full
```
qos traffic-police

Enables and configures traffic policing through bandwidth limitations and action for the subscriber traffic if it exceeds or violates the peak or committed data rate. Uplink and downlink limits are configured separately.

**Product**
- PDSN
- HA
- GGSN
- ASN-GW

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration > Context Configuration > Subscriber Configuration

```
configure > context context_name > subscriber { default | name subscriber_name }
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

**Syntax**

```
qos traffic-police direction { downlink | uplink } [ burst-size bytes ] [ committed-data-rate bps ] [ exceed-action { drop | lower-ip-precedence | transmit } ] [ peak-data-rate bps ] [ violate-action { drop | lower-ip-precedence | transmit } ]
```

```
no qos traffic-police direction { downlink | uplink }
```

- **downlink**
  - Applies the specified limits and actions to the downlink (data to the subscriber).

- **uplink**
  - Apply the specified limits and actions to the uplink (data from the subscriber).

- **burst-size bytes**
  - Default: 3000
  - Specifies the allowed peak burst size allowed in bytes.
  - `bytes` must be an integer from 0 through 4294967295.

**Important:** This parameter should be configured to at least the greater of the following two values: 1) three times greater than packet MTU for the subscriber connection, OR 2) three seconds worth of token accumulation within the “bucket” for the configured peak-data-rate.

- **committed-data-rate bps**
  - Default: 144000
  - Specifies the committed data rate (guaranteed-data-rate) in bits per second (bps).
  - `bps` must be an integer from 0 through 4294967295.
```
exceed-action { drop | lower-ip-precedence | transmit }
```

Default: lower-ip-precedence
Specifies the action to take on packets that exceed the committed-data-rate but do not violate the peak-data-rate. The following actions are supported:
- `drop`: Drops the packet
- `lower-ip-precedence`: Transmits the packet after lowering the IP precedence
- `transmit`: Transmits the packet

```
peak-data-rate bps
```

Default: 256000
Specifies the peak data-rate for the subscriber in bits per second (bps).
`bps` must be an integer from 0 through 4294967295).

```
violate-action { drop | lower-ip-precedence | transmit }
```

Default: drop
Specifies the action to take on packets that exceed both the committed-data-rate and the peak-data-rate. The following actions are supported:
- `drop`: Drops the packet
- `lower-ip-precedence`: Transmits the packet after lowering the IP precedence
- `transmit`: Transmits the packet

```
no
```

Disables traffic policing in the specified direction for the current subscriber.

## Usage

Use this command to limit the bandwidth a subscriber uses in the uplink and downlink directions.

**Important:** If the exceed/violate action is set to “lower-ip-precedence”, the TOS value for the outer packet becomes “best effort” for packets that exceed/violate the traffic limits regardless of what the `ip user-datagram-tos copy` command is configured to. In addition, the “lower-ip-precedence” option may also override the configuration of the `ip qos-dscp` command. Therefore, it is recommended that command not be used when specifying this option.

## Example

Details on the QoS traffic policing can be found in the *System Administration Guide*.

The following command sets an uplink peak data rate of 128000 bps and lowers the IP precedence when the committed-data-rate and the peak-data-rate are exceeded:

```
qos traffic-police direction uplink peak-data-rate 128000 violate-action lower-ip-precedence
```

The following command sets a downlink peak data rate of 256000 bps and drops packets when the committed-data-rate and the peak-data-rate are exceeded:

```
qos traffic-police direction downlink peak-data-rate 256000 violate-action drop
```
qos traffic-shape

Enables and configures traffic shaping functionality when buffering the data packets during congestion or when the subscriber exceeds the configured peak or committed data rate limit. The system buffers the data packets during an instantaneous burst and deliver them to the subscriber when traffic flow drops below the peak or committed data rate. Uplink and downlink traffic shaping are configured separately.

Important: This feature is NOT supported for real-time traffic.

Product
PDSN
HA
GGSN
ASN-GW

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Subscriber Configuration
configure > context context_name > subscriber { default | name subscriber_name }

Entering the above command sequence results in the following prompt:
[context_name]host_name(config-subscriber)#

Syntax
qos traffic-shape direction { downlink | uplink } [ burst-size bytes ] [ committed-data-rate bps ] [ exceed-action { drop | lower-ip-precedence | transmit } ] [ peak-data-rate bps ] [ violate-action { drop | lower-ip-precedence | buffer [ transmit-when-buffer-full ] | transmit } ] +

no qos traffic-shape direction { downlink | uplink }

downlink
Applies the specified limits and actions to the downlink (data to the subscriber).

uplink
Applies the specified limits and actions to the uplink (data from the subscriber).

burst-size bytes
Default: 3000
Specifies the allowed peak burst size in bytes.
bytes must be an integer from 0 through 4294967295.
**Important:** It is recommended that this parameter be configured to at least the greater of the following two values: 1) three times greater than packet MTU for the subscriber connection, OR 2) three seconds worth of token accumulation within the “bucket” for the configured peak-data-rate.

*committed-data-rate*  
Default: 144000  
Specifies the committed data rate (guaranteed-data-rate) in bits per second (bps).  
*bps* must be an integer from 0 through 4294967295).

*exceed-action*  
Default: lower-ip-precedence  
Specifies the action to take on packets that exceed the committed-data-rate but do not violate the peak-data-rate. The following actions are supported:  
drop: Drops the packet  
lower-ip-precedence: Transmits the packet after lowering the ip-precedence  
transmit: Transmits the packet

*peak-data-rate*  
Default: 256000  
Specifies the peak data-rate for the subscriber in bits per second (bps).  
*bps* must be an integer from 0 through 4294967295).

*violate-action*  
Default: See the Usage section for this command  
The action to take on the packets that exceed both the committed-data-rate and the peak-data-rate. The following actions are supported:  
drop: Drops the packet  
lower-ip-precedence: Transmits the packet after lowering the IP precedence  
buffer [transmit-when-buffer-full]: Enables traffic shaping and buffers user packets when subscriber traffic violates the allowed peak/committed data rate. The [transmit-when-buffer-full] keyword allows the packet to be transmitted when buffer memory is full.  
transmit: Transmits the packet

+  
More than one of the above keywords can be entered within a single command.

*no*  
Disables traffic policing for the specified direction for the current subscriber.

**Usage**

Use this command to provide the traffic shaping function to a subscriber in the uplink and downlink directions. This feature is providing a traffic flow control different to QoS traffic policing. When a subscriber violates or exceeds the peak data rate instead of dropping the packets, as in QoS traffic policing, this feature buffers subscriber data packets and sends the buffered data when the traffic flow is low or not in congestion state.
**Important:** If the exceed or violate action is set to “lower-ip-precedence”, the TOS value for the outer packet becomes “best effort” for packets that exceed or violate the traffic limits regardless how the `ip user-datagram-tos copy` command is configured. In addition, the “lower-ip-precedence” option may also override the configuration of the `ip qos-dscp` command. Therefore, this command should not be used when specifying this option.

**Example**

Details on the QoS traffic policing functionality is located in the System Administration Guide.

The following command sets an uplink peak data rate of 128000 bps and lowers the IP precedence when the committed-data-rate and the peak-data-rate are exceeded:

```bash
qos traffic-shape direction uplink peak-data-rate 128000 violate-action lower-ip-precedence
```

The following command buffers the excess user packets when the subscriber traffic violates the configured peak-data-rate 256000 bps in downlink direction. Once the peakcommitted data rate for that subscriber goes below the configured limit it transmit them. It also transmits them if buffer memory is full:

```bash
qos traffic-shape direction downlink peak-data-rate 256000 violate-action buffer transmit-when-buffer-full
```
radius accounting

Sets the RADIUS accounting parameters for the subscriber or domain. This command takes precedence over the similar Context Configuration command and is disabled by default.

Product
All

Privilege
Administrator

Mode
Exec > Global Configuration > Context Configuration > Subscriber Configuration
configure > context context_name > subscriber { default | name subscriber_name }

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-subscriber)#

Syntax

radius accounting { interim { interval-timeout timeout | normal | suppress } | ip remote-address list-id list_id | mode { session-based | access-flow-based { none | auxiliary-flows | all-flows | main-a10-only } } | start { normal | suppress } | stop { normal | suppress } }

no radius accounting { ip remote-address list-id list_id | interim { interval-timeout } }

interim { interval-timeout timeout | normal | suppress }

interval-timeout timeout: Indicates the time (in seconds) between updates to session counters (log file on RADIUS or AAA event log) during the session. timeout must be an integer from 50 to 4000000.

Caution: Interim interval settings received from the RADIUS server take precedence over this setting on the system. While the low limit of this setting on the system is a minimum of 50 seconds, the low limit setting on the RADIUS server can be as little as 1 second. To avoid increasing network traffic unnecessarily and potentially reducing network and system performance, do not set this parameter to a value less than 50 on the RADIUS server.

normal: If RADIUS accounting is enabled, sends this Acct-Status-Type message when required by normal operation
suppress: If RADIUS accounting is enabled, suppresses the sending of this Acct-Status-Type message.

ip remote-address list-id list_id

Specifies the identification number of the IP address list to use for the subscriber for remote address-based accounting.

list_id: Specifies the RADIUS accounting remote IP address list identifier for remote-address accounting for the subscriber. list_id must be an integer from 1 through 65535.

This command is used as part of the Remote Address-based accounting feature and associates the subscriber with a list of remote addresses. Remote address accounting data is collected each time the subscriber communicates with any of the addresses specified in the list.
Remote address lists are configured using the list keyword in the radius accounting ip remote-address command in the Context Configuration mode.
mode { session-based | access-flow-based { none | auxillary-flows | all-flows | main-a10-only } }

Default: session-based

Specifies if the radius accounting mode is either session-based or access-flow-based.

- **session-based**: configures session-based RADIUS accounting behavior for the subscriber - which means a single radius accounting message generated for the subscriber session not separate accounting messages for individual A10 connections or flows.
- **access-flow-based**: configures access-flow-based RADIUS accounting behavior for the subscriber. This offers flexibility by generating separate accounting messages for flows and A10 sessions.
  - **all-flows**: Generates separate RADIUS accounting messages per access flow. Separate accounting messages are not generated for data path connections. (For example, separate messages are not sent for the main A10 or auxiliary connections.).
  - **auxillary-flows**: Generates RADIUS accounting records for the main data path connection and for access-flows for all auxiliary data connections. (For example, separate RADIUS accounting messages are generated for the main A10 session and for access-flows within auxiliary A10 connections. The main A10 session accounting does not include octets or other accounting information from the auxiliary flows.)
  - **main-a10-only**: Configures access-flow-based single accounting messages (for example only single start/interim/stop) are generated for the main A-10 flows only.
  - **none**: Generates separate RADIUS accounting messages for all data path connections (for example, PDSN main or auxiliary A10 connections) but not for individual access-flows. This is essentially A10 connection-based accounting.

**start** { normal | suppress }

- **normal**: If RADIUS accounting is enabled, sends this Acct-Status-Type message when required by normal operation
- **suppress**: If RADIUS accounting is enabled, suppresses the sending of this Acct-Status-Type message.

**stop** { normal | suppress }

- **normal**: If RADIUS accounting is enabled, sends this Acct-Status-Type message when required by normal operation
- **suppress**: If RADIUS accounting is enabled, suppresses the sending of this Acct-Status-Type message.

**no**

ip remote-address list-id list_id: Deletes the entry for the specified list_id.
interim [ interval-timeout ]: Disables the interim interval setting.

**Usage**

Use this command to allow a per-domain setting for the RADIUS accounting.

**Example**

Set the accounting interim interval to one minute (60 seconds) for all sessions that use the current subscriber configuration:

```
radius accounting interim interval-timeout 60
```

Do not send RADIUS interim accounting messages:

```
radius accounting interim suppress
```
Sets the accounting message start normal for main A-10 flows only.

```
radius accounting mode main-a10-only start normal
```
radius group

Applies a RADIUS server group at the subscriber level for AAA functionality.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context context_name > subscriber { default | name subscriber_name }

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-subscriber)#

Syntax

radius group group_name

{ default | no } radius group

radius group_name

Specifies the name of the server group that is used for authentication and/or accounting for the specific subscriber. group_name must be an alphanumeric string of 1 through 63 characters. It must have been preconfigured within the same context of subscriber.

default

Sets or restores the default RADIUS server group specified at the context level or in the default subscriber profile.

no

Disables the applied RADIUS group for specific subscriber.

Usage

This feature provides the RADIUS configurables under radius group node. Instead of having a single list of servers per context, this feature configures multiple server groups within a context and applies individual RADIUS server group for subscriber in that context. Each server group consists of a list of AAA servers. IF no RADIUS group is applied for this subscriber or the default subscriber profile, the default server group available at context level is used for accounting and authentication of the subscriber.

Example

Following command applies a previously configured RADIUS server group named starl to a subscriber within the specific context:

    radius group starl

Following command disables the applied RADIUS server group for the specific subscriber.

    no radius group
radius returned-framed-ip-address

Sets the policy whether or not to reject a call when the RADIUS server supplies 255.255.255.255 as the framed IP address and the MS does not supply an address.

**Product**
- GGSN

**Privilege**
- Security Administrator, Administrator

**Mode**
- Exec > Global Configuration > Context Configuration > Subscriber Configuration

```
configure > context context_name > subscriber { default | name subscriber_name }
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

**Syntax**

```
radius returned-framed-ip-address 255.255.255.255-policy { accept-call-when-ms-ip-not-supplied | reject-call-when-ms-ip-not-supplied }

default radius returned-framed-ip-address 255.255.255.255-policy
```

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>accept-call-when-ms-ip-not-supplied</td>
<td>Accepts calls when the RADIUS server does not supply a framed IP address and the MS does not supply an address.</td>
</tr>
<tr>
<td>reject-call-when-ms-ip-not-supplied</td>
<td>Rejects calls when the RADIUS server does not supply a framed IP address and the MS does not supply an address.</td>
</tr>
<tr>
<td>default</td>
<td>Sets the policy to its default of rejecting calls when the RADIUS server does not supply a framed IP address and the MS does not supply an address.</td>
</tr>
</tbody>
</table>

**Usage**

Use this command to set the behavior for the current subscriber when the RADIUS server supplies 255.255.255.255 as the framed IP address and the MS does not supply an address.

**Example**

The following command sets the subscriber profile to reject calls when the RADIUS server does not supply a framed IP address and the MS does not supply an address:

```
radius returned-framed-ip-address 255.255.255.255-policy reject-call-when-ms-ip-not-supplied
```
**rohc-profile-name**

Identifies the robust header compression (RoHC) profile configuration that will be applied to bearer sessions belonging to this subscriber.

**Product**
- HSGW
- PDSN

**Privilege**
Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Subscriber Configuration
configure > context context_name > subscriber { default | name subscriber_name }

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

**Syntax**

```
rohc-profile-name name
```

*name*

Specifies the name of the RoHC profile that the system will use to apply header compression and decompression parameters to bearer session data for this subscriber. *name* must be an existing RoHC profile expressed as an alphanumeric string of 1 through 63 characters.

**Usage**

Use this command to specify a RoHC configuration profile to be applied to bearer sessions belonging to this subscriber. RoHC profiles are configured through the Global Configuration Mode using the `rohc-profile` command.

**Example**

The following command specifies that the RoHC profile named `rohc-cfg1` is to be applied to all bearer sessions belonging to this subscriber:

```
rohc-profile-name rohc-cfg1
```
secondary ip pool

Specifies a secondary IP pool to be used as backup pool for Network Address Translation (NAT).

**Important:** This command requires the purchase and installation of a license. Please contact your Cisco sales representative for more information.

**Product**
NAT

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Subscriber Configuration

```
configure > context context_name > subscriber { default | name subscriber_name }
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#!
```

**Syntax**

```
secondary ip pool pool_name

no secondary ip pool
```

- **no**
  Removes the previous secondary IP pool configuration.

- **secondary ip pool pool_name**
  Specifies the secondary IP pool name. 
  *pool_name* must be an alphanumeric string of 1 through 31 characters.

**Usage**

Use this command to configure a secondary IP pool for NAT subscribers, which is not overwritten by the RADIUS supplied list. The secondary pool will be appended to the RADIUS supplied IP pool list or subscriber template provided IP pool list, as applicable, during call setup.

**Example**

The following command configures a secondary IP pool named test123:

```
secondary ip pool test123
```
send-destination-pgw

Configures how the HSGW selects a P-GW address for the “Destination-PGW” AVP.

**Product**
HSGW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context context_name > subscriber { default | name subscriber_name }

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-subscriber)#

**Syntax**

```
send-destination-pgw { all | explicit-only | implicit-only }
```

```
no send-destination-pgw
```

- **no**
  Removes the configuration for this command.

- **all**
  P-GW address is obtained either by explicit or implicit mechanism.

- **explicit-only**
  The UE performs LCP/PPP procedures, and attaches with a specific APN. The HSGW queries the AAA over the STa interface and receives a MIP6-Agent-Info AVP that includes a sub AVP of Destination-Host. The HSGW copies the value of the Destination-Host AVP in the Destination-PGW AVP which is sent in the CCR-I to the PCRF.

- **implicit-only**
  The UE performs LCP/PPP procedures, and attaches with a specific APN. The AAA does not return the P-GW to use, so the HSGW performs NAPTR procedures to determine the P-GW which will be used.

**Usage**
Use this command to configure how the HSGW selects a P-GW address for the “Destination-PGW” AVP. This AVP is sent over Gxa to the PCRF.

**Example**

Configures the HSGW to select either implicit or explicit selection method.

```
send-destination-pgw all
```
simultaneous

Enables or disables the simultaneous use of both Mobile and Simple IP services.

**Product**
PDSN
FA
HA
ASN-GW

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Subscriber Configuration

```
configure > context context_name > subscriber { default | name subscriber_name }
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)#
```

**Syntax**

```
[ no ] simultaneous simple-and-mobile-ip
```

- **no**
  
  Disables the simultaneous use.

**Usage**

Subscribers with mobile devices that concurrently support mobile and simple IP services require this option to be set.

**Example**

```
no simultaneous simple-and-mobile-ip
simultaneous simple-and-mobile-ip
```
timeout absolute

Configures the maximum duration of the session before the system automatically terminates the session.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context context_name > subscriber { default | name subscriber_name }

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-subscriber)#

Syntax

timeout absolute seconds

{ default | no } timeout absolute

default | no
Indicates the timeout specified is to be returned to its default behavior. If a timeout value is not specified, all timeouts are set to their default values.

timeout absolute
Default: 0
Specifies the absolute maximum time a session may exist (in seconds) in any state (active or dormant).

seconds
Specifies the maximum amount of time (in seconds) before the specified timeout action is activated.
seconds must be an integer from 0 through 4294967295. The special value 0 disables the timeout specified.

Usage
Use this command to set the absolute maximum time a session may exist in any state.

Example

timeout absolute 18000
timeout idle

Configures the idle timeout duration for the long duration timer associated with a subscriber session.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context context_name > subscriber { default | name subscriber_name }

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-subscriber)#

Syntax

timeout idle idle_dur

{ default | no } timeout idle

default | no

Indicates the timeout specified is to be returned to its default behavior. If no specific timeout is specified, then all are set to their default behavior.

timeout idle

Default: 0

Specifies the maximum duration of the session (in seconds) can remain idle before the system automatically terminates the session due to inactivity.

idle_dur

Specifies the maximum amount of time (in seconds) before the specified timeout action is activated. idle_dur must be an integer from 0 through 2147483647. The special value 0 disables the timeout specified.
timeout long-duration

Configures the long duration timeout and optionally the inactivity duration of HA subscriber session.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Subscriber Configuration

```
configure > context context_name > subscriber { default | name subscriber_name }
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-subscriber)>
```

**Syntax**

```
timeout long-duration ldt_timeout [ inactivity-time inact_timeout ]
```

[ no | default ]timeout long-duration

- **no**
  Indicates the timeout specified is to be returned to its default behavior. If no specific timeout is specified then all are set to their default behavior.

- **long-duration ldt_timeout**
  Default: 0
  Designates the maximum duration of the session (in seconds) before the system automatically reports/terminates the session.
  *ldt_timeout* must be a value in the range from 0 through 4294967295. The special value 0 disables the timer.

- **inactivity-time inact_timeout**
  Specifies the maximum amount of time (in seconds) before the specified session is marked as dormant.
  *inact_timeout* must be a value in the range from 0 through 4294967295. The special value 0 disables the inactivity time specified.

**Usage**

Use this command to set the long duration timeout period and inactivity timer for subscriber sessions. Reduce the idle timeout to free session resources faster for use by new requests.
Refer to the `long-duration-action detection` and `long-duration-action disconnection` commands for more information.

**Example**

The following command sets the long duration timeout duration to 300 seconds and inactivity timer for subscriber session to 45 seconds:
timeout long-duration 300 inactivity-time 45
tpo policy

The Traffic Performance Optimization (TPO) in-line service is not supported in this release.
tunnel address-policy

Specifies the policy for address allocation and validation for all tunneled calls (IP-IP, IP-GRE) except L2TP calls. With this command enabled, GGSN IP address validation could be disabled for specified incoming calls.

For GGSN systems, this command can also be specified in the APN Configuration mode (tunnel address-policy) which would mean the system defers to the old l3-to-l2-tunnel address policy command for calls coming through L2TP tunnels.

Product
PDSN
GGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context context_name > subscriber { default | name subscriber_name }

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-subscriber)#

Syntax

tunnel address-policy { alloc-only | alloc-validate | no-alloc-validate }

default tunnel address-policy

 alloc-only
Allocates IP addresses locally without validation.

 alloc-validate
Default.
The VPN Manager allocates and validates all incoming IP addresses from a static pool of IP addresses.

 no-alloc-validate
No IP address assignment or validation is done for calls coming in via L3 tunnels. Incoming static IP addresses are passed. This option allows for the greatest flexibility.

 default
Resets the tunnel address-policy to alloc-validate.

Usage
This command supports scalable solutions for Corporate APN deployment as many corporations handle their own IP address assignments. In some cases this is done to relieve the customer or the mobile operators from the necessity of reconfiguring the range of IP addresses for the IP pools at the GGSN.
The following command resets the IP address validation policy to validate against a static pool of address:

```
default tunnel address-policy
```

The following command disables IP address validation for calls coming through tunnels:

```
tunnel address-policy no-alloc-validate
```
tunnel ipip

Configures IP-in-IP tunnelling parameters for the current subscriber.

Product
PDSN
GGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Subscriber Configuration
configure > context context_name > subscriber { default | name subscriber_name }

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-subscriber)#

Syntax

tunnel ipip peer-address peer_address local-address local_addr ]

no tunnel ipip

<table>
<thead>
<tr>
<th>peer-address peer_address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the IP address of the external gateway terminating the IP-in-IP tunnel.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>local-address local_addr</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the IP address of the interface in the destination context originating the IP-in-IP tunnel.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>no</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disables IP-in-IP tunneling for the current subscriber.</td>
</tr>
</tbody>
</table>

Usage
Subscriber IP payloads are encapsulated with IP-in-IP headers and tunneled by the GGSN or PDSN to an external gateway.

Example
The following command configures the system to encapsulate subscriber traffic using IP-in-IP and tunnel it from a local address of 192.168.1.100 to a gateway with an IP address of 192.168.1.225:

tunnel ipip peer-address 192.168.1.225 local-address 192.168.1.100 preference 1
tunnel ipsec

Configures sessions for the current subscriber to use an IPSec tunnel based on the IP pool corresponding to the subscriber’s assigned IP address.

Product
PDSN
GGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Subscriber Configuration

Syntax

```plaintext
tunnel ipsec use-policy-matching-ip-pooler-address
no tunnel ipsec use-policy-matching-ip-pooler-address
```

Usage
Use this command to set the current subscribers sessions to use an IPSec policy that is assigned to the IP pool that the subscribers assigned IP address relates to.

Example
The following command enables the use of the policy that matches the IP pool address:

```plaintext
tunnel ipsec use-policy-matching-ip-pooler-address
```
tunnel l2tp

Configures L2TP tunnel parameters for the subscriber.

Product
All products supporting L2TP

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Subscriber Configuration

configure > context context_name > subscriber { default | name subscriber_name }

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-subscriber)#

Syntax

```
tunnel l2tp [ peer-address ip_address [ [ encrypted ] [secret secret] ] [ preference number ] [ tunnel-context context ] [ local-address ip_address ] [ crypto-map map_name [ [ encrypted ] isakmp-secret secret ] ] ]
no tunnel l2tp [ peer-address ip_address ]
```

**peер-address ip_address**

A peer L2TP Network Server (LNS) associated with this LAC (L2TP Access Concentrator). *ip_address* must be an IP address entered using IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal format.

```
[ encrypted ] secret secret
```

Specifies the shared key (secret) between the L2TP Network Server (LNS) associated with this LAC (L2TP Access Concentrator). *secret* must be an alphanumeric string of 1 through 63 characters that is case sensitive.

**encrypted**: Specifies the encrypted shared key between the L2TP Network Server (LNS) associated with this LAC (L2TP Access Concentrator). *secret* must be an alphanumeric string of 1 through 128 characters that is case sensitive.

The *encrypted* keyword is intended only for use by the system while saving configuration scripts. The system displays the encrypted keyword in the configuration file as a flag that the variable following the *secret* keyword is the encrypted version of the plain text secret. Only the encrypted secret is saved as part of the configuration file.

**preference number**

Default: 1

Specifies the order in which a group of tunnels configured for this subscriber will be tried. *number* must be an integer from 1 through 65535.

**tunnel-context context**

Specifies the name of the context containing ports through which this subscriber’s data traffic is to be communicated between this LAC and the LNS. *context* must be an alphanumeric string of 1 through 79 characters.
tunnel l2tp

local-address ip_address

Specifies a LAC service bind address which is given as a hint that is used to select a particular LAC service.

ip_address must be an IP address entered using IPv4 dotted-decimal or IPv6 colon-separated-hexadecimal notation.

crypto-map map_name { [encrypted] isakmp-secret secret }

Specifies the name of a crypto map that has been configured in the current context. map_name must be an alphanumeric string from 1 to 127 alphanumeric characters.

isakmp-secret secret: Specifies the pre-shared key for the Internet Key Exchange (IKE). secret must be an alphanumeric string of 1 through 127 characters.

encrypted isakmp-secret secret: Specifies the pre-shared key for IKE. Encryption must be used when sending the key. secret must be an alphanumeric string of 1 through 127 characters.

no

Disables tunneling for the current subscriber. When peer-address is included, the tunneling for that specific L2TP Network Server (LNS) is disabled but tunneling to other configured LNSs is still enabled.

Usage

Use this command to configure specific L2TP tunneling parameters for the current subscriber.

Example

To specify L2tp tunneling to the LNS peer at the IP address 198.162.10.100 with a shared secret of bigco and preference of 1, enter the following command:

```
tunnel l2tp peer-address 198.162.10.100 secret bigco preference 1
```
w-apn

This command allows you to configure the default APN to be used for the UE connections when the AAA server does not return the subscriber APN name in the service-selection AVP in RADIUS Access-Accept message.

**Product**
eWAG

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Subscriber Configuration

```bash
configure > context context_name > subscriber { default | name subscriber_name }
```

Entering the above command sequence results in the following prompt:

```bash
[context_name]host_name(config-subscriber)#
```

**Syntax**

```bash
w-apn apn_name

no w-apn
```

---

**Usage**

If previously configured, removes the specified configuration.

```bash
apn-name apn_name
```

Specifies the APN name.

*apn_name* must be the name of an APN and must be a string of 1 to 62 characters in length consisting of alphabetic characters (A-Z and a-z), digits (0-9), dot(.) and the dash (-).

**Example**

The following command configures an APN named *apn123*:

```bash
w-apn apn123
```
Chapter 291
TACACS+ Configuration Mode Commands

This chapter describes all commands available in the TACACS+ Configuration Mode. TACACS+ (Terminal Access Controller Access-Control System Plus) is a secure, encrypted protocol. By remotely accessing TACACS+ servers that are provisioned with the administrative user account database, the ASR 5000 and ASR 5500 support TACACS+ accounting and authentication services for system administrative users.

**Important:** TACACS Configuration Mode is available in releases 11.0 and later.

**Mode**

Exec > Global Configuration > TACACS+ Configuration

`configure > tacacs mode`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-tacacs)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
accounting

Enables the recording of the start and the stop time each command issued during a TACACS+-authenticated CLI session.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > TACACS+ Configuration  
configure > tacacs mode

Entering the above command sequence results in the following prompt:

[local]host_name(config-tacacs)#

Syntax

[ no ] accounting { start-stop | command }

no

Disables a configured TACACS+ accounting setting (either accounting start-stop or accounting command).

{start-stop | command}

Specifies the type of accounting records to be recorded.

•start-stop: Records the time at which the session starts (the time at which the user passes authentication) and the time at which the user exits. If a user exits before passing authentication, only a stop time is recorded.

•command: Enables accounting on a command-by-command basis. The TACACS+ server is contacted prior to the execution of the command and the command which is about to be executed is recorded. Only commands which are valid for the user privilege and context (mode) in which they are about to be executed will be recorded. StarOS does not record whether the command itself succeeded or failed. For security reasons, some secure or restricted commands are not recorded. In such cases, the accounting record will record the command as three asterisks (“***”).

Usage

Use this command to configure the accounting method for TACACS+-based CLI sessions.

Important: For releases after 15.0 MR4, TACACS+ accounting (CLI event logging) will not be generated for Lawful Intercept users with privilege level set to 15 and 13.

Example

The following command enables TACACS+ accounting for commands:

accounting command
authorization

Enables the authorization of TACACS+ CLI users on a command-by-command, command + command argument, or command prompt basis. If the user is not authorized to execute the command, the command will fail.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > TACACS+ Configuration

configure > tacacs mode

Entering the above command sequence results in the following prompt:

[local]host_name(config-tacacs)#

Syntax

[ no ] authorization { command | prompt | arguments }

no

Disables a configured TACACS+ authorization command, prompt, or arguments setting.

{ command | prompt | arguments }

Specifies the type of authorization behavior to enforce:

•command: Enables per-command authorization. The TACACS+ server is contacted for each command and each command is authorized for the user. If the user is not authorized to execute the command, then the command fails. If the user is authorized for the command, the command is executed.

•prompt: Enables per-command authorization, as described for the command option above. However, since commands may be duplicated in different CLI modes, this version of the command authorization also passes the command prompt string to the server. The TACACS+ server is contacted for each prompt and command and must have a matching string for the prompt/command combination. Enabling prompt authorization supersedes command authorization, since the prompt and command must be authorized together.

•arguments: Enables per-command and command + argument authorization. The TACACS+ server authorizes each command and its arguments for the user. If the user is not authorized to execute the command and the corresponding arguments, the command fails. If the command does not contain any arguments, then the command only is passed to the authorization server.

Usage

Use this command to configure the authorization method for TACACS+-based CLI sessions.

Example

The following command requires per-command TACACS+ authorization:

authorization command
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Use this command to return to the parent configuration mode.
on-authen-fail

Defines system behavior when an administrative login fails due to a TACACS+ authentication failure. This command also can be used to configure system behavior separately for TACACS+ authentication failures for administrative users accessing the system via the StarOS Console port.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > TACACS+ Configuration
configure > tacacs mode

Entering the above command sequence results in the following prompt:

[local]host_name(config-tacacs)#

Syntax

on-authen-fail { continue | stop } [ tty console ]

{ continue | stop }
Specifies the type of authentication behavior to enforce:

• continue: After a TACACS+ authentication failure, the system will continue with authentication using non-TACACS+ authentication services.
• stop: After a TACACS+ authentication failure, the system forces the failed TACACS+ user to exit.

tty console

Release 12 and later systems only: Used after the stop or continue parameters to specify system behavior for users being authenticated via the StarOS Console port:

• stop tty console: Forces the failed TACACS+ user to exit.
• continue tty console: The system will continue with authentication using non-TACACS+ authentication services.

Usage

Use this command to configure system behavior for users that fail TACACS+ authentication.

Example

The following command instructs the system to stop upon TACACS+ authentication failure:

on-authen-fail stop
on-network-error

Configures StarOS behavior when a TACACS+ login fails due to a network error. This command also can be used to configure system behavior separately for TACACS+ network error login failures for administrative users accessing the system via the Console port.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > TACACS+ Configuration  
configure > tacacs mode

Entering the above command sequence results in the following prompt:

> [local]host_name(config-tacacs)#

**Syntax**

on-network-error { continue | stop } [ tty console ]

**continue**

The system will continue with authentication using non-TACACS+ authentication services.

**stop**

The system forces the failed TACACS+ user to exit.

**tty console**

*Release 12 and later systems only*: Can be used after the continue or stop options to specify system behavior for TACACS+ CLI users being authenticated via the StarOS Console port:

- **stop tty console**: Forces the failed user to exit when authentication fails.
- **continue tty console**: The system will continue with authentication using non-TACACS+ authentication services.

**Usage**

Use this command to configure system behavior for users who fail TACACS+ authentication due to a network error.

**Example**

The following command configures the system to stop when a TACACS+ login fails due to a network error:

```
on-network-error stop
```
on-unknown-user

Configures StarOS behavior when a TACACS+ server cannot authenticate a given user name. This command also can be used to configure system behavior separately for TACACS+ unknown user login failures for administrative users accessing the system via the StarOS console port.

⚠️ Important: Some TACACS+ server implementations will not send a Reply message indicating that the user name is invalid. Instead, these types of implementations will accept the username, whether valid or not, and then examine the username and password in combination before sending a Reply message indicating a failed TACACS+ login. In these cases, specifying on-unknown-user will not enforce the desired system behavior. To avoid this scenario, determine the method the configured TACACS+ servers will use to validate user names before deciding whether specifying the on-unknown-user command will provide the desired result.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > TACACS+ Configuration
configure > tacacs mode

Entering the above command sequence results in the following prompt:

[local]host_name(config-tacacs)#

Syntax

on-unknown-user { continue | stop } [ tty console ]

{ continue | stop }

Specifies the particular behavior to enforce:

- **continue**: The system continues with authentication using non-TACACS+ authentication services.
- **stop**: The system forces the failed TACACS+ user to exit.

[ ]

**tty console**

*Release 12 and later systems only*: Can be used after the continue or stop options to specify the behavior of the system for TACACS+ CLI users being authenticated via the StarOS console port.

- **stop tty console**: The system forces the failed user to exit when authentication fails.
- **continue tty console**: The system will continue with authentication using non-TACACS+ authentication services.

Usage

Use this command to configure StarOS behavior for users who fail TACACS+ user name authentication.
Example

The following command forces users who fail TACACS+ user name authentication to exit StarOS:

```
on-unknown-user stop```

rem_addr client-ip

Sends a remote client IPv4 address field in the TACACS+ protocol for use by a Cisco Secure ACS server.

**Product**
All products

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > TACACS+ Configuration
configure > tacacs mode

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-tacacs)#
```

**Syntax**

```
rem_addr client-ip

no rem_addr client-ip

default rem_addr client-ip

no
```

Disables the sending of a remote client IP address field to a Cisco Secure ACS server for a TACACS+ login request.

```
default
```

Disables the sending of a remote client IP address field to a Cisco Secure ACS server for a TACACS+ login request.

**Usage**

A Cisco Secure ACS server can be configured to explicitly check the NAS source address for TACACS+ connections. StarOS may not properly set the rem_addr field in the TACACS+ protocol packet when initiating a connection with the Cisco Secure ACS server. This may cause the Cisco Secure ACS server to reject the TACACS+ login request.

*Important:* The default behavior is to not fill in the rem_addr field.

This CLI command enables the setting and sending of the remote address to the IPv4 address associated with the local context management interface for customers who require this field to be verified via the Cisco Secure ACS server.

When enabled the rem_addr field contains the ssh client IP address in ASCII form. If the IP address cannot be retrieved, the length is set to zero.

**Example**

The following command enables the sending of the rem_addr field to a Cisco Secure ACS server for a TACACS+ login request:
rem_addr client-ip arg1
server

Configures TACACS+ AAA service-related parameters for use in authenticating StarOS administrative users via a TACACS+ server.

**Important:** Once a TACACS+ server is configured with the `server` command, TACACS+ AAA services for StarOS must be enabled using the `aaa tacacs+` command in Global Configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > TACACS+ Configuration
`configure > tacacs mode`

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-tacacs)#
```

**Syntax**

```plaintext
server priority priority_number ip-address ip_address [ service { authentication | authorization | accounting } ] [ port port_number ] [ { encrypted password shared_secret | password text_password | key text_password } ] [ timeout seconds ] [ retries num_retries ] [ nas-source-address ip_address ]
```

no server priority priority_number

Removes a specified server (by priority number) from the TACACS+ server list.

**priority priority_number**

Specifies the order in which TACACS+ servers are to be tried. The priority number corresponds to a configured TACACS+ server.

*For releases prior to 18.2,* `priority_number` can be an integer from 1 (highest priority) to 3 (lowest priority).

*For releases 18.2+,* `priority_number` can be an integer from 1 (highest priority) to 4 (lowest priority).

If no server with priority 1 is specified, the next highest priority is used. If the specified priority matches that of a TACACS+ server already configured, any previously defined server configuration parameter(s) for that priority are returned to the default setting(s).

**ip-address**

Specifies the IP address of the TACACS+ server in IPv4 dotted-decimal notation. Only one IP address can be defined for a given `server priority`
[ service { authentication | authorization | accounting } ]

**service**: *Release 12 and later systems only*: Specifies one or more of the AAA services that the specified TACACS+ server will provide. Use of the `service` keyword requires that at least one of the available services be specified. If the `service` keyword is not used, StarOS will use the TACACS+ server for all AAA service types. The default is to use authentication, authorization and accounting. Available service types are:

- **authentication**: The specified TACACS+ server should be used for authentication. If a TACACS+ authentication server is not available, TACACS+ will not be used for authorization or accounting.
- **authorization**: The specified TACACS+ server should be used for authorization. If TACACS+ authentication is not used, TACACS+ authorization will not be used. If no authorization server is specified and the user is authenticated, the user will remain logged in with minimum privileges (Inspector level).
- **accounting**: The specified TACACS+ server should be used for accounting. If TACACS+ authentication is not used, TACACS+ accounting will not be used. If no accounting server is specified and the user is authenticated, no accounting will be performed for the user.

**port**

Specifies the TCP port number to use for communication with the TACACS+ server. `port_number` can be an integer from 1 through 65535. If a port is not specified, StarOS will use port 49.

[ { encrypted password shared_secret | password text_password | key text_password } ]

Specify the encrypted or plain-text password:

- **encrypted password shared_secret**: Specifies the encrypted value of the shared secret key. The server-side configuration must match the decrypted value for the protocol to work correctly. If `encrypted password` is specified, specifying `password` is invalid. No encryption is used if this value is null (""). The encrypted password can be an alphanumeric string of 1 through 100 characters. If neither an `encrypted password` or `password` is specified, StarOS will not use encryption.

- **password plain_text_password**: *Release 12.0 and later systems*. Instead of using an encrypted password value, the user can specify a plain-text value for the password. If the `password` keyword is specified, specifying `encrypted password` is invalid. A null string ("") represents no encryption. The password can be an alphanumeric string of 1 through 32 characters. If neither an `encrypted password` or `password` is specified, then StarOS will not use encryption.

- **key plain_text_password**: *Release 11.0 systems only*. Instead of using an encrypted password value, the user can specify a plain-text key value for the password. If the `key` keyword is specified, then specifying `encrypted password` is invalid. A null string represents no encryption. The password can be from 1 to 32 alphanumeric characters in length. If neither an `encrypted password` or `key` is specified, then StarOS will not use encryption.

[ timeout seconds ]

Specifies the number of seconds to wait for a connection timeout from the TACACS+ server. `seconds` can be an integer from 1 through 1000. If no timeout is specified, StarOS will use the default value of 10 seconds.
Server Configuration Mode Commands

retries number

**Release 12 and later systems only:** Specifies the number of retry attempts at establishing a connection to the TACACS+ server if the initial attempt fails. `retries number` can be an integer from 0 through 100. The default is 3. Specifying 0 (zero) retries results in StarOS trying only once to establish a connection. No further retries will be attempted.

```
server priority 2 ip-address 192.156.1.1 authentication
```

Usage

Use this command to specify TACACS+ service parameters for a specified TACACS+ server.

Example

The following command configures a priority 2, TACACS+ authentication server at IP address 192.156.1.1:

```
server priority 2 ip-address 192.156.1.1 authentication
```
Chapter 292
Telnet Configuration Mode Commands

The Telnet Configuration Mode is used to manage the telnet server options for the current context.

**Mode**

Exec > Global Configuration > Context Configuration > Telnet Configuration

```
classic > context context_name > server telnet
```

Entering the above command sequence results in the following prompt:

```
[local] host_name(config-telnetd) #
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

dend

**Usage**
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Use this command to return to the parent configuration mode.
max servers

Configures the maximum number of telnet servers that can be started within any 60-second interval. If this limit is reached, the system waits two minutes before trying to start any more servers.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Telnet Configuration
    configure > context context_name > server telnet

Entering the above command sequence results in the following prompt:

[local]host_name(config-telnetd)#

Syntax

max servers count

    count

Default: 40
Specifies the maximum number of servers that can be spawned in any 6-second interval. count must be an integer from 1 through 100.

Usage
Set the number of servers to tune the system response as a heavily loaded system may need more servers to support the incoming requests.
The converse would be true as well in that a system can benefit by reducing the number of servers such that telnet services do not cause excessive system impact to other services.

Example

max servers 50
Chapter 293
TFTP Configuration Mode Commands

The TFTP configuration mode is used to manage the TFTP (Trivial File Transfer Protocol) servers for the current context.

Mode

Exec > Global Configuration > Context Configuration > Tunnel TFTP Configuration

configure > context context_name > server tftpd

Entering the above command sequence results in the following prompt:

[local]host_name(config-tftpd)#

Important: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

end

**Usage**
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**
Use this command to return to the parent configuration mode.
max servers

Configures the maximum number of TFTP servers that can be started within any 60-second interval. If this limit is reached, the system waits two minutes before trying to start any more servers.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Tunnel TFTP Configuration

configure > context context_name > server tftp

Entering the above command sequence results in the following prompt:

[local] host_name(config-tftp)#

Syntax

max servers count

count

Default: 40
Specifies the maximum number of servers that can be spawned in any 60-second interval. count must be an integer from 1 through 100.

Usage
Set the number of servers to tune the system response as a heavily loaded system may need more servers to support the incoming requests.
The converse would be true as well in that a system can benefit by reducing the number of servers such that TFTP services do not cause excessive system impact to other services.

Example

max servers 50
Policy-Group is used to form a set of configured Policy-Maps for the Traffic Policy feature. Multiple policies can be applied for a subscriber session flow within a destination context.

Mode

Exec > Global Configuration > Context Configuration > Traffic Policy Group Configuration

configure > context context_name > policy-group name group_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-policy-group)#

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Use this command to return to the parent configuration mode.
policy

Assigns traffic policies, pre-configured in Policy-Map Configuration mode, to a Policy Group for flow-based traffic policing of a subscriber session flow.

Product

- HA
- HSGW
- PDSN
- P-GW
- SAEGW
- SCM

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > Context Configuration > Traffic Policy Group Configuration

```
configure > context context_name > policy-group name group_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-policy-group)#
```

Syntax

```
[ no ] policy policy_map_name precedence value direction [ in | out ]
```

- **no**
  
  Disables/removes configured policy for traffic policing.

- **direction [ in | out ]**
  
  Specifies the direction in which the policies need to be applied.

- **policy policy_map_name**
  
  Specifies the policy name as an alphanumeric string of 1 through 15 characters.

- **precedence value**
  
  Specifies the precedence of traffic policies to resolve.
  *value* is an integer from 1 through 16. If a session flow matches multiple policies, this keyword resolves them.

Usage

Use this command to form a policy-group with a set of pre-configured Policy-Maps.

Example

The following commands assigns the traffic policy *policymap1* with precedence 2.
policy policymap1 precedence 2
Chapter 295  
Traffic Policy-Map Configuration Mode Commands

A Policy-Map imposes a flow-based traffic policy for Traffic Policy feature within a destination context. It designates the flow treatment based on the classification rules configured in Class-Map mode for a subscriber session flow.

Mode

Exec > Global Configuration > Context Configuration > Traffic Policy Map Configuration

`configure > context context_name > policy-map name map_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-policy-map)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
3gpp2 data-over-signaling

Configures 3GPP2-related flow treatment policy for the flow-based traffic policing of subscriber sessions.

**Product**
- HA
- HSGW
- PDSN
- P-GW
- SAEGW
- SCM

**Privilege**
- Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > Traffic Policy Map Configuration

`configure > context context_name > policy-map name map_name`

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-policy-map)#`

**Syntax**

3gpp2 data-over-signaling marking [ class-map class_name ]

no 3gpp2 data-over-signaling marking

- **no**
  
  Disables configured 3GPP2-related flow treatment policy.

- **class-map class_name**
  
  Associates class map to be used for selective data over signaling (DOS) marking. `class_name` is an alphanumeric string of 1 through 15 characters.

- **marking**
  
  Indicates 3GPP2-related traffic flow for data over signaling channel.

**Usage**

Use this command to mark traffic flows for 3GPP2-related policy.

**Example**

```
3gpp2 data-over-signaling marking
```
access-control

Configures the access control action for traffic flows matching the Class-Map rules.

Product
ASN-GW
HA
HSGW
PDSN
P-GW
SAEGW
SCM

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Traffic Policy Map Configuration
configure > context context_name > policy-map name map_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-policy-map)#

Syntax

access-control { allow | discard }

allow
Allows the packets, if the policy matches with the criteria defined in the Class-Map assigned to the specific traffic policy.

discard
Discards the packets, if the policy matches with the criteria defined in the Class-Map assigned to the specific traffic policy.

Usage
Configures the action or treatment for traffic flows match criteria specified in the assigned Class-Map.

Example
The following command allows the packets or traffic flow on matching with criteria specified in assigned Class-Map for specific traffic policy.

access-control allow
accounting suppress

Suppresses accounting action for traffic flows matching the policy map.

**Product**

ASN-GW

HA

HSGW

PDSN

P-GW

SAEGW

SCM

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > Traffic Policy Map Configuration

```
configure > context context_name > policy-map name map_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-policy-map)#
```

**Syntax**

```
[ no ] accounting suppress
```

- **no**

Removes the suppression of accounting for traffic flow matching this policy map.

**Usage**

Use this command to suppress accounting action on traffic flow matching this policy map. Policy maps configured for accounting suppression are used to implement the QChat Billing Suppression feature that selectively starts and terminates accounting sessions based on the categorization of traffic as being interesting or non-interesting. See the `accounting trigger` command.

**Example**

The following command configures suppression of accounting on traffic flows matching this policy map:

```
accounting suppress
```
accounting trigger

Configures an accounting trigger policy map to selectively start and terminate accounting sessions based on the categorization of traffic as being interesting or non-interesting. This command supports the QCHAT Billing Suppression feature.

Product
HSGW
PDSN
P-GW
SAEGW
SCM

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Traffic Policy Map Configuration
configure > context context_name > policy-map name map_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-policy-map)#

Syntax

[ no | default ] accounting trigger { inactivity-timeout | interesting-traffic | intra-service-handoff }

default
Sets or restores the default value assigned for specified parameter.

no
Disables previously configured triggers.

inactivity-timeout
Generates an accounting Stop message if there has been no data activity on the session for the interim accounting timeout interval.
Default: disabled

interesting-traffic
Generates an accounting Start message upon arrival of interesting traffic.
Default: disabled

intra-service-handoff
Generates accounting Start and Stop messages during intra-service handoffs.
Default: enabled
If disabled, the messages are suppressed during the handoffs. The current accounting session continues and no Stop or Start messages are generated during the intra-service handoff.

Usage

Use this command to configure an accounting trigger policy map (ATPM) to selectively start and terminate accounting sessions based on the categorization of traffic as being interesting or non-interesting. This command supports the QChat Billing Suppression feature.

Interesting traffic is identified as traffic that does not match any of the other Accounting Policy Maps (APMs) configured for accounting suppression. See the `accounting suppress` command.

An ATPM is similar to an APM, but without the class map rules. The ATPM is configured as of type accounting using the `type accounting` command.

Optionally, timeout can be triggered when there is no data traffic for the interim accounting timeout interval using the `accounting trigger inactivity-timeout stop` command. On timeout, the accounting session is terminated and an Accounting Stop message is sent. A new accounting session is created if interesting traffic resumes.

In the ATPM, the trigger to start accounting for interesting traffic is configured using the `accounting trigger interesting-traffic` command. Accounting Start is triggered on arrival of interesting traffic, or change in airlink parameters conveyed through active-start airlink record. If an active-start record was included in the initial connection setup, Accounting Start is not triggered. But if the active-start comes separately and is the first one for the session, it is treated as airlink change and an Accounting Start is sent.

The ATPM should have the lowest precedence among the APMs.

As the airlink events are generated on the ingress side, the ATPM must be included in a policy group that is applied to the ingress direction in the subscriber profile. The configuration is applicable only for standard trigger policy and session based accounting mode.

Example

The following command sets the trigger to generate accounting start message upon arrival of interesting traffic:

```
accounting trigger interesting-traffic
```
class-map

Assigns a traffic classification rule (Class-Map) to the policy map.

**Product**
- ASN-GW
- HA
- HSGW
- PDSN
- P-GW
- SAEGW
- SCM

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Traffic Policy Map Configuration

```
configure > context context_name > policy-map name map_name
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-policy-map)#
```

**Syntax**

```
[ no ] class-map name
```

- **no**
  Enables or disables `class-map`

- **name**
  Specifies the name of the class map assigned for this policy map. The class map should have been preconfigured via the Class Map Configuration Mode.
  `name` must be an alphanumeric a string of 1 through 15 characters.

**Usage**

Use this command to assign a class map to the policy map for traffic policing. The class map is configured in the Class Map Configuration Mode.

**Example**

The following command assigns the class map `classification1` to the current policy map:

```
class classification1
```
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Use this command to return to the parent configuration mode.
flow-tp-trigger

This command specifies that the traffic volume will be calculated based on the traffic on the flow.

**Product**

ASN-GW
HA
HSGW
PDSN
P-GW
SAEGW
SCM

**Privilege**

Security Administrator, Administrator

**Mode**

Exec > Global Configuration > Context Configuration > Traffic Policy Map Configuration

configure > context context_name > policy-map name map_name

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-policy-map)#
```

**Syntax**

```
flow-tp-trigger volume traffic_volume_threshold

no flow-tp-trigger volume

traffic_volume_threshold
```

Specifies the volume threshold to trigger traffic policing. `volume` must be an integer from 1 through 4294967295.

**Usage**

This command is available if you have purchased and installed the Intelligent Traffic Control License on your system. Use this command to calculate the traffic volume based on the traffic on the flow.

**Example**

```
flow-tp-trigger volume 500
```
ip header-compression

Enables the system to mark IP flows for Robust Header Compression (RoHC).

Product

ASN-GW
HA
HSGW
PDSN
P-GW
SAEGW
SCM

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > Context Configuration > Traffic Policy Map Configuration

configure > context context_name > policy-map name map_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-policy-map)#

Syntax

[ no ] ip header-compression rohc flow-marking

no

Disables the setting.

rohc flow-marking

Marks the IP flow for SO67 and PPP RoHC.

Usage

Use this command to mark IP flows for SO67 and PPP RoHC.

Example

ip header-compression rohc flow-marking
qos encaps-header

Enables and configures Quality of Service (QoS) policy to use Differentiated Service Code Point (DSCP) marking in IP header fields for the flow-based traffic policing to subscriber session flow.

Product
- ASN-GW
- HA
- HSGW
- PDSN
- P-GW
- SAEGW
- SCM

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Traffic Policy Map Configuration

configure > context context_name > policy-map name map_name

Entering the above command sequence results in the following prompt:

[context_name] host_name(config-policy-map) #

Syntax

qos encaps-header dscp-marking { dscp_code | copy-from-user-datagram [ ignore-pcf-signaled-dscp ] | user-datagram }

no qos encaps-header dscp-marking { dscp_code | copy-from-user-datagram [ ignore-pcf-signaled-dscp ] }

no
Enables/Disables the qos encaps-header.
The value must be expressed as a hexadecimal value from 0x00 through 0x3F.

dscp-marking dscp_code
Uses the DSCP code value marked in the IP header of packet/flow to determine the QoS for traffic policing.
dscp_code must be expressed as a hexadecimal number from 0x00 through 0x3F.

copy-from-user-datagram
Uses the DSCP code value from the user datagram (UDP header) to determine the QoS for traffic policing.

ignore-pcf-signaled-dscp
Overrides the highest priority DSCP value signaled by the PCF.
user-datatype

Uses the DSCP value copied from the user datagram.

Usage

Use this command to apply the QoS policy based on the DSCP value encapsulated in the IP packet header to police subscriber session traffic flows.

Important: For more information on the QoS traffic policing, see the System Administration Guide.

Example

The following command sets QoS policy with DSCP code value to 0x0C for Class 1, silver (AF12):

```
qos encaps-header dscp-marking 0x0c
```
qos traffic-police

Enables and configures Quality of Service (QoS) policy for flow-based traffic policing of subscriber session flows on a per-flow basis.

Product

ASN-GW
HA
HSGW
PDSN
P-GW
SAEGW
SCM

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > Context Configuration > Traffic Policy Map Configuration
configure > context context_name > policy-map name map_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-policy-map)#

Syntax

qos traffic-police committed bps peak bps burst-size byte exceed-action { drop | lower-ip-precedence | allow } violate-action { drop | lower-ip-precedence | allow }

no qos traffic-police

no

Enables/Disables the qos traffic-police

Important: This parameter should be configured to be greater than the following two values: 1) three times greater than packet MTU for the subscriber connection, OR 2) three seconds worth of token accumulation within the “bucket” for the configured peak-data-rate.

burst-size bytes

Default: 3000
Specifies the allowed peak burst size in bytes. bytes must be an integer from 0 through 4294967295.

Important: This parameter should be configured to be greater than the following two values: 1) three times greater than the packet MTU for the subscriber connection, OR 2) three seconds worth of token accumulation within the “bucket” for the configured peak-data-rate.
Traffic Policy-Map Configuration Mode Commands

**qos traffic-police**

---

**committed bps**
Default: 144000
Specifies the committed data rate (guaranteed-data-rate) in bits per second (bps). 
*bps* must be an integer from 0 through 4294967295.

**exceed-action { drop | lower-ip-precedence | allow }**
Default: *lower-ip-precedence*
Specifies the action to take on packets that exceed the committed-data-rate but do not violate the peak-data-rate. The following actions are supported:
*drop*: Drops the packet
*lower-ip-precedence*: Transmits the packet after lowering the *ip-precedence*
*allow*: Transmits the packet

**peak bps**
Default: 256000
Specifies the peak data-rate for the subscriber in bits per second (bps). 
*bps* must be an integer from 0 through 4294967295.

**violate-action { drop | lower-ip-precedence | allow }**
Default: *drop*
Specifies the action to take on the packets that exceed both the committed-data-rate and the peak-data-rate. The following actions are supported:
*drop*: Drops the packet
*lower-ip-precedence*: Transmits the packet after lowering the *IP precedence*
*allow*: Transmits the packet

---

**Usage**

Use this command to apply the QoS policy to a subscriber session flow for flow-based traffic policing.

---

**Important:** For additional information on the QoS traffic policing, see the *System Administration Guide*.

---

**Example**

The following command sets the committed data rate to 102400 bps with a peak data rate of 128000 bps and a burst size of 2048 bytes. This lowers the IP precedence when the committed-data-rate is exceeded and drops the packets when the peak-data-rate are violated:

```
qos traffic-police committed 102400 peak 128000 burst-size 2048 exceed-
action lower-ip-precedence violate-action drop
```
qos user-datagram dscp-marking

Enables and configures Quality of Service (QoS) policy related to differentiated service code point (DSCP) marking in the user datagrams of subscriber session flows on a per-flow basis.

Product
ASN-GW
HA
HSGW
PDSN
P-GW
SAEGW
SCM

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Traffic Policy Map Configuration
configure > context context_name > policy-map name map_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-policy-map)#

Syntax

qos user-datagram dscp-marking dscp_code

no qos user-datagram dscp-marking

---

dscp_code

Specifies the use of the DSCP code value marked in the IP header of packet/flow to determine the QoS for traffic policing. dscp_code must be expressed as a hexadecimal number from 0x00 through 0x3F.

Usage

Use this command to apply the QoS policy to subscriber session flow by DSCP marking in user datagram.

Example

The following command sets DSCP marking for user datagram as 0x01 for QoS to subscriber session flow:

qos user-datagram dscp-marking 0x01
**sess-tp-trigger**

Configures the trigger for traffic policing based on the traffic volume for a subscriber session.

**Product**
- ASN-GW
- HA
- HSGW
- PDSN
- P-GW
- SAEGW
- SCM

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Traffic Policy Map Configuration
`configure > context context_name > policy-map name map_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-policy-map)#
```

**Syntax**

```
(sess-tp-trigger volume volume direction { both | downlink | uplink })
no sess-tp-trigger
```

**Usage**
Use this command to trigger traffic control based on the traffic volume for a subscriber session. This command requires the purchase and installation of a license.

**Example**
```
sess-tp-trigger 500
```
**type**

Specifies the type of traffic policy within a specific Policy-Map.

**Product**

- ASN-GW
- HA
- HSGW
- PDSN
- P-GW
- SAEGW
- SCM

**Privilege**

Administrator

**Mode**

Exec > Global Configuration > Context Configuration > Traffic Policy Map Configuration

`configure > context context_name > policy-map name map_name`

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-policy-map)#`

**Syntax**

```
type { accounting | dynamic { three-gpp2 rev-A profile-id { any | id profile_id | range low_value to high_value } flow-id { any | id flow_id | range low_value to high_value } | pre-provisioned wimax asn-service-profile-id { any | id service_id } asn-pdfid { any | id pdf_id } | static | template }
```

---

**accounting**

Specifies the type of traffic policing as accounting for this specific policy map. This configuration is used for enabling/disabling the accounting of different flows matching conditions within this Policy-Map.

---

**dynamic**

Identifies the type of policy map as dynamic.

---

**three-gpp2 rev-A**

Configures the dynamic policy map type for CDMA2000-3GPP2 RevA service.

---

**profile-id { any | id profile_id | range low_hex to high_hex }**

Specifies the profile id matching within this policy map.

- `any`: allows any profile identifier matching this policy map.
- `id profile_id`: allows specific profile identifier matching with in this policy map. `profile_id` must be a hexadecimal number from 0x0 to 0xFFFF.
**range low_value to high_value:** identifies a range in which a profile identifier must fall within to be considered a match. `low_value` and `high_value` must be either a hexadecimal number from 0x0 to 0xFFFF, or an integer from 0 through 65535 characters.

**flow-id { any | id flow_id | range low_hex to high_hex }**

Specifies the flow id matching in this policy map.

- **any** allows any flow identifier matching within this policy map.
- **id flow_id** allows specific flow identifier matching within this policy map. `flow_id` must be either a hexadecimal number from 0x0 to 0xFFFF, or an integer from 0 to 65535.
- **range low_value to high_value** identifies a range in which a flow identifier must fall within to be considered a match. `low_value` and `high_value` must be either a hexadecimal number from 0x0 to 0xFFFF, or an integer from 0 to 65535.

**pre-provisioned**

Identifies the type of policy map as pre-provisioned.

**wimax**

Configures WiMAX service policy map in an ASN-GW service.

**asn-service-profile { any | id service_id }**

Specifies the ASN Service profile identifier to match within this policy map.

- **any** Allows any ASN Service Profile Identifier matching within this policy map.
- **id service_id** Allows specific Service Profile matching to a specified identifier. `service_id` must be an integer from 1 to 65535 that matches a service ID that was configured in the Subscriber Configuration Mode.

**asn-pdfid { any | id pdf_id }**

Specifies the ASN Packet Data Flow Identifier to match within this policy map.

- **any** Allows any ASN Packet Data Flow Identifier matching within this policy map.
- **id pdf_id** Allows specific Packet Data Flow matching to a specified identifier. `pdf_id` must be an integer from 1 to 255 that matches a PDF ID that was configured in the Subscriber Configuration Mode.

**static**

Specifies the type of traffic policing as static for this specific Policy Map. In this type of policy, the traffic flow classification and flow treatment is pre-defined with classification rules through Class-Map configuration.

This is the detailed type of policy map.

**template**

Specifies the type of traffic policy to as a template to all subscribers associated with this policy map.

**Usage**

**Example**

The following commands configures the traffic policy for this Policy-Map as static:

```
  type static
```
The following commands configure the traffic policy for this Policy-Map as pre-provisioned for WiMAX service requiring a match of any service profile and PDF id of 3:

```
  type pre-provisioned wimax asn-service-profile any asn-pdfid id 3
```
The Tunnel Interface Configuration Mode is used to create and manage the IP interfaces for various types of tunnels including associated parameters, such as addresses and address resolution options.

Mode

Exec > Global Configuration > Context Configuration > Tunnel Interface Configuration

configure > context context_name > interface interface_name tunnel

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-if-tunnel)#

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
description

Enters descriptive text for the current interface.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Tunnel Interface Configuration

configure > context context_name > interface interface_name tunnel

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-if-tunnel)#

Syntax

description text

no description

no

Clears the description for the interface.

text

Contains the descriptive text for this interface. text must be an alphanumeric string of 0 through 79 characters. If spaces are required, the string must be bracketed with double quotation marks (""). The interface description is case sensitive.

Usage

Set the description to provide useful information regarding the interface’s primary function, services, end users, etc.

Example

The following command describes this interface:

    description sampleInterfaceDescriptiveText
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
dend

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

exit

Usage
Use this command to return to the parent configuration mode.
ip address

Configures the IPv4 address for this tunnel interface.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Tunnel Interface Configuration

```
configure > context context_name > interface interface_name tunnel
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-tunnel)#
```

**Syntax**

```
ip address [ip_address/ip_mask | ip_address ip_mask]
no ip address ip_address
```

- **no**
  - Removes the configured IPv4 address bound to a tunnel interface.

```
ip_address/ip_mask | ip_address ip_mask
```

- Specifies a destination IP address or group of addresses that will use this route.
  - `ip_address/ip_mask`: Specifies a combined IP address subnet mask bits to indicate what IP addresses to which the route applies. `ip_address/ip_mask` must be specified using IPv4 dotted-decimal and CIDR notation. `ip_mask` is an integer which is the number of bits in the subnet mask.
  - `ip_address ip_mask`: Specifies an IP address and the networking (subnet) mask pair which is used to identify the set of IP addresses to which the route applies. `ip_address` must be specified using the IPv4 dotted-decimal notation. `ip_mask` must be specified using the IPv4 dotted-decimal notation as network mask for subnets.

The mask as specified by `ip_mask` or resulting from `ip_address/ip_mask` is used to determine the network for packet routing.

- Zeros (“0”) in the resulting mask indicate that the corresponding bit in the IP address is not significant in determining the network for packet routing.
- Ones (“1”) in the resulting mask indicate the corresponding bit in the IP address is significant in determining the network.

**Usage**

Use this command to bind the IPv4 address to a tunnel interface. This address does not affect the encapsulation of packets going out on the tunnel interface.

**Example**

The following command will assign the 10.2.3.4 as IPv4 address to this tunnel interface:

```
ip address 10.2.3.4
```
ipv6 address

Configures the IPv6 address for the specific tunnel interface.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Tunnel Interface Configuration
configure > context context_name > interface interface_name tunnel

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-if-tunnel)#

Syntax

ipv6 address ipv6_address/ipv6_mask

no ipv6 address ipv6_address

no

Removes the configured IPv6 address bound to a tunnel interface.

ipv6_address/ipv6_mask

Specifies a destination IP address or group of addresses that will use this route.
ipv6_address/ipv6_mask: Specifies a combined IP address subnet mask bits to indicate what IP addresses to which the route applies. ipv6_address/ipv6_mask must be specified using IPv6 colon-separated-hexadecimal and CIDR notation. ipv6_mask is a numeric value which is the number of bits in the subnet mask.

Usage

Use this command to bind the IPv6 address to a tunnel interface. This address does not affect the encapsulation of packets going out on the tunnel interface.

Example

The following command will assign the 1001::2:010:1234 as IPv6 address to this tunnel interface:

ipv6 address 1001::2:010:1234
tunnel-mode

Configures the tunnel mode type for this tunnel interface. It also enters the specific tunnel configuration mode, if required.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > Tunnel Interface Configuration

```bash
configure > context context_name > interface interface_name tunnel
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-if-tunnel)#
```

**Syntax**

```bash
tunnel-mode { gre | ipv6ip }
```

**default tunnel-mode**

---

**default**

Sets the default tunnel mode for this interface. By default, the tunnel mode is set to IPv6-to-IPv4 type.

---

**gre**

Default: Disabled

Sets the tunnel interface mode to Generic Routing Encapsulation (GRE) type and enters the GRE Tunnel Configuration mode, if required.

---

**ipv6ip**

Default: Enabled

Sets the tunnel interface mode to IPv6-to-IPv4 type and creates the IPv6-to-IPv4 Tunnel Configuration mode, if required.

---

**Usage**

Use this command to set the tunnel mode type of GRE or IPv6-to-IPv4 for the tunneling interface.

**Example**

The following command sets the tunnel mode to GRE for specific interface:

```bash
tunnel-mode gre
```
Chapter 297
UDR Format Configuration Mode Commands

The UDR Format Configuration Mode enables configuring User Detail Record (UDR) formats.

Mode

Exec > ACS Configuration > UDR Format Configuration

`active-charging service service_name > udr-format format_name`

Entering the above command sequence results in the following prompt:

`[local]host_name(config-acs-udr)#`

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
attribute

This command allows you to specify the fields and their order in UDRs.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > UDR Format Configuration

```
active-charging service service_name > udr-format format_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acs-udr)#
```

**Syntax**

```
```

**no attribute attribute [ priority priority ]**

- `no`
  - If added previously, removes the specified attribute from the UDR format.

**attribute attribute**

Specifies the attribute.

- `attribute` must be one of the following:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>diameter-session-id</td>
<td>This attribute reports Diameter session identifier.</td>
</tr>
<tr>
<td></td>
<td><strong>Important:</strong> This attribute is customer specific, and is only available in 8.3 and later releases.</td>
</tr>
<tr>
<td>failure-handling-mode</td>
<td>This attribute reports failure handling mode in case the Online Charging System (OCS) goes abnormal.</td>
</tr>
<tr>
<td>radius-called-station-id</td>
<td>This attribute reports the Called Station ID of the mobile handling the flow.</td>
</tr>
<tr>
<td>radius-calling-station-id</td>
<td>This attribute reports the Calling Station ID of the mobile handling the flow.</td>
</tr>
<tr>
<td>radius-fa-nas-identifier</td>
<td>This attribute reports the RADIUS NAS identifier of Foreign Agent (FA).</td>
</tr>
<tr>
<td>radius-fa-nas-ip-address</td>
<td>This attribute reports the RADIUS IP address of Foreign Agent (FA).</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>radius-nas-identifier</td>
<td>This attribute reports the RADIUS NAS identifier.</td>
</tr>
<tr>
<td>radius-nas-ip-address</td>
<td>This attribute reports the RADIUS NAS IP address.</td>
</tr>
<tr>
<td></td>
<td>Note that this attribute is interchangeable with sn-st16-ip-addr for the user.</td>
</tr>
<tr>
<td>radius-user-name</td>
<td>This attribute reports the user name associated with the flow.</td>
</tr>
<tr>
<td>sn-3gpp2-bsid</td>
<td>This option has been deprecated.</td>
</tr>
<tr>
<td></td>
<td>To configure this attribute see the rule-variable command.</td>
</tr>
<tr>
<td>sn-3gpp2-carrier-id</td>
<td>This option has been deprecated.</td>
</tr>
<tr>
<td></td>
<td>To configure this attribute see the rule-variable command.</td>
</tr>
<tr>
<td>sn-3gpp2-esn</td>
<td>This option has been deprecated.</td>
</tr>
<tr>
<td></td>
<td>To configure this attribute see the rule-variable command.</td>
</tr>
<tr>
<td>sn-3gpp2-meid</td>
<td>This option has been deprecated.</td>
</tr>
<tr>
<td></td>
<td>To configure this attribute see the rule-variable command.</td>
</tr>
<tr>
<td>sn-3gpp2-service-option</td>
<td>This option has been deprecated.</td>
</tr>
<tr>
<td></td>
<td>To configure this attribute see the rule-variable command.</td>
</tr>
<tr>
<td>sn-acct-beginning-session</td>
<td>This attribute reports the Session Beginning information.</td>
</tr>
<tr>
<td></td>
<td><strong>Important:</strong> This attribute is customer specific, and is only available in 8.3 and later releases.</td>
</tr>
<tr>
<td>sn-acct-continue</td>
<td>This attribute reports the Session Continue information.</td>
</tr>
<tr>
<td></td>
<td><strong>Important:</strong> This attribute is customer specific, and is only available in 8.3 and later releases.</td>
</tr>
<tr>
<td>sn-acct-session-id</td>
<td>This attribute reports the Accounting Session identifier.</td>
</tr>
<tr>
<td>sn-acct-session-time</td>
<td>This attribute reports the duration from acct-status-type:start to acct-status-type:stop.</td>
</tr>
<tr>
<td></td>
<td><strong>Important:</strong> This attribute is customer specific, and is only available in 8.3 and later releases.</td>
</tr>
<tr>
<td>sn-acct-status-type</td>
<td>This attribute reports the Accounting Status identifier.</td>
</tr>
<tr>
<td></td>
<td><strong>Important:</strong> This attribute is customer specific, and is only available in 8.3 and later releases.</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>sn-charging-type</td>
<td>This attribute reports the charging type: offline or online.</td>
</tr>
<tr>
<td></td>
<td><strong>Important:</strong> This attribute is customer specific, and is only available in 8.3 and later releases.</td>
</tr>
<tr>
<td>sn-closure-reason</td>
<td>This attribute reports the reason for termination of the flow/UDR:</td>
</tr>
<tr>
<td></td>
<td>• 0 = CALL_TERMINATION — normal, such as subscriber session ended</td>
</tr>
<tr>
<td></td>
<td>• 1 = PDSN_HO — handoff control processing specified</td>
</tr>
<tr>
<td></td>
<td>• 2 = TIME_LIMIT</td>
</tr>
<tr>
<td></td>
<td>• 3 = VOLUME_LIMIT</td>
</tr>
<tr>
<td></td>
<td>• 4 = MGMT_INTERVENTION</td>
</tr>
<tr>
<td></td>
<td>• 5 = ACCT_SESS_START</td>
</tr>
<tr>
<td></td>
<td>• 6 = CCRU_RESPONSE</td>
</tr>
<tr>
<td></td>
<td>• 7 = OFFLINE_CHARGING — for UDRs generated when offline charging trigger is received from DCCA</td>
</tr>
<tr>
<td>sn-content-id</td>
<td>This attribute reports the unique identifier for the content-id.</td>
</tr>
<tr>
<td>sn-content-label</td>
<td>This attribute reports the identifier for text label for content-id.</td>
</tr>
<tr>
<td>sn-content-vol</td>
<td>This attribute reports the identifier for content volume.</td>
</tr>
<tr>
<td>sn-correlation-id</td>
<td>This attribute reports the RADIUS correlation identifier.</td>
</tr>
<tr>
<td>sn-duration</td>
<td>This attribute reports the time difference between the first and last packet of a single data flow accounted in the UDR record. For example, the time difference between the first ICMP echo request and the last ICMP echo response before the record gets written for the content-id.</td>
</tr>
<tr>
<td>sn-end-time [ format format]</td>
<td>This attribute reports the timestamp for last packet of flow in UTC.</td>
</tr>
<tr>
<td>sn-fa-correlation-id</td>
<td>This attribute reports the RADIUS Correlation Identifier of the Foreign Agent (FA).</td>
</tr>
<tr>
<td>sn-fa-ip-address</td>
<td>This attribute reports IP address of the FA.</td>
</tr>
<tr>
<td>sn-filler-blank</td>
<td>This attribute inserts a blank filler field, generates an empty UDR field.</td>
</tr>
<tr>
<td>sn-filler-zero</td>
<td>This attribute inserts a “0” in the UDR field.</td>
</tr>
<tr>
<td>sn-format-name</td>
<td>This attribute reports name of the UDR format used.</td>
</tr>
<tr>
<td>sn-group-id</td>
<td>This attribute reports the sequence group identifier for the records.</td>
</tr>
<tr>
<td>sn-ha-ip-address</td>
<td>This attribute reports IP address of the Home Agent (HA).</td>
</tr>
<tr>
<td></td>
<td><strong>Important:</strong> This attribute is customer specific, and is only available in 8.3 and later releases.</td>
</tr>
<tr>
<td>Attribute</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>sn-local-seq-no</strong></td>
<td>This attribute reports unique local sequence number of UDR identifier per ACSMgr/SessMgr and linearly increasing in UDR file.</td>
</tr>
<tr>
<td><strong>sn-ocs-ip-address</strong></td>
<td>This attribute reports IP address of the Online Charging Server. <strong>Important:</strong> This attribute is customer specific, and is only available in 8.3 and later releases.</td>
</tr>
<tr>
<td><strong>sn-rulebase</strong></td>
<td>This attribute reports name of the ACS rulebase used.</td>
</tr>
<tr>
<td><strong>sn-sequence-no</strong></td>
<td>This attribute reports unique sequence number (per <strong>sn-sequence-group</strong> and <strong>radius-nas-ip-address</strong>) of UDR identifier and linearly increasing in UDR file.</td>
</tr>
<tr>
<td><strong>sn-served-bsa-addr</strong></td>
<td>This attribute reports address of Base Station Area being served.</td>
</tr>
<tr>
<td><strong>sn-service-name</strong></td>
<td>This attribute reports name of the ACS service.</td>
</tr>
<tr>
<td><strong>sn-st16-ip-addr</strong></td>
<td>This option has been deprecated.</td>
</tr>
<tr>
<td><strong>sn-start-time [format format]</strong></td>
<td>This attribute reports timestamp for first packet of flow in UTC. <strong>Important:</strong> This attribute is customer specific, and is only available in 8.3 and later releases.</td>
</tr>
<tr>
<td><strong>sn-stream-number</strong></td>
<td>This attribute reports unique UDR billing record identifier. <strong>Important:</strong> This attribute is customer specific, and is only available in 8.3 and later releases.</td>
</tr>
<tr>
<td><strong>sn-subscriber-id</strong></td>
<td>This attribute reports subscriber ID.</td>
</tr>
<tr>
<td><strong>sn-subscriber-nat-flow-ip</strong></td>
<td>This attribute reports NAT IP address(es) of NAT-enabled subscriber.</td>
</tr>
<tr>
<td><strong>sn-timestamp</strong></td>
<td>This attribute reports timestamp when the UDR is actually generated. <strong>Important:</strong> This attribute is customer specific, and is only available in 8.3 and later releases.</td>
</tr>
</tbody>
</table>


Specifies the timestamp format.

**localtime**

Specifies the local time. By default, timestamps are displayed in Coordinated Universal Time (UTC).
attribute

( bytes | pkts ) { downlink | uplink }
Specifies bytes/packets sent/received from/by mobile.

priority priority
Specifies the position priority of the field within the UDR. Lower numbered priorities (across all attribute, event-label, and rule-variable) occur first. priority must be an integer from 1 through 65535. Up to 50 position priorities (across all attribute, event-label, and rule-variable) can be configured.

Usage
Use this command to set the attributes and priority for UDR file format. A particular field in UDR format can be entered multiple times at different priorities. While removing the UDR field using the no attribute command, you can either remove all occurrences of a particular field by specifying the field name or remove a single occurrence by additionally specifying the optional priority keyword.

Consider the following scenario. If the volume/time threshold interval is large enough (or disabled). At time t=0, 10 ICMP packets are sent, which takes 9 seconds. There is nothing for the next 100 seconds, and then again 10 ICMP packets are sent which takes 10 seconds, and then again nothing for next the 60 seconds and then the session is terminated.

In this scenario:

- sn-start-time should be t = 0.
- sn-end-time should be t = 0+9+100+10 (sn-end-time would be the last ICMP packet sent).
- sn-duration should be sn-end-time minus sn-start-time, i.e. 0+9+100+10 – 0 = 119 seconds (since the ICMP flow would exist between the two intervals of sending ICMP packets, the sn-start-time would be that of the first packet of the flow and sn-end-time of the last packet (20th packet). Hence, sn-duration would take into account all the seconds between the first and last packet of the flow).

Example
The following is an example of this command:

    attribute radius-user-name priority 12
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```plaintext
end
```

**Usage**
Use this command to return to the Exec mode.
event-label

This command allows you to specify an optional event label/identifier to be used as an attribute in the UDRs.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > ACS Configuration > UDR Format Configuration

active-charging service service_name > udr-format format_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-acs-udr)#

Syntax

event-label event_label priority priority

no event-label

no
If previously configured, removes the event label configuration.

event_label
Specifies the event label/identifier to be used as UDR attribute.

event_label must be an alphanumeric string of 1 through 63 characters.

priority priority
Specifies the Comma Separated Value (CSV) position of the attribute (label/identifier) in the UDR.

priority must be an integer from 1 through 65535.

Usage
Use this command to configure an optional event label/identifier as an attribute in the UDR and its position in the UDR.

Example
The following is an example of this command:

    event-label radius_csv1 priority 23
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**

Use this command to return to the parent configuration mode.
**rule-variable**

This command allows you to specify fields and their order in UDRs.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > ACS Configuration > UDR Format Configuration

```
active-charging service service_name > udr-format format_name
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-acsc-udr)#
```

**Syntax**

```text
rule-variable rule_variable priority priority
no rule-variable rule_variable [ priority priority ]
```

- **no**
  If previously configured, removes the specified rule variable configuration.

```
rule-variable rule_variable
```

Specifies the rule variable for the UDR format.

**rule_variable** must be one of the following options:

- **bearer 3gpp2**: Bearer-related configuration:
  - *always-on*
  - *bsid*
  - *carrier-id*
  - *esn*
  - *ip-qos*
  - *ip-technology*
  - *meid*
  - *release-indicator*
  - *serv-MDN*
  - *service-option*
  - *session-begin*
  - *session-continue*
**Important:** For more information on protocol-based rules see the *ACS Ruledef Configuration Mode Commands* chapter.

```plaintext
priority priority
```

Specifies the CSV position of the field (protocol rule) in the UDR.

*priority* must be an integer from 1 through 65535.

**Usage**

Use this command to specify what field appears in which order in the UDR.
A particular field in UDR format can be entered multiple times at different priorities. While removing the UDR field using the `no rule-variable` command, you can either remove all occurrences of a particular field by specifying the field name, or remove a single occurrence by additionally specifying the optional priority keyword.

**Example**

The following is an example of this command:

```
rule-variable bearer 3gpp2 bsid priority 36
```
Chapter 298
UDR Module Configuration Mode Commands

The UDR Module Configuration Mode allows you to configure Usage Data Record (UDR) file transfer parameters.

**Mode**

Exec > Global Configuration > Context Configuration > UDR Module Configuration

```bash
configure > context context_name > udr-module active-charging-service
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-udr)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).


**cdr**

This command allows you to configure EDR/UDR file transfer parameters.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Context Configuration > UDR Module Configuration

```
configure > context context_name > udr-module active-charging-service
```

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-udr)#
```

**Syntax**

```
cdr { purge { storage-limit storage_limit | time-limit time_limit } [ max-files max_records_to_purge ] | push-interval push_interval | push-trigger space-usage-percent trigger_percentage | remove-file-after-transfer | transfer-mode { pull [ module-only ] | push primary { encrypted-url encrypted_url | url url } [ [ max-files max_records ] [ max-tasks task_num ] [ module-only ] [ secondary { encrypted-secondary-url encrypted_secondary_url | secondary-url secondary_url } ] [ via local-context ] + ] | use-harddisk }

default cdr [ purge | push-interval | push-trigger space-usage-percent | remove-file-after-transfer | transfer-mode { module-only | push via } | use-harddisk ] +

no cdr [ purge | remove-file-after-transfer | use-harddisk ] +
```

**default**

Configures the default setting for the specified keyword(s):

- **purge**: Disabled
- **push-interval**: 300 seconds
- **push-trigger**: 80 percent
- **remove-file-after-transfer**: Disabled
- **transfer mode**: Pull
- **push via**: line cardMIO is used for push
- **use-harddisk**: Disabled

**Important:** The **use-harddisk** keyword is only available on ASR 5000 chassis.

**no**

If previously configured, disables the specified configuration:

- **purge**: Disables purging of records.
UDR Module Configuration Mode Commands

• **remove-file-after-transfer**: Retains a copy of the file even after it has been pushed or pulled to another server.

• **use-harddisk**: Disables data storage on the SMC hard disk.

---

**Important**: The **use-harddisk** keyword is available only on the ASR 5000 chassis.

```plaintext
purge { storage-limit storage_limit | time-limit time_limit } [ max-files
max_records_to_purge ]
```

Specifies to purge/delete the UDR records based on "time" or "volume" limit. When the configured threshold limit is reached on the hard disk drive, the records that are created dynamically in the `/mnt/hd-raid/data/records/` directory are automatically deleted. Files that are manually created should be deleted manually.

• **storage-limit storage_limit**: Specifies to start deleting files when the specified megabytes of space is used for storage.
  
  `storage_limit` specifies the volume limit for the record files, in megabytes, and must be an integer from 10 through 143360.

• **time-limit time_limit**: Specifies to start deleting files older than the specified time limit.
  
  `time_limit` specifies the time limit for the record files, and must be an integer from 600 through 2592000.

• **max-files max_records_to_purge**: Specifies the maximum number of records to purge.
  
  `max_records_to_purge` can be 0, or an integer from 1000 through 10000. If the value is set to 0, during each cycle, the records will be deleted until the purge condition is satisfied. If the value is set between 1000 and 10000, during each cycle, the records will be deleted until either the purge condition is satisfied or the number of records deleted equals the configured `max-files` value.

  Default: 0

```plaintext
push-interval value
```

Specifies the transfer interval (in seconds) to push UDR/EDR files to an external file server. `value` must be an integer from 60 through 3600.

Default: 300

```plaintext
push-trigger space-usage-percent trigger_percentage
```

Specifies the UDR/EDR disk space utilization percentage, upon reaching which an automatic push is triggered and files are transferred to the configured external server.

`trigger_percentage` specifies the UDR/EDR disk utilization percentage for triggering push, and must be an integer from 10 through 80.

Default: 80%

```plaintext
remove-file-after-transfer
```

Specifies that the system must delete UDR/EDR files after they are transferred to the external file server.

Default: Disabled

Specifies the UDR/EDR file transfer mode.

- **pull**: Specifies that the L-ESS is to pull the UDR files.
- **push**: Specifies that the system is to push UDR files to the configured L-ESS.
- **max-files max_records**: Specifies the maximum number of files sent per iteration based on configured file size.
  Default: 4000
- **max-tasks task_num**: Specifies the maximum number of tasks (child processes) that will be spawned to push the files to the remote server. The `task_num` must be an integer from 4 through 8.
  Default: 4

**Important**: Note that increasing the number of child processes will improve the record transfer rate. However, spawning more child will consume additional resource. So, this option needs to be used with proper resource analysis.

- **module-only**: Specifies that the transfer-mode is only applicable to the UDR module; if not configured it is applicable to both EDR and UDR modules. This enables support for individual record transfer-mode configuration for each module.

- **primary encrypted-url encrypted_url**: Specifies the primary location in encrypted format to which the system pushes the UDR files.
  `encrypted_url` must be the primary location name in an encrypted format, and must be an alphanumeric string of 1 through 1024 characters.

- **primary url url**: Specifies the primary location to which the system pushes the UDR files.
  `url` must be the primary location, and must be an alphanumeric string of 1 through 1024 characters in the format: `//user:password@host:[port]/directory`.

- **secondary encrypted-secondary-url encrypted_secondary_url**: Specifies the secondary location in encrypted format to which the system pushes the UDR files when the primary location is unreachable or fails.
  `encrypted_secondary_url` must be the location in an encrypted format, and must be an alphanumeric string of 1 through 1024 characters.

- **secondary secondary-url secondary_url**: Specifies the secondary location to which the system pushes the UDR files when the primary location is unreachable or fails.
  `secondary_url` must be the secondary location, and must be an alphanumeric string of 1 through 1024 characters in the format: `//user:password@host:[port]/directory`.

- **via local-context**: Selects the LC/SPIO for transfer of UDRs. The system pushes the UDR files via SPIO in the local context.

- **via local-context**: Selects the MIO for transfer of UDRs. The system pushes the UDR files via the MIO in the local context.
### use-harddisk

**Important:** The `use-harddisk` keyword is available only on the ASR 5000 chassis.

Specifies that on an ASR 5000 chassis, the hard disk on the SMC will be used to store UDR/EDR files. When configured to use the hard disk for UDR/EDR storage, UDR/EDR files are transferred from packet processing cards to the hard disk on the SMC.

Specifies that on an ASR 5500 chassis, the hard disk array on the FSCs will be used to store UDR/EDR files. On configuring to use the array for UDR/EDR storage, UDR/EDR files are transferred from DPCs to the array.

Default: Disabled

+ Indicates that more than one of the previous keywords can be entered within a single command.

### Usage

Use this command to configure how UDRs are moved and stored.

On the ASR 5000/ASR 5500 chassis, run this command only from the local context. Running in any other context would fail and deliver an error message.

If PUSH transfer mode is configured, the L-ESS server URL to which the UDR files need to be transferred must be specified. The configuration allows a primary and a secondary server to be configured. Configuring the secondary server is optional. Whenever a file transfer to the primary server fails for four consecutive times, the files will be transferred to the secondary server. The transfer will switch back to the original primary server when:

- Four consecutive transfer failures to the secondary server occur
- After switching from the primary server, 30 minutes elapses

When changing the transfer-mode from pull to push, disable the PULL from L-ESS and then change the transfer mode to push. Make sure that the push server URL configured is accessible from the local context. Also, make sure that the base directory that is mentioned contains udr directory created within it.

When changing the transfer-mode from push to pull, after changing, enable PULL on the L-ESS. Any of the ongoing PUSH activity will continue till all the scheduled file transfers are completed. If there is no PUSH activity going on at the time of this configuration change, all the PUSH related configuration is nullified immediately.

The `cdr use-harddisk` command is available only on the ASR 5000/ASR 5500 chassis. This command can be run only in a context where CDRMOD is running. Configuring in any other context will result in failure with the message “Failure: Please Check if CDRMOD is running in this context or not.”

The `cdr use-harddisk` command can be configured either in the UDR or EDR module, but will be applicable to both record types. Configuring in one of the modules will prevent the configuration to be applied in the other module. Any change to this configuration must be done in the module in which it was configured, the change will be applied to both record types.

The VPNMgr can send a maximum of 4000 files to the remote server per iteration. However if the individual file size is big (say when compression is not enabled), then while transferring 4000 files SFTP operation takes a lot of time. To prevent this, the `cdr transfer-mode push` command can be configured with the keyword `max-files`, which allows operators to configure the maximum number of files sent per iteration based on configured file size.

### Example

The following command configures the system to retain a copy of the data file after it has been transferred to the storage location:
no cdr remove-file-after-transfer
**end**

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
```
end
```

**Usage**
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**
Use this command to return to the parent configuration mode.
file

This command allows you to configure UDR file parameters.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > UDR Module Configuration

configure > context context_name > udr-module active-charging-service

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-udr)#

Syntax

file [ charging-service-name { include | omit } ] [ compression { gzip | none } ] [ current-prefix string ] [ delete-timeout seconds ] [ directory directory_name ] [ exclude-checksum-record ] [ field-separator { hyphen | omit | underscore } ] [ file-sequence-number rulebase-seq-num ] [ headers ] [ name file_name ] [ reset-indicator ] [ rotation [ num-records number | time seconds | volume bytes ] ] [ sequence-number { length length | omit | padded | padded-six-length | unpadded } ] [ storage-limit limit ] [ time-stamp { expanded-format | rotated-format | unix-format } ] [ trailing-text string ] [ trap-on-file-delete ] [ udr-seq-num ] [ xor-final-record ] +

default file [ charging-service-name ] [ compression ] [ current-prefix ] [ delete-timeout ] [ directory ] [ field-separator ] [ file-sequence-number ] [ headers ] [ name ] [ reset-indicator ] [ rotation [ num-records | time | volume ] ] [ sequence-number ] [ storage-limit ] [ time-stamp ] [ trailing-text ] [ udr-seq-num ]

default

Configures the default setting for the specified keyword(s). Using the default file command will reset some but not all keyword parameters to their default values. To ensure that the default is reset for a specific parameter, include the corresponding keyword in the command.

charging-service-name { include | omit }

Specifies to include/exclude name of the charging service in the file name.

• include: Includes name of the charging service in the UDR file name.
• omit: Excludes name of the charging service in the UDR file name.

Default: include

compression { gzip | none }

Configures gzip compression of the UDR file.

• gzip: Enables GNU zip compression of the UDR file at approximately 10:1 ratio.
• none: Disables Gzip compression.
Current-prefix string

Specifies a string to add to the beginning of the UDR file that is currently being used to store UDR records. string must be an alphanumeric string of 1 through 31 characters.
Default: curr

delete-timeout seconds

Specifies a timeout period (in seconds) when completed UDR files are deleted. By default, files are never deleted.
seconds must be an integer from 3600 through 31536000.
Default: Disabled

directory directory_name

Specifies a subdirectory in the default directory in which to store UDR files.
directory_name must be an alphanumeric string of 1 through 191 characters.
Default: /records/udr

exclude-checksum-record

When entered, this keyword excludes the final record containing #CHECKSUM followed by the 32-bit Cyclic Redundancy Check (CRC) of all preceding records from the UDR file.
Default: Disabled, inserts checksum record into the UDR file header.

field-separator { hyphen | omit | underscore }

Specifies the field separators to be used between two fields of a UDR file name.

- **hyphen**: Specifies to use ‘-’ (hyphen) as the field separator.
- **omit**: Excludes the field separator.
- **underscore**: Specifies to use ‘_’ (underscore) as the field separator.

Default: underscore

file-sequence-number rulebase-seq-num

Generates unique file sequence numbers for different rulebase-format-name combinations.

headers

Includes a file header summarizing the record layout.

name file_name

Default: udr

Specifies a string to use as the base file name for UDR files.
file_name must be an alphanumeric string of 1 through 31 characters. The file name format is as follows:
base_rulebase_format_sequence_num_timestamp

- **base**: Specifies type of record in file or contains the operator-specified string. Default: udr
- **rulebase**: Specifies the name of the ACS rulebase. UDRs from different rulebases go into different UDR files.
- **format**: Specifies the name of the UDR format if single-udr-format is specified, else the format field (and the trailing underscore) is omitted from the file name.
• **sequencenum**: This is a 5-digit sequence number to detect the missing file sequence. It is unique among all UDR files on the system.

• **timestamp**: Contains a timestamp based on file creation time in UTC formatted as: MMDDYYYYHHMMSS.

UDR files that have not been closed have a string added to the beginning of their file names. File name for a UDR file in CSV format that contains information for a rulebase named `rulebase1` and a UDR schema named `udr_sch1` appears as follows: `udr_rulebase1_udr_sch1_00005_01302006143409`

If file name is not configured, the system creates files for EDRs/UDRs/FDRs (xDRs) using the following name template with limits to 256 characters:

```
basename_ChargSvcName_timestamp_SeqNumResetIndicator_FileSeqNumber
```

• **basename**: A global-based configurable text string that is unique per system that uniquely identifies the global location of the system running ACS.

• **ChargSvcName**: A system context-based configurable text string that uniquely identifies a specific context-based charging service.

• **timestamp**: Date and time at the instance of file creation. Date and time in the format: “MMDDYYYYHHmmSS”, where HH is a 24-hour value from 00-23.

• **SeqNumResetIndicator**: A one-byte counter used to discern the potential for duplicated FileSeqNumber with a range of 0 through 255, which is incremented by a value of 1 for the following conditions:

  • Failure of an ACS software process on an individual packet processing card
  • Failure of the system such that a second system takes over (for example, a standby or backup chassis put in place according to Inter-chassis Session Recovery)
  • File Sequence Number (FileSeqNumber) rollover from 999999999 to 0

• **FileSeqNumber**: unique file sequence number for the file is a 9-digit integer from 000000000 through 999999999. It is unique on each chassis.

File name for a closed xDR file in CSV format that contains information for ACS `xyz_city1` and charging service name `preapaid2` with timestamp `12311969190000`, and file sequence number counter reset indicator to `002` for file sequence number `0349390002` appears as follows: `xyz_city1_preapaid2_12311969190000_002_034939002`

File name for a running xDR file in CSV format that contains information for the same parameters for file sequence number `034939003` prefixed with `curr_` and appears as follows: `curr_xyz_city1_preapaid2_12311969190000_002_034939002`

---

**Important**: When the "rulebase name" and "edr-format-name" options are enabled through this `file` command, if the "field-separator" value is "underscore" (default value) then, in the filename, the fields Rulebase name and EDR format name will be separated by "hyphen". If the "field-separator" value is "hyphen" then, in the filename, the fields Rulebase name and EDR format name will be separated by "underscore". This will ensure that the number of the fields in the filename is not increased and does not affect the backend billing system.

**reset-indicator**

Specifies to include the reset indicator counter value, from 0 to 255, in the UDR file name and is incremented (by one) whenever any of the following conditions occur:

• An ACSMgr/SessMgr process fails.

• An Inter-chassis Session Recovery (ICSR) peer chassis has transitioned from standby to active.

• The sequence number in sequence-number keyword has rolled over to zero.
UDR Module Configuration Mode Commands

---

**rotation** { num-records records | time seconds | volume bytes }

Specifies when to close a UDR file and create a new one.

- **num-records records**: Specifies the number of records that should be added to the file. When the number of records in the file reaches this specified value, the file is complete.
  - *records* must be an integer from 100 through 10240.
  - Default: 1024

- **time seconds**: Specifies the period of time to wait before closing the UDR file and creating a new one.
  - *seconds* must be an integer from 30 through 86400.
  - Default: 3600 seconds

- **volume bytes**: Specifies the maximum size of the UDR file before closing it and creating a new one.
  - *bytes* must be an integer from 51200 through 62914560.
  - Default: 102400 bytes

  Note that higher settings may provide the best compression ratio when the **compression** keyword is set to gzip.

---

**sequence-number** { length length | omit | padded | padded-six-length | unpadded }

Specifies including or excluding the sequence number in the file name.

- **length length**: Includes the sequence number with the specified length.
  - *length* must be the length of the file sequence number with preceding zeroes in the file name, and must be an integer from 1 through 9.

  *Important*: The length configuration is applicable in both UDR and EDR modules. When applied in both modules without the file udr-seq-num configuration, the minimum among the two values will come into effect for both modules. With the file udr-seq-num config, each module will use its own value of length.

- **omit**: Excludes the sequence number from the file name.

- **padded**: Includes the padded sequence number with preceding zeros in the file name. This is the default setting.

- **padded-six-length**: Includes the padded sequence number with six preceding zeros in the file name.

- **unpadded**: Includes the unpadded sequence number in the file name.

  Default: padded

---

**storage-limit limit**

Specifies deleting files when the specified amount of space, in bytes, is used up for UDR/EDR file storage on packet processing card RAM.

On an ASR 5000/ASR 5500 chassis, *limit* must be an integer from 10485760 through 536870912.

Default: 33554432

*Important*: On the ASR 5000 chassis, the total storage limit is 536870912 bytes (512 MB). This limit is for both UDR and EDR files combined.
time-stamp { expanded-format | rotated-format | unix-format }

Specifies the timestamp of when the file was created be included in the file name.

- **expanded-format**: Specifies the UTC MMDDYYYYHHMMSS format.
- **rotated-format**: Specifies the YYYYMMDDHHMMSS format.
- **unix-format**: Specifies the UNIX format of \( x.y \), where \( x \) is the number of seconds since 1/1/1970 and \( y \) is the fractional portion of the current second that has elapsed.

trailing-text string

Specifies the inclusion of arbitrary text string in the file name. 
string must be an alphanumeric string of 1 through 30 characters.

trap-on-file-delete

Instructs the system to send an SNMP notification (starCDRFileRemoved) when an UDR/EDR file is deleted due to lack of space.
Default: Disabled

udr-seq-num

Specifies that the file sequence numbers that are part of the UDR file names be independently generated. If disabled, a single set of sequence numbers are shared by both UDR and EDR files.
Default: Disabled

xor-final-record

Specifies inserting an XOR checksum (in place of the CRC checksum) into the UDR file header if the exclude-checksum-record keyword is left at its default setting.
Default: Disabled

More than one of the previous keywords can be entered within a single command.

Usage

Use this command to configure UDR file characteristics.

Example

The following command sets the prefix of the current active UDR file to **current**:

`file current-prefix current`

The following command sets the base file name to **UDRfile**:

`file name UDRfile`

---

Cisco ASR 5x00 Command Line Interface Reference
Chapter 299
Video Group Configuration Mode

The Video Group Configuration Mode is used to add CAEs to a CAE group and configure the CAEs for load balancing and health-check monitoring. The CAE (Content Adaptation Engine) is an optional component of the Mobile Videoscape. For additional information, refer to the Mobile Video Gateway Administration Guide.

Mode

Exec > Global Configuration > Context Configuration > Video Group Configuration

`configure > context context_name > cae-group group_name`

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-vgroup)#
```

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
end

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
exit
```

**Usage**
Use this command to return to the parent configuration mode.
keepalive-server

Specifies keep-alive messaging information for Content Adaptation Engine (CAE) health-check monitoring, which is part of CAE load balancing on the Mobile Video Gateway. Note that this command and its options configure settings that apply to all CAEs in the CAE group, not to an individual CAE.

Product

MVG

Privilege

Security Administrator, Administrator

Mode

Exec > Global Configuration > Context Configuration > Video Group Configuration

configure > context context_name > cae-group group_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-vgroup)#

Syntax

[ default ] keepalive-server
deadtime seconds interval seconds num-retry num-retries port
port_number timeout seconds [ -noconfirm ]

default keepalive-server

Sets the CAE keep-alive settings to their default values.

keepalive-server
deadtime seconds interval seconds num-retry num-retries port
port_number timeout seconds [ -noconfirm ]

Specifies keep-alive messaging information for CAE health-check monitoring.

deadtime seconds

Specifies the periodic retry interval (in seconds) after a CAE is detected down. seconds is an integer from 1 through 1800. The default value is 120 seconds.

interval seconds

Specifies the interval (in seconds) for how often the Mobile Video Gateway sends a keep-alive message to the CAEs. seconds is an integer from 0 through 120. The default value is 10 seconds. A value of 0 turns off keep-alive detection and marks the state of all CAEs to Up.

num-retry num_retries

Specifies the number of keepalive retries after a CAE does not respond. num_retries is an integer from 1 through 20. The default value is 3 retries.

port port_number

Specifies the TCP port number for health-check monitoring, which is an integer from 1 through 65535. The default value is 5100.
timeout seconds
Specifies the keep-alive timeout (in seconds) which is an integer from 1 through 30. The default value is 3 seconds.

-noconfirm
Specifies that the command must execute without prompting for confirmation.

Usage
Use this command to specify keep-alive messaging information for CAE health-check monitoring, which is part of CAE load balancing on the Mobile Video Gateway.

Example
The following command specifies keep-alive messaging information for the CAEs in the CAE group:

    keepalive-server deadtime 120 interval 10 num-retry 3 port 5100 timeout 3
local-address

Specifies the local IPv4 address on the Mobile Video Gateway for the keepalive TCP connection used for Content Adaptation Engine (CAE) load balancing.

Product
MVG

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Video Group Configuration
configure > context context_name > cae-group group_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-vgroup)#

Syntax

[ no ] local-address IPv4_address [ -noconfirm ]

no local-address IPv4_address
Deletes the local IPv4 address if previously specified.

local-address IPv4_address
Specifies the local IPv4 address on the Mobile Video Gateway for the keep-live TCP connection used for CAE load balancing. IPv4_address must be in dotted decimal notation.

-noconfirm
Specifies that the command must execute without prompting for confirmation.

Usage

Use this command to specify the local IPv4 address on the Mobile Video Gateway, in dotted-decimal notation.

Example

The following command specifies the local IPv4 address on the Mobile Video Gateway:

local-address 10.2.3.4
server

Adds a CAE (Content Adaptation Engine) and its IPv4 address and port number to the associated CAE group. The Mobile Video Gateway uses this information for CAE load balancing. The Mobile Video Gateway has a system limit of 64 CAEs.

Product
MVG

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Context Configuration > Video Group Configuration
configure > context context_name > cae-group group_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-vgroup)#

Syntax

[ no ] server cae_name address IPv4_address port port_number [ -noconfirm ]

no server cae_name

Deletes the CAE from the CAE group if previously configured.

server cae_name address IPv4_address port port_number

Adds a CAE and its IPv4 address and port number to the associated CAE group. cae_name is an alphanumeric string of 1 through 15 characters. IPv4_address must be in dotted-decimal notation. port_number is an integer from 1 through 65535. The default value is 80.

-noconfirm

Specifies that the command must execute without prompting for confirmation.

Usage

Use this command to add a CAE and its IPv4 address and port number to the associated CAE group.

Example

The following command adds a CAE named cae_1 and its IPv4 address and port number to the associated CAE group:

server cae_1 address 10.2.3.4 port 80
Chapter 300
VLAN Configuration Mode Commands

The VLAN Configuration Mode is used to create and manage Virtual LANs and their bindings with contexts.

Mode

Exec > Global Configuration > Port Configuration > VLAN Configuration

configure > port ethernet slot_number/port_number > vlan vlan_tag_id

Entering the above command sequence results in the following prompt:

[local]host_name(config-port-slot_number/port_number-vlan-vlan-id)#

Important: Available commands or keywords/variables vary based on platform type, product version, and installed license(s).
bind interface

Associates a VLAN interface with a context.

Product
HA
HSGW
PDSN
P-GW
SAEGW
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Port Configuration > VLAN Configuration

configure > port ethernet slot_number/port_number > vlan vlan_tag_id

Entering the above command sequence results in the following prompt:

[local]host_name(config-port-slot_number/port_number-vlan-vlan-id)#

Syntax
[ no ] bind interface interface_name context_name

no
Disasscoiates the VLAN interface from the context.

interface_name context_name

Specifies the name of the virtual interface and the context to which it will be bound.
interface_name must be an alphanumeric string of 1 through 79 characters.
context_name must refer to a previously configured context expressed as an alphanumeric string of 1 through 79 characters.

Usage
Bind a VLAN interface to a context to suport VLAN service.

Example
bind interface sampleVirtual sampleContext

no bind interface sampleVirtual sampleContext
end

Exits the current configuration mode and returns to the Exec mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax

end

Usage
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

Product
All

Privilege
Security Administrator, Administrator

Syntax
exit

Usage
Use this command to return to the parent configuration mode.
ingress-mode

Enables or disables port ingress (incoming) mode for this VLAN ID on this port.

**Product**
- HA
- HSGW
- PDSN
- P-GW
- SAEGW
- SGSN

**Privilege**
Security Administrator, Administrator

**Mode**
Exec > Global Configuration > Port Configuration > VLAN Configuration

```plaintext
configure > port ethernet slot_number/port_number > vlan vlan_tag_id
```

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-port-slot_number/port_number-vlan-vlan-id)#
```

**Syntax**

```
[ no ] ingress-mode
```

- **no**
  Disables the port ingress mode.

**Usage**

Use this command to enable or disable the VLAN ingress mode for this port.

**Example**

```
ingress-mode
```
priority

Sets the 802.1p VLAN priority bit.

Product
All

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Port Configuration > VLAN Configuration

configure > port ethernet slot_number/port_number > vlan vlan_tag_id

Entering the above command sequence results in the following prompt:

[local]host_name(config-port-slot_number/port_number-vlan-vlan-id)#

Syntax

priority value

no priority

no
Disables the setting of the 802.1p priority bit.

value
Sets the value of the 802.1p priority bit as an integer from 0 through 7, with 7 being the highest priority.

Usage
Set a value for the VLAN priority bit.

Example
To set a VLAN priority bit value, use the following command:

    priority 3

To disable the use of a VLAN priority bit, use the following command:

    no priority
shutdown

Disables or enables traffic over this VLAN.

Product
HA
HSGW
PDSN
P-GW
SAEGW
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Port Configuration > VLAN Configuration

configure > port ethernet slot_number/port_number > vlan vlan_tag_id

Entering the above command sequence results in the following prompt:

[local]host_name(config-port-slot_number/port_number-vlan-vlan-id)#

Syntax

[ no ] shutdown

no

Enables the VLAN. When omitted the VLAN is shutdown.

Usage
Shut down a VLAN.
To bring a VLAN into service, execute this command using the no keyword.

Example
To disable a VLAN from sending or receiving network traffic use the following command:

shutdown

To enable a VLAN use the following command:

no shutdown
vlan-map

Associates an IP interface having a VLAN ID with a context.

Product
HA
HSGW
PDSN
P-GW
SAEGW
SGSN

Privilege
Security Administrator, Administrator

Mode
Exec > Global Configuration > Port Configuration > VLAN Configuration

configure > port ethernet slot_number/port_number > vlan vlan_tag_id

Entering the above command sequence results in the following prompt:

[local]host_name(config-port-slot_number/port_number-vlan-vlan-id)#

Syntax

vlan-map interface if_name context_name

interface if_name context_name

Associates the specified VLAN interface with a context.
if_name is an existing interface name specified as an alphanumeric string of 1 through 79 characters.
context_name is an existing context name specified as an alphanumeric string of 1 through 79 characters.

Usage
Use vlan-map to associate multiple VLAN interfaces with a single context. This feature is used in conjunction with nexthop forwarding and overlapping IP pools.

Example

vlan-map interface vlan234 ingress
Chapter 301
WSG Lookup Priority List Configuration Mode Commands

The Wireless Security Gateway Lookup Priority List Configuration Mode is used to set the priority of subnet components for site-to-site tunnels. This is a Security Gateway (SecGW) feature [VPC-VSM only].

Mode

Exec > Global Configuration > WSG-Lookup Priority List Configuration

cconfigure >> wsg-lookup

Entering the above command sequence results in the following prompt:

host_name(config-wsg-lookup)#

⚠️ **Important**: The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).
**end**

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
```
end
```

**Usage**
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**

All

**Privilege**

Security Administrator, Administrator

**Syntax**

`exit`

**Usage**

Use this command to return to the parent configuration mode.
priority

Sets the priority level for a WSG subnet combination (source and destination netmasks). It also disables an existing priority for a specified subnet combination. (VPC-VSM only).

Product
SecGW

Privilege
Security Administrator

Mode
Exec > Global Configuration > WSG-Lookup Priority List Configuration

configure >> wsg-lookup

Entering the above command sequence results in the following prompt:

Syntax

priority priority_level source-netmask subnet_size destination netmask subnet_size

no priority priority_level source-netmask subnet_size destination netmask subnet_size

no
Disables the priority for the specified subnet combination.

priority priority_level
Specifies the priority level for the subnet combination as an integer from 1 through 6.

source-netmask subnet_size
Specifies the subnet size for the source netmask as an integer from 1 through 128.

destination netmask subnet_size
Specifies the subnet size for the destination netmask as an integer from 1 through 128.

Usage
Use this command to set the priority level for a WSG subnet combination (source and destination netmasks). It can also be used to disable an existing priority for a specified subnet combination.

Example
The following command sets a priority of 2 for a subnet combination with a /32 subnet size.

priority 2 source-netmask 32 destination-netmask 32
Chapter 302
WSG Service Configuration Mode Commands

The Wireless Security Gateway Configuration Mode is used to define the operating parameters for IPSec-based access control and handling of Encapsulating Security Payload (ESP) packets.

Mode

Exec > Global Configuration > Context Configuration > WSG-Service Configuration

configure > context context_name > wsg-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-wsg-service)#

**Important:** The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

**Important:** Any changes made to a WSG service require that the service be restarted to apply any changed parameters. You restart the service by unbinding and binding the IP address to the service context.
**bind address**

Binds the WSG service to the specified IPv4 or IPv6 address and crypto template (VPC only).

**Product**
SecGW (WSG)

**Privilege**
Security Administrator

**Mode**
Exec > Global Configuration > Context Configuration > WSG-Service Configuration
configure > context context_name > wsg-service service_name

Entering the above command sequence results in the following prompt:

```
/context_name/host_name(config-wsg-service)#
```

**Syntax**

```
bind address ip_address crypto-template template_name

no bind address
```

**Usage**

Unbinds the WSG service from the IP address.

**Example**

The following command binds the WSG service to 10.1.1.1.

```
bind address 10.1.1.1 crypto template tplt01
```
deployment-mode

Specifies the deployment mode for the WSG service (VPC only).

Product
SecGW (WSG)

Privilege
Security Administrator

Mode
Exec > Global Configuration > Context Configuration > WSG-Service Configuration
configure > context context_name > wsg-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-wsg-service)#

Syntax

deployment-mode { remote-access | site-to-site }

no deployment-mode

no

Deletes deployment mode from the configuration.

{ remote-access | site-to-site }

Specifies the deployment mode as either:

- remote-access – support direct user communication with this WSG
- site-to-site – support bidirectional communication with two or more WSGs

Usage
Specifying remote access or site-to-site communication as the deployment mode for this WSG.

Example
This command deploys this WSG for remote access:

deployment-mode remote-access
**end**

Exits the current configuration mode and returns to the Exec mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**

```
end
```

**Usage**
Use this command to return to the Exec mode.
exit

Exits the current mode and returns to the parent configuration mode.

**Product**
All

**Privilege**
Security Administrator, Administrator

**Syntax**
exit

**Usage**
Use this command to return to the parent configuration mode.
ip

Specifies the IPv4 access group and address allocation method for this WSG service (VPC only).

Product
SecGW (WSG)

Privilege
Security Administrator

Mode
Exec > Global Configuration > Context Configuration > WSG-Service Configuration
 configure > context context_name > wsg-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-wsg-service)#

Syntax

ip { access-group group_name | address { alloc-method { dhcp-proxy | local } | pool name pool_name }

no ip access-group group_name

no ip address alloc-method pool_name

no ip address pool name pool_name

Usage

Use this command to specify the IPv4 access group and IPv4 address allocation method for this WSG service. This command and its keywords are subject to the following limitations:
• The WSG service configuration takes precedence over the equivalent configuration in Subscriber mode or the template payload.

• The WSG service must be restarted to apply the parameters. You restart the service by doing an unbind and bind.

• Up to 16 named IPv4 pools can be configured. The list is sorted, and the addresses are allocated from the first pool in the list with available addresses.

• One IPv4 ACL can be configured.

• The IPv4 pools will only be used for IPv4 calls.

**Example**

This command specifies the IPv4 address pool named *pool401*:

```
ip address pool name pool401
```

This command specifies the use of a previously configure DHCPv4 service to allocate IPv4 addresses:

```
ip address alloc-method dhcp-proxy
```
ipv6

Specifies the IPv6 access group and prefix pool for this WSG service (VPC only).

Product
SecGW (WSG)

Privilege
Security Administrator

Mode
Exec > Global Configuration > Context Configuration > WSG-Service Configuration
configure > context context_name > wsg-service service_name

Entering the above command sequence results in the following prompt:

[context_name]host_name(config-wsg-service) #

Syntax

ipv6 { access-group group_name | address prefix-pool pool_name }
no ipv6 access-group group_name
no ipv6 address prefix-pool

no

Deletes the specified parameter.

access-group group_name

Specifies an existing IPv6 ACL access group as an alphanumeric string of 1 through 47 characters. For additional information, see IPv6 ACL Configuration Mode Commands.

address prefix-pool pool_name

Specifies an existing IPv6 prefix pool as an alphanumeric string of 1 through 31 characters. For additional information, see Subscriber Configuration Mode Commands.

Usage

Specify the IPv6 access group and prefix pool for this WSG service.
This command and its keywords are subject to the following limitations:
• The WSG service configuration takes precedence over the equivalent configuration in Subscriber mode or the template payload.
• The WSG service must be restarted to apply the parameters. You restart the service by doing an unbind and bind.
• One named IPv6 pool can be configured.
• One named IPv6 ACL can be configured.
• The IPv6 pools will only be used for IPv6 calls.

Example
This command specifies the IPv6 prefix pool named pool601:

```
ipv6 prefix-pool name pool601
```
pre_fragment mtu

Specifies the Maximum Transmission Unit (MTU) size which when exceeded initiates pre-tunnel (before encryption) fragmentation of IPSec Encapsulated Security Payload (ESP) packets within this WSG service (VPC only).

Product
SecGW (WSG)

Privilege
Security Administrator

Mode
Exec > Global Configuration > Context Configuration > WSG-Service Configuration
configure > context context_name > wsg-service service_name

Entering the above command sequence results in the following prompt:

[context_name] host_name(config-wsg-service)#

Syntax

pre_fragment mtu size

no pre_fragment size

default pre_fragment size

Usage
Disables this function.

Sets the MTU size to the default value of 1400 bytes.

Specifies the MTU size in bytes as an integer from 576 through 2048. Default = 1400

Example
The following command sets MTU size to 2048 bytes.

pre_fragment mtu 2048